Digital Image Watermarking Techniques and Applications: A Survey

Chauhan Usha¹, Singh Rajeev Kumar²

¹ Assistant Professor, JRE Group of Institution, Greater Noida, U.P., India
² Associate Professor, Bhagwant University, Ajmer, Rajasthan, India

Abstract—Digital image watermarking technique is a process of embedding perceptually transparent digital information into an original image. Watermarking can be fragile or non fragile depending upon the user’s requirements. The main concern of digital watermarking is to prove ownership as well as protection of the embedded information. This paper gives brief overview of existing image watermarking techniques, their applications and future prospects of digital watermarking.

Keywords—Image watermarking; Human Auditory System (HAS); Human Visual System (HVS); Quantization; Quantization Index Modulation (QIM); Dither Modulation (DM); Mean Quantization; Vector Quantization;

I. INTRODUCTION

The development and growth of the internet has created new challenges to protect digital data from piracy [35]. Digital watermarking technique provides a superior and robust solution for ownership problem. It becomes much important to maintain the copyright of the digital data which is a form of intellectual properties. Digital watermarking technique embeds copyright information or watermark in to original host image. The embedded information should be imperceptible. These watermarks are difficult to remove by altering or damaging the original host image. The digital image watermarking is a process of embedding watermark in to audio signal to show authenticity and ownership proof. The watermark is permanently embedded in to the digital image and embeddingshould not degrade the quality of digital image. Different categories of information hiding are described in the following diagram.

![Different Categories of Information Hiding](image)

II. REQUIREMENTS OF IMAGE WATERMARKING

To devise an optimal image watermarking system, some design features need to be taken into consideration. Some important features are as follows:

A. Perceptual Transparency

The main requirement of watermarking is perceptual transparency [38]. The watermark which has embedded as the owner’s information should not degrade the quality of the host signal. The watermark cannot be seen by human eye. It can be detected by special processing or dedicated algorithms.

B. Robustness

The embedded watermark should not be removed from the host image even after exploring the watermarked information to different types of attack. Robustness [39] is one of the major design issues for all watermarking applications. The watermark should be robust against various signal processing attacks including D/A & A/D conversion, linear & non linear filtering, compression and geometric transformation [40] of host image.
C. Security
The security of the watermarking system is dependent on the use of private or secret key. The watermarking must be strongly resistant against unauthorized detection. It is also desirable that watermark should resist against an unwanted agent to pirate the information.

D. Data Rate
The number of watermark that is embedded within a host signal is termed as data payload [41]. For audio, data payload refers to the number of watermark bits that may be reliably embedded within a host signal per unit time, usually measured using bits per second (bps).

E. Verification and reliability
Watermark should be able to provide complete & reliable information for proving ownership of copyright products. The watermarking technique should be giving the reliability of recovery of watermark.

III. WATERMARKING PROCESS
Watermarking is the process that embeds watermark in to an image such that watermark can be detected as well as extracted later to make an assertion about the image. The technique consists of two main sub processes:

1. Embedding process
2. Extraction process

Figure 2: Digital Watermarking Embedding process

The embedding block, shown in figure 2 [1] consists of watermark embedding technique, original host signal and secret key as the inputs creates the watermark signal. [1].

Figure 3: Digital Watermarking Extraction process

On the other hand, the inputs for the extraction process is watermarked signal, secret key and sometimes watermark as shown in figure 3 [1].

The watermarking technique that does not use the original image during extraction process is called as “Blind Watermarking”. Blind watermarking is better than non blind watermarking that uses original signal to extract watermark from watermarked signal and secret key are sufficient to find the embedded secret information [2,43].

IV. APPLICATIONS OF WATERMARKING
There are various applications of digital image watermarking. In this section, some application areas for digital watermarking are discussed:
A. Copy Control
Watermark may contain information required by the content owner that decided the policy of copying the digital content. The information contained by the watermark may specify ‘content may not be copied’ or ‘only one copy’ etc. subsequently, the devices used for copying the content may be required by law to contain watermark detector, which follows directives given by the content owner [17],[22].

B. Digital Signatures
Watermarks may be used to identify the owner of the content. By having this information the user may contact the owner for acquiring the legal rights to copy or using the content [15].

C. Authentication
Watermark is used to provide authentication. Providing an incorrect watermarked image can either destroy the watermark or leads to incorrect watermark after extraction.

D. Broadcast Monitoring
Automatic identification of owners of data may be required to be done and used in systems responsible for monitoring the broadcasts. This may help in deciding the royalty payments. It also helps in ensuring that commercials of a particular advertiser are played at right time and for a right duration.

E. Fingerprinting
Watermarks may be used to identify the content buyers. This may help in tracing illegal copies. When a digital media is distributed, it can contain the hidden and imperceptible information about the user, which can be detected by a watermark detector. Thus a licensed copy belonging to a specific user can be ascertained. This also resolves the possible conflicts as regards to the ownership of a digital or intellectual property. This thing is referred to as “Fingerprinting”.

F. Secret communication
The technique of watermarking is also used in transmitting secretly information from source to destination in a hidden way. Several public domain and shareware programs are available which use watermarking for secret communication [18].

Looking at the important applications of watermarking, it becomes very important to enhance the watermarking techniques for providing better “robustness”, “fidelity”, “payload” while preserving the “authenticity” aspect of watermarking.

V. IMAGEWATERMARKINGTECHNIQUES
The watermarking of an image can be done in time domain as well as in frequency domain. The different categories of watermarking techniques are:

5.1 Watermarking Based on Spatial Domain
The most straightforward and fundamental schemes for the fields of digital watermarking are watermarking in the spatial domain. Spatial Domain utilizes the concept of manipulating the pixel intensities of the cover image directly to encode a desired watermark.

At the beginning of the digital watermarking research, while designing the embedding and extraction algorithms, researchers tended to propose schemes to add a pseudo-random noise pattern, or the watermark, to the original image by modifying the luminance values of the pixels in the spatial domain, like the methods in one of the earliest papers with this approach [49],[1].

Spatial watermarks are embedded easily and fast, but they are generally considered fragile [50], [51], [52].

General Embedding Structures in the Spatial Domain:
For spatial-domain watermarking, the watermark is embedded by altering the pixel values slightly in the spatial domain pixels. A typical example is proposed by Pitas [53],[18]. Assuming that the binary bit pattern watermark W to be embedded into the original media X. If the watermark size is smaller than that of the original, it can be replicated until its size is larger than the original. The embedding procedure can be represented by

\[ X'_i = X_i + \alpha_i . W_i \]

Where i represents the positions to be embedded, \( \alpha_i \) denotes the strength factor [54], [55].

By employing the general methods of spatial watermarking, a simple example is presented here to embed a binary watermark with size (128x128) into the original image lena with size (512x512), as shown in the upper part of Figure 4(b) and Figure 4 (a), respectively. On the one hand, the watermark is permuted according to a secret key, key0, to disperse its spatial locations by employing a pseudo-random number traversing method [56]. And the permuted watermark, shown in the lower part of Figure 4(b), looks like random patterns. Spread-spectrum scheme for watermark embedding may also be employed[57],[58].

General Extraction Structures in the Spatial Domain:
Watermark extraction in the spatial domain is a cross-correlation process. To detect a watermark in a possibly watermarked image X', we calculate the correlation between the received image X', which is possibly corrupted or attacked, and the pseudo-random noise pattern W, by [59],[60].
Example of Spatial Domain watermarking
The method described here uses the manipulation of the least significant-bit (LSB) of images, in a manner which is undetectable and imperceptible to the human eyes. The 8-bit gray level original image is first compressed into 7-bit representations, or the LSB’s are discarded directly. Then, the LSB’s of the original image are replaced by the permuted watermark bits. This is demonstrated in [1].

5.2 Watermarking Based on Transform Domain:
Watermarking based on transform domain is mostly encountered in literature. Transform-domain watermarking schemes are generally considered to be robust against attacks. The transform domain techniques convert the spatial digital image into a particular transform domain and then embed the watermarks using that transformation domain coefficients. Among the practical schemes, discrete Cosine transform (DCT)[55] and discrete wavelet transform (DWT)[56],[57] are the most popular transform coding schemes for academic researches and practical implementations. Watermarking related to transform coding schemes is embedded mainly into the perceptually most significant components of the image if the robustness requirement is the main concern for protecting the image content [50].

General Structures for Transform Domain Watermarking:
For transform domain image watermarking, three main steps must be specified: image transformation, watermark casting, and watermark recovery [57]. For different applications and approaches, image transformation can be applied to the whole image [19], or to the block-by-block manner [49]. After that, the transform domain coefficients can be obtained. Watermark casting refers to the selection of the transform-domain coefficients to embed the watermark bits. Algorithms for achieving transform domain watermarking would modify the selected coefficients in the transform domain. The schemes for embedding the watermark in the transform domain is also called the multiplicative embedding rule, which can be denoted by

\[ X'_i = X_i \cdot (1 + \gamma W_i), \]

where \( X' \) and \( X \) stand for the watermarked media and the original counterpart, respectively, \( W \) denotes the watermark, \( i \) represents the positions to be embedded, and \( \gamma \) is the gain factor. For the watermark with length \( L \), \( i \in [0, L - 1] \).

For detection or verification, the receiver needs to verify if a specific watermarking pattern exists or not. A correlation is often used for full extraction of the watermark. The correlation \( R_{X'', W} \) between the possibly attacked image \( X'' \) and the watermark \( W \), can be calculated by

\[ R_{X'', W} = \frac{1}{L} \sum_{i=0}^{L-1} X''_i \cdot W_i. \]

Given a pre-determined threshold \( T \), it can be compared with the correlation in Eq. (2) for deciding the presence of the watermark. Therefore, the decision rule for the presence of the watermark can be expressed by

\[ R_{X'', W} \begin{cases} \geq T \Rightarrow \text{watermark is present} ; \\ < T \Rightarrow \text{watermark is not present}. \end{cases} \]

5.2.1 Discrete Cosine Transform (DCT)
For DCT with block size \((M \times N)\), the connection between the spatial domain image pixels \(X(i,j)\) and the transform domain coefficients \(Y(u,v)\) is

\[ Y(u,v) = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} X(i,j) \cos \left( \frac{2\pi i u}{M} \right) \cos \left( \frac{2\pi j v}{N} \right), \]

where \(u = 0, 1, ..., M-1\) and \(v = 0, 1, ..., N-1\).
where \( u = 0, 1, \ldots, M - 1, \) \( v = 0, 1, \ldots, N - 1, \) and

\[
c(i) = \begin{cases} 
\frac{1}{2^i}, & \text{if } k = 0; \\
1, & \text{otherwise}.
\end{cases}
\]

Researches in DCT-domain watermarking started since 1996 [52]. Watermarking in the DCT domain is popular, because DCT serves as the transform coding module in image. Conventional schemes for embedding the watermark in the DCT domain is to modify the selected coefficients in the blocks [53],[54],[55].

5.2.2 Discrete Wavelet Transform (DWT)

Wavelet techniques provide excellent space and frequency energy compaction, in which energy tends to a cluster spatially in each subband. For DWT, the link between the spatial/temporal domain signal \( s(t) \), and the DWT of \( F(t) \), \( d(k, l) \), is

\[
f(i) = \sum_{k=\infty}^{\infty} \sum_{l=\infty}^{\infty} d(k, l) 2^{-k/2} \psi(2^{-k}i-1)
\]

Where \( \psi(\bullet) \) denotes the mother wavelet. One example of the wavelet function \( \psi(t) \) for the D4 wavelet, is presented in Figure 6.

5.2.3 Spread Spectrum Transform (SS)-Domain Watermarking:

Another well-known transform-domain scheme is the spread spectrum method proposed by Cox [22],[19]. The term “spread spectrum” is used to name this approach because the watermark is spread throughout the spectrum of an image. The marks are added to the significant DCT components not to the lower magnitude components, which are less visible. The authors argue that because the insignificant components can be attacked with little loss in image quality, they are insecure.

Figure 5 shows the basic steps of the embedding process. We first take the transform DCT or DWT of the entire image. Then, select the significant transform components. The zero mean, unit variance Gaussian mark, \( W \), is added to these significant components, \( X \), by the following formula according to the multiplicative embedding rule:

\[
X'(i, j) = X(i, j) (1 + cW(i, j)),
\]

Where \( c \) is a properly chosen value. In their example, the value of \( c \) is 0.1. It is clear that a large \( c \) would distort the marked image quality.

The watermark extracting process is shown in Figure 6. The original image DCT components are needed to retrieve the mark. A correlation can be used to detect the existence of the embedded mark. The standard detection theory can be used to analyze its performance, including error rate, etc. It is reported that this scheme works well under image size scaling, cropping and JPEG compression [22],[19].

5.3 Image Adaptive Transform-Domain Watermarking:

All the previous watermarking schemes do not employ explicitly the human visual model in the marking process. The image adaptive scheme proposed by Podilchuk and Zeng[81],[82] has a specific feature : it uses the human perceptual model and thus is picture-dependent. Its basic operation is similar to that of the Spread Spectrum scheme. However,
instead of performing the entire picture DCT, Podilchuk and Zeng take the block DCT transform and evaluate the Just Noticeable Difference (JND) for each coefficient, \( J(i, j) \), using the Safranek-Johnston model SJM [83], which was originally developed for compression purpose. The zero mean, unit variance white Gaussian mark is added as follows:

\[
X(i, j) = \begin{cases} 
X^r(i, j) + J(i, j)W(j, j), & \text{if } X(i, j) > J(i, j) \\
X^r(i, j), & \text{otherwise.}
\end{cases}
\]

Because the mark is added to the components that are greater than \( J(i, j) \), the number of marked components is picture-dependent. A process similar to the decoding process of the Spread Spectrum scheme is used to extract/detect the mark. It is reported that this scheme can survive strong cropping, scaling and JPEG compression [81].

VI. ATTACKS AGAINST WATERMARKING SCHEMES

In this section we briefly review some common attacks on robust image watermarking system[7]. Any procedure that can decrease the performance of the watermarking scheme may be termed as an “attack”. To achieve the high reliability of watermark detection, the watermark detection process has to be robust to the alterations in the host signal caused from both common signal processing operations and malicious attacks. Depending on the application and watermarking requirements, the list of attacks to be considered includes, but not limited to:

- Additive and multiplicative noise;
- Linear and nonlinear filtering, for example, low-pass filtering;
- Data compression, for example, MPEG image layer 3;
- Quantization of sample values;
- Temporal scaling, for example, stretch by 5%;
- Removal and insertion of samples;
- Averaging multiple watermarked copies of a signal;
- D/A and A/D conversions;

Figure 7[23] shows some common attacks on image watermarking system.

![Figure 7: Classification of different image watermarking attacks](image)

The aim of these attacks is not always to completely remove or destroy the watermark but usually to disable its detection.

VII. CONCLUSION

From the literature and survey of various watermarking techniques based on time domain and transform domain, transform domain techniques contains much robustness, good results of bit error rates and normalized correlation as comparison of time domain based techniques. Mean quantization based techniques has high data pay load than quantization index modulation. Dither modulation and vector quantization are far better techniques than other quantization based techniques in terms of imperceptibility, robustness, reliability, cropping, filtering, etc.

In future, watermark will be equipped with intelligence that can potentially tell the content of an image file, where it originated from, the distribution channel, date distributed, to whom it was distributed (legal customer profile) and possibly the type of media the track was last used on.
REFERENCES

[9] Chen et al./ J Zhejiang “Multipurpose audio watermarking algorithm” Journal of Zhejiang University SCIENCE A ISSN 1673-565X (Print); ISSN 1862-1775 (Online) 2008 9(4):517-523


