Image Watermarking: A Review of Literature

Amrinder Singh

M phil. Research Scholar at Department of Computer Science
Punjabi University, Patiala, Punjab, India

Abstract—Image watermarking is the process of embedding secret information without degrading the quality original image. The main objective of watermarking is to provide copyright protection, content authentication, ownership identification and data integrity. In this paper we classify the robust, fragile and semi-fragile watermarking techniques based on different domains in which data is embedded. Detailed literature survey of various applications and existing watermarking techniques is done. To evaluate the performance of watermarking scheme Peak signal to noise ratio (PSNR), Bit error rate (BER) and normalised correlation (NC) are described.

Keywords—Robust watermarking, Fragile watermarking, Semi-fragile watermarking DCT, DWT, DFT.

I. INTRODUCTION

WATERMARKING is the process of hiding digital information in a carrier signal to protect the digital multimedia data [1]. Digital multimedia such as digital photographs, digital music or digital video. Watermarks are embedded in the multimedia objects (digital content) for several reasons like copyright protection, content authentication, tamper detection etc. Various types of watermarks have been developed for different types of applications. One is visible watermarks and other is invisible watermarks. Visible watermarks are easily detected by the observer but invisible watermarks are imperceptible. There are three essential factors those are generally used to determine quality of watermarking scheme [2].

A. Robustness to Attacks

It means that the Watermark should be difficult to remove or destroy. Robust is a measure of resistance of watermark against various types of attacks to image like compression, filtering, rotation, scaling, collision attacks, resizing, cropping etc.

B. Visual Imperceptibility

It means that the quality of host image should not be degraded by presence of watermark and it is very difficult to perceive by the viewers. In order to achieve good visual imperceptibility, digital watermarking scheme takes the advantage of the human visual system (HVS) models.

C. Capacity

The maximum amount of watermark information is embedded into the host image without degradation of image.

II. GENERAL PROCEDURE

The general process of watermarking consists of watermark generation, watermark embedding and watermark detection. The watermark can be pseudo random numbers, binary image, logo or gray scale image which is embedded into the original image. Once the watermark is embedded to the original image it suffers from various unintentional attacks (like compression) and intentionally attacks (like cropping). Watermark should be robust against these types of attacks. Watermark detector is used to check the existence of the watermark either by comparing it with the original image and find out the watermark (known as non-blind watermarking) or by using correlation measure is used to detect the strength of the extracted watermark (blind watermarking) [3].

III. CLASSIFICATION OF WATERMARKING

The classification of image watermarking is done according to application specification, embedding domain, human perceptibility and detection process.

A. Robust, Fragile and Semi-fragile Watermarking

According to the specific application requirements, watermarking can be categorised into robust, fragile and semi fragile. Robust watermark is embedded in the digital image and resist against various transformations like geometric transformation (such as rotation, scaling) and compression. Robust watermarking is used in various types of application like owner identification, proof of ownership and copy right protection. In the fragile watermarking the
watermarks are sensitive against malicious or non-malicious attacks. Various applications like image authentication and content integrity verification use the fragile watermarking. If any slightest amount of modification is done the watermarks are expected to be completely destroyed. And in semi fragile watermarking minor transformations are allowed such as lossy compression but major changes are not allowed.

B. Spatial and Frequency Domain

In spatial domain the watermark is embedded into the digital image by directly modifying the intensity of the pixels. Mostly modifications are done in the least significant bits of original contents. In frequency domain watermarks are inserted into the digital contents by modifying the transform coefficients of an image and inverse transform is applied to obtain the watermarked image. Various transform such as discrete Fourier transform, discrete cosines transform and discrete wavelets transforms are existed.

C. Visible and Invisible

Visible watermarking is associated with the perception of the human eye. A visible watermark is a visible semi-transparent text or image overlaid on the original image such as owner logo or copyright sign. A watermarking technique in which watermark is embedded in the digital image in such a way that it cannot be perceived with human’s eyes and only detected by using the watermark detecting techniques is called the invisible watermarking.

D. Blind and Informed Watermarking

Both blind and informed detectors are available to detect the watermark in the digital images. The detector which is used to detect the watermark without the knowledge of the original image or embedded watermark is known as the blind detector. The detector which requires some information about the host watermark signal for extraction is known as informed detector. Blind detector is more complicated to implement as compared to the informed detector.

IV. APPLICATION AREAS OF WATERMARKING

There are various applications of digital watermarking. Some broad application areas in which digital watermarking can be classified are broadcast monitoring, owner identification, authentication, proof of ownership, transaction tracking, copy control, device control, and legacy enhancements [1].

A. Broadcast Monitoring

A major scandal broke out in Japan regarding the overbooking of air time by a broadcasting station in 1997. Advertisers were paying for thousands of commercials that were never aired. For more than 20 years broadcast stations cheated the advertisers because there were no systems in place to monitor the actual broadcast of advertisements. To avoid such scams, watermarking is an alternative method for active monitoring to ensure that the commercials are broadcast at the times and locations of their agreement with broadcasters. Broadcast monitoring is becoming trendy because it is used for the prevention of illegal distribution of digital data, to ensure that accurate royalty payments are given to musicians and actors ensuring the advertisers that they received correct air time purchased from broadcasting firms. In broadcast monitoring we can add a unique watermark in each video or sound clip before broadcast and automated monitoring stations can then receive broadcasts and look for these watermarks, identifying when and where the content appears. Numerous companies provide watermark based broadcast monitoring services. For example, Teletrax offers a service that is based on video watermarking technology from Philips.

B. Owner Identification

Text copyright notice is no longer essential to give assurance of copyrights but still recommended. The main limitation of such a copyright is that it is very easy to remove. Digital watermarking provides the security of copyrights through owner identification. Robust watermarking is used to insert the information about the original owner of the digital data because it stays alive after intentional or unintentional attacks to remove watermark. A robust watermark cannot be removed without affecting the quality of watermarked digital data. A watermark is the integral part of digital content so no extra space is required to store it. The Digimarc Corporation provides a watermarking system in which watermark embedder and detector are bundled with Adobe’s popular image processing program, Photoshop. When the detector finds a watermark, it contacts a central database to identify the watermark’s owner. And use the watermark message as a key to find contact information for the image’s owner.

C. Content Authentication

The content of digital data can easily be altered such that it is very complicated to detect what has been changed. Digital contents related to medical images, identity proofs, commercials transactions, paintings, photographs for court evidence, it is extremely important to make sure that the contents from a specific source are authentic. Fragile watermark is embedded to the digital data at the source that can authenticate the integrity of digital contents if there is minor change in digital contents watermark is not detected. In some cases we need a watermark which survive after minor transformations,
such as lossy compression, but are invalidated by major changes is called semi fragile watermarks. Temper detection and content authentication are closely related. If content is detected to be tempered, this means that it is not authenticate, but in temper detection techniques are based on the concept of localisation to discover the particular regions where the modification is done.

D. Proof of Ownership

Watermarking is not only used to identify copyright ownership but to actually prove ownership. This cannot be done with the textual notice because it can be so easily forged. Let’s take an example two person claims to own copyright of a digital image. In such a case it is very hard to find the rightful owner. To solve this problem in order to directly prove the image ownership, it is easy to prove ownership of the watermarked message inserted in it. Embedding a watermark in the digital images is constructive to prove the ownership.

E. Transaction Tracking

In transaction tracking each recipient is provided with the customized copy of the electronic data to prevent the illegal distribution. Unique label is embed in the digital content is known as fingerprint. If later unauthorised copies of the contents are found, with the help of fingerprints the origin of the piracy can be located. The transaction tracking system was implemented by DiVX Corporation. Each DiVX-enabled player inserts a unique watermark into every video that it played. If illegal copies of movies are found, then DiVX track the source of piracy by using watermarks.

F. Copy Control

To prevent the illegal copying of the digital data watermarking plays an effective role. Watermarks are embedded in the digital content itself, indicating the number of copies that are permitted. Only numbers of permission able copies are accepted and implemented with a special kind of detector that controls the watermark after each copy is created.

G. Legacy Enhancement

Sometimes a system needs an upgrade to enhance the functionality but this upgrade may be incompatible with the existing system. For example most of the countries in the world are currently transitioning from analog to digital television. This process is a costly and time-consuming. During this transition, the legacy analog system must continue to function until totally new digital broadcasting equipment must be introduced and consumers must purchase digital television receivers. Digital watermarking can be used to improve the functionality of legacy system. One example is Tektronix’s digital watermark encoder for synchronizing audio and video signals [4]. When the video and audio channels of a television signal are processed separately problem of lip-sync occurs. In which the motion of the lips is either ahead or behind the speech. The Tektronix product inserts a highly compressed version of the audio signal within the video signal, before any digital signal processing. After signal processing the real-time audio signal is compared with the embedded signal to adjust the time delays before broadcasting.

V. ROBUST WATERMARKING

Robust image watermarking is a technique in which watermark has ability to resist against various types of attacks such as geometric attacks and non geometric attacks. Literature survey of the robust digital image watermarking algorithms and techniques is presented subsequently.

A. Robust Watermarking Techniques in Spatial Domain

Nikolaidis and Pitas [5] in this paper spatial domain copyright protection method is proposed in which watermark is embedded by slightly modifying the intensity of randomly selected pixels of image. Blind watermarking is used in the detection process i.e. Original image is not required at the time of watermark detection and the process is carried out by comparing the mean intensity value of marked pixels against that of the unmarked pixels. Watermark is resistant to JPEG compression and low pass filter. Kampan et al. [6] in this paper spatial domain watermarking for digital image is proposed. The watermark which is binary image embedded into the original image. First the host image is divided into several blocks of different sizes and then brightness of pixels in each block is adjusted. Quality of watermarked image is least affected and robust against various types of degradation. Nasir et al. [7] have proposed a new robust watermarking technique based on a block probability in spatial domain for colour images. A binary watermark image is embedded four times in different positions. Non blind watermarking scheme is used i.e. original image is required at the time of watermark extraction. Watermark is robust against various image processing operations such as filtering, compression, scaling, cropping, rotation, randomly removal of some rows and columns lines, self similarity and salt and pepper noise.

B. Robust Watermarking Techniques in Frequency Domain

1) DCT Domain Techniques: Cox et al. [8] introduces a technique for robust watermarking, the watermark is based on the 1000 random samples which are added into the 1000 largest DCT coefficients of the original image except the DC term located in (0,0) of the DCT matrix and inverse DCT is
performed to retrieve the watermarked image. Watermark extraction was based on presence of original image and exact frequency locations of the watermark. Lin et al. [9] have proposed a new approach to image watermarking based on the DCT. By the concept of mathematical reminder we adjust the DCT low frequency coefficients to safeguard the visual quality of the watermarked image. Watermark is embedded into the low frequency components of the covered image in DCT frequency domain. This technique is more suitable for robustness of watermark against highly JPEG compressed image. Gupta et al. [10] have proposed efficient algorithm which is useful for protecting the distribution rights of digital images. Watermark bits are pseudo random numbers generated by Linear Feedback Shift Register (LFSR). Watermark is embedded into the DCT coefficients of the host image. Robustness against major image processing attacks is achieved.

2) DFT Domain Techniques: Solachidis and Pitas [11] have proposed a method for digital image watermarking in which they embed a circularly symmetric watermark in the magnitude of the DFT domain. Since the watermark is circular in shape with its centre at image centre it is robust against geometric rotation attacks. Watermarking detection is done by the correlation and original image is not required in the process. The technique is computationally not expensive to recover from rotation. Robustness against cropping, scaling, JPEG compression, filtering, noise addition and histogram equalization is demonstrated. Poljicak et al. [12] have developed a method to minimize the degradation of an image due to the implementation of a watermark in the frequency domain of the image. Embedding process of watermark is done in the magnitudes of the DFT. Quality of degradation is measure by using the PSNR ratio. The obtained results were used to develop a watermarking strategy that chooses the optimal radius of the implementation to minimize quality degradation. The proposed method showed excellent robustness to the attacks from the StirMark benchmark, halftoning, print-scan process and print-cam process.

3) DWT Domain Techniques: Barni et al. [13] have proposed a novel blind watermarking algorithm, which embeds the watermark in the DWT domain by exploiting the characteristics of the HVS, is presented. In contrast to previous methods in the DWT domain, masking is accomplished pixel by pixel by taking into account the texture and the luminance content of all the image sub bands. The watermark is adaptively embedded to the largest detail bands which consist of a pseudorandom sequence. For detection procedure compute the correlation between the watermarked coefficients and the watermarking code. The value of the correlation is compared to a threshold to decide whether the watermark is present or not. Robustness is checked under the JPEG and wavelet-based compression, median filtering, Gaussian noise addition, multiple marking, cropping plus zero padding, and morphing. Wang and Lin have [14] proposed a blind watermarking technique for copyright protection based on wavelet tree quantization. Wavelet coefficients of original image are combined to form super trees. Watermark bits are embedded into different frequency bands and watermark is spread throughout large spatial regions. This watermark scheme resist to both frequency based and time domain geometric attacks. Experimental results show that proposed method is robust to various frequency based attacks such as JPEG compression and time domain attacks such as rotation. Lin et al. [15] have proposed a blind watermarking based on maximum wavelet coefficient quantization. Variable numbers of wavelet coefficients are grouped into blocks which are selected from different sub bands. To embed a watermark bit we quantize the maximum coefficients of the block. In the extraction phase the watermark is extracted without using the original image. Experimental results show that proposed method is robust against common geometric and non geometric attacks. Keyvanpour and Merrikh-Bayat [16] in this paper robust watermarking scheme in DWT domain is proposed. For selecting the positions of the embedding watermark bits dynamic blocking scheme is used instead of static one. The change to the blocks with strong edge strength is less visible to human eyes. Then according to binary algorithm watermark is embedded into the significant wavelet coefficients of dynamic blocks with strong edge. The watermark detection process is based on the correlation method. Zhou and Jin have [17] proposed a new robust multi-watermarking scheme in DWT domain. In this approach three independent binary watermarks are embedded in the original image. To embed multi-watermarks simultaneously, the three 2-D watermarks were first recombined into a 3-D watermarking sequence. First the original image is decompose into sub bands using the DWT and then split the approximation sub band into multiple non-overlapping blocks and blocks with best abundant texture information were selected according to the size of binary watermark. The multi-watermark embedded by modifying the fractional part values of selected blocks pixels based on discrete operation rule. The experimental analysis shows that one watermark is robust against common image processing attacks like filtering, noise and JPEG compression and while other two watermarks are immune to any image attacks. Wang et al. [18] introduces a new digital image watermarking algorithm in DWT domain based on texture block and edge detection. By using the masking property of human visual system, texture blocks are extracted after the edge detection using canny operator of the original image. Watermark is embedded into both low frequency and high frequency sub bands in discrete wavelet domain. Watermark is capable of maintaining the effective balance between invisibility and robustness.
C. Robust Watermarking Techniques Using Moments

Xin et al. [19] introduces that due to invariance properties, circularly orthogonal moments, such as Zernike moments and pseudo Zernike moments are very popular. In this paper Multi –bit watermarking scheme is used, watermark bits are embedded into the magnitude of selected ZM/PZM by using quantization approach. The proposed algorithm is robust against various types of geometric attacks such as image scaling, rotation and cropping as well as other attacks such as lossy compression, additive noise and low pass filtering. Singhal et al. [20] in this paper using local Zernike moments a robust image watermarking technique is proposed. To achieve robustness against cropping and other geometric attacks local Zernike moments (LZMs) which are computed over circular patches around feature points and the watermark bits are inserted into it. For scaling attacks the proposed method extracts salient region parameters and transmits to the decoder. At decoder parameters are used to normalized the suspect image and detect the watermark. Watermark is detected at lower error rate after various attacks. Wang [21] in this paper robust image watermarking based on pseudo Zernike moments and image normalization is proposed. Image normalization is apply on the original image and pseudo Zernike moments are computed. Watermarks bits are embedded by quantizing the magnitudes of selected pseudo Zernike moments. This technique is robust against various geometric attacks and common signal processing.

VI. FRAGILE WATERMARKING

A. Fragile Watermarking Techniques in Spatial Domain

Yeung and Mintzer [22] have proposed a fragile watermarking scheme in which all the bits are used for watermark embedding and extraction. This algorithm uses the secret key to generate a unique mapping that randomly assigns a binary value to gray levels of the image. Image integrity is checked by the comparison between decoded binary image and the inserted watermark. This algorithm has high localization accuracy because each pixel is individually watermarked. The technique offers fast image verification to detect and localize unauthorized image alterations but it does not detect changes in image size due to scaling or cropping. Zong et al. [23] have proposed a new fragile watermarking technique which is used for image authentication. A logo is embedded as the watermark for the integrity authentication and tamper detection. In this method a image feature is selected and hashed to generate the chaotic key, which adds uncertainty to each watermark bits. The extracted images feature varies for different images, the watermark bits encrypted by this chaotic sequence are different, and thus collage attack fails. This scheme is especially fit for the application in digital camera. Suthaharan [24] proposed new fragile watermarking algorithm for image authentication and tamper detection. To achieve superior localization with greater security against many attacks including vector quantization attack it uses a gradient image and its structure. The proposed scheme is a block-wise independent scheme like the Wong's scheme but it uses distinct input keys for each image block based on a gradient image and user supplied master key and a session key. Zang and Wang [25] have proposed a novel fragile watermarking scheme capable of perfectly recovering the original image from its tampered version. The watermark data is derived from the entire original content and embedded into the host using a reversible data-hiding technique. Although a malicious modification may destroy part of the embedded watermark, the tampered areas can still be located and the watermark data extracted from the reserved regions can be used to restore the host image without any error. Munir [26] has proposed a fragile watermarking method based on the chaos map for image authentication. Before embedding watermark is encrypted by XOR-ing with a chaotic image which by using logistic map. And then encrypted watermark is embedded using LSB of pixels. For authentication extraction of watermark is done from watermarked image and compared with the original watermark. To check the performance typical attacks like histogram equalization, text addition, image flipping, copy-paste attack in the same image, and copy-paste attack into another watermarked image. This method is able to detect the tempering at pixel level.

B. Fragile Watermarking Techniques in Frequency Domain

1) DCT Domain Techniques: Wu and Liu [27] have proposed a frequency domain technique for image authentication. The watermark is inserted by changing the quantized DCT coefficients before entropy coding. Special lookup table of binary values is used to partition the space of all possible DCT coefficient values into two sets. The two sets are then used to modify the image coefficients to encode a bi-level image (such as a logo). To reduce the blocking effects of altering coefficients the DC coefficient and other lower energy coefficients are not marked. This scheme is to be able to determine whether an image has been altered or not and able to locate any alteration made on the image. Chen et al. [28] in this paper a new digital image authentication and recovery method is described. The original image is divided into smaller blocks. Blocks of image are DCT transformed and then encoded with different patterns. To find the best pattern for each block an optimal selection is adopted which results in better image quality. This method is able to identify and localize the tempered regions.
2) **DWT Domain Techniques**: HongJie et al. [29] have proposed a wavelet-based fragile watermarking scheme for secure image authentication. By using the discrete wavelet transform (DWT) embedded watermark is generated and then the improved security watermark scrambled by scrambling encryption is embedded into the LSB of the image data. The proposed algorithm possesses excellent tamper localization properties, enhances the security against VQ attack and transplantation attack and also evaluate whether the modification made to the image is on the contents or the embedded watermark. Rajawat and Tomar [30] have proposed a new algorithm for digital watermarking and tampering detection technique. In which the RGB component of the input original image is taken and 2-level DWT is applied, which divides the image into low frequency and high frequency components. The same process is done for the watermark which is embedded into the original image. New watermarked image is obtained by multiply the scaling factor with separated components of the input original image and the watermark. The experimental results gave good PSNR value which is reached up to 55 %.

**VII. SEMI-FRAGILE WATERMARKING**

A. **Semi-fragile Watermarking Techniques in Frequency Domain**

1) **DCT Domain Techniques**: Lin et al. [31] have proposed a semi-fragile watermarking scheme for digital images which detect the image alterations. Pseudo-random Gaussian distributed numbers are used as watermark. Watermark is embedded into each block after DCT such that DC value and high frequency AC coefficients are unmarked. The detector was based on spatial domain differences. Experimental results show that proposed method can identify altered regions within a watermarked image with 75 % accuracy under moderate compression and 90 % accuracy under low compression. Ho and Li [32] have proposed new semi-fragile watermarking technique in which watermark is embedded in the quantized DCT domain. This scheme is robust to JPEG compression attack to a pre determined lowest quality factor and fragile to all other malicious attacks either in spatial or frequency domain. Non-deterministic block-wise dependence is obtained using the nine neighbourhood mechanism. Experimental results show the effectiveness of proposed method.

2) **DWT Domain Techniques**: Wang et al. [33] have proposed a novel Semi-fragile watermarking scheme in DWT domain. To generate watermark, content based image features are extracted from approximation sub-band in wavelet domain. Watermark is embedded into the middle frequency sub-band. The extracted watermark is compared with the extracted image feature matrix such that malicious attacks are distinguishable from non malicious tempering. Experimental results show that proposed algorithm is robust to non malicious attacks such as JPEG compression and fragile to malicious attacks. It can also detect the temper location accurately. Qi and Xin [34] have proposed semi-fragile watermarking scheme for content authentication based on quantization. Divide the original image to 4×4 non overlapping blocks. For each block private key based watermark is embedded into the wavelet coefficients of approximation sub-band after 1 level DWT. To ensure the semi-fragile property round operation is used to extract the watermark bits. To check the watermark authentication construct a binary error map and computes two authentication measures \( M_1 \) and \( M_2 \), where \( M_1 \) is measure of overall similarity between embedded and extracted watermarks and \( M_2 \) measure the overall clustering level of the tempered error pixels. Experimental results show that proposed algorithm is capable of localizing tempered regions.

**VIII. PERFORMANCE EVALUATION**

To evaluate the performance of watermarking scheme imperceptibility is one of the significant measures. The good watermarking scheme is one in which the embedded watermark should not provoke any perceptible marks over the original image. To estimate the good quality of watermarked image one should evaluate with the help of Peak signal to noise ratio (PSNR). Higher is the value of PSNR better would be the quality of watermarked image. Bit error rate (BER) and normalized correlation (NC) used to check the robustness of watermarking techniques.

A. **Peak Signal-to-Noise Ratio**

The peak signal-to-noise ratio (PSNR) is defined as the measure of the quality between the original image and attacked image. Mathematically equation of PSNR is given by

\[
PSNR = 10\log_{10}\frac{255 \times 255}{MSE}
\]

where MSE is mean square error and is given by the following equation

\[
MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (f(x, y) - g(x, y))^2
\]

where \( M \) and \( N \) are height and width of image respectively. \( f(x, y) \) and \( g(x, y) \) are the original image and watermarked image at \((x, y)\) coordinates respectively.

B. **Bit Error Rate**

Bit Error Rate (BER) is defined as the ratio of the incorrect number of bits extracted to the total number of bits embedded. BER metrics is used to measure the
Robustness of the watermarking scheme. Robustness of watermark is refers to the ability of watermark to resist various forms of attacks. Mathematically it is given by following equation

\[ BER = \frac{\text{Number of bits extracted inaccurately}}{\text{Total numbers of bits embedded}} \]  

### C. Normalized Correlation

Normalized correlation coefficient (NC) is used to measure the correctness of extracted watermark. In other words it computes the degree of similarity between original image and extracted watermark. It is defined as follow

\[ NC = \frac{1}{W_h \times W_w} \sum_{i=0}^{W_h-1} \sum_{j=0}^{W_w-1} W(i,j) \times W'(i,j) \]  

where \( W_h \) and \( W_w \) are the height and width of the watermark respectively. \( W(i,j) \) and \( W'(i,j) \) are the watermark bits of original watermark and extracted watermark respectively. The value of \( W(i,j) \) is set to 1 if watermark bit is 1 and -1 otherwise. \( W'(i,j) \) is set in similar manner.

### IX. CONCLUSION

Various applications of watermarking like broadcast monitoring, owner identification, authentication, transaction tracking, copy control, device control, legacy enhancements and proof of ownership are discussed. We classify the robust, fragile and semi-fragile watermarking techniques based on different domains in which watermark is embedded. Watermark is embedded into the image in such a way that it difficult to perceive by viewers and the quality of the image is not degraded. Robust watermarks are resistant against various image processing transformations where as the fragile watermarks are very sensitive to malicious and non-malicious attacks. Semi-fragile watermarks are robust to non malicious attacks and fragile to malicious attacks.

### REFERENCES


