Digital Image Watermarking for Copy Right Protection: Survey, Classification and Attacks

Shivanjali Kashyap, Shashi B. Rana*
Department Electronics and Communication Engineering
Guru Nanak Dev University, Regional Campus, Gurdaspur (*Corresponding Author)

Abstract: Digital Image Watermarking is the procedure of embedding message/information/logo into a digital image which may be used to verify its accuracy or the uniqueness of its user. The data is also passed in copy, if the image watermarked is to be copied. Too many Image watermarking methods have to be proposed in digital watermarking. We have study a variety of methods in this paper, the way to express the watermark scheme, and their comparison process. The field of image watermarking can be investigated in this paper. This paper includes a general depiction of the usage of watermarking, when using watermarking the fundamentals for different approaches that can be used.

Keyword: LSB, CBT, DCT, DWT, Attacks

1. INTRODUCTION
Image Watermarking became popular in the 1990s because of the growing of the Internet. A concealed watermark message is to be inserted into a host image such that the hidden message will survive intended or inadvertent attacks. The example of which is to be taken initial of a technology is similar to digital watermarking is a patent filed in 1954 by Emil Hembrooke for identifying piece of melody works. In 1988, Komatsu and Tominaga which appear into sight to be the first persons to use the term digital watermarking [1]. The most important function of the digital watermarks can be providing copyright protection for intellectual property (IP) that's in digital layout. The message/information/symbol where the watermark is to be inserted is known as the host (original) image [2, 3].

Digital image watermarking method provides perceptibility. A watermarking system is of no use to anybody if it distorts the cover or main image to the point of being not any of use, but still highly disrupted. If probable the watermarked imaged should look indistinguishable from the original even on the equipment which has utmost quality. The watermark which be supposed to be ideal also be very much robust, throughout any ordinary use totally resistant to deformation introduced (not intentional attack), or an attempt which may be halt or eliminate the present watermark (premeditated, or malicious attack). Safety measures and inseparability are also two main requirement of ideal watermarking [4, 5]. A robust watermark be attention to reside alive a wide selection of attacks both subsidiary (Means modifications applied with a purpose other than to destroy the watermark) and malicious (attacks designed specifically to remove or weaken the watermark) [6].

a) Imperceptibility (quality): The watermark must not have an effect on the excellence of the host image.
b) Robustness: The watermarked data should be robust adjacent to attacks such filtering with compression, filtering and firmness.
c) Capacity: The extent of the bits which can be put into it at onetime of the original image.

2. PROCESS OF WATERMARKING
Digital image watermarking is similar to watermarking physical substance with the exception of that the watermarking method is used for digital contented instead of physical material. In digital image watermarking a secret message/information/logo is imperceptibly embedded into a different image. The secret logo/information/message is known as watermark and some metadata like protection or information rights about the host image depicts in it. The watermark is inserted in the original image which is referred to as cover or main image since it covers the watermark. The digital watermarking system can be efficiently consists of a watermark embedded and a watermark detector as shown in given below figure 1.1.

![Figure 1.1 Digital Image Watermarking](image_url)

The watermark embedder inserts a watermark onto the cover or main image and the watermark detector detects the presence of watermark information, or
log. For a while a watermark key can also be used during the process of insertion and detection the watermarks. The watermark key has a one to one communication with watermark information/symbol. The watermark key can be a message not public and be known to only authorize parties and it ensures that only authoritative parties can detect the watermark. Additionally, note that the communiqué channel network can be noisy and hostile in the digital image watermarking (i.e., prone to the safety attacks) and so the digital image watermarking techniques should be resilient to both noise and security attacks [7].

3. TYPES OF WATERMARKING
There are a variety of types of watermarking techniques having a different application are given below.

3.1 Inserted Media Category: Watermarking techniques can be classified on the basis of whether they are used for Text, Audio, Image, and Video.

3.2 Robust & Fragile Watermarking:
Robust watermarking is a method in which watermark will not affect when the watermarked content is modified whereas fragile watermarking is a method in which watermark gets ruined when watermarked content is modified or tampered with.

3.3 Visible & Transparent Watermarking:
Visible watermarking: Visible watermarks are ones, which are inserted in the visual content in such a way that they are visible when the content is to be seen. Transparent watermarks are unnoticeable and they cannot be detected by just viewing the digital content.

3.4 Public & Private Watermarking:
In public watermarking, users are to be known to detect the watermark while in private watermarking the users are not authorized to detect the watermark.

3.5 Asymmetric & Symmetric Watermarking:
Asymmetric is a technique where different keys are used for embedding (insertion) and detecting (extraction) the watermark. In symmetric watermarking the same keys are used for embedding and detecting watermarks.

3.6 Steganographic & Non-Steganographic watermarking:
Steganographic watermarking is the method where contented users are unacquainted of the presence of a watermark, whereas in non-steganographic watermarking is the technique where content users are aware of the presence of a watermark. Steganographic watermarking technique is mainly used in fingerprinting applications while non steganographic watermarking techniques can be used to detect piracy.

4. WATERMARKING ATTACKS
A robust watermark should survive a wide variety of attacks both incidental (modifications applied with a purpose other than to destroy the watermark) and malicious (designed to remove or weaken the watermark) [6, 8]. We classified the watermarking attacks as:

4.1 Simple attacks:
Simple or waveform or noise attacks are conceptually simple attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked data (host data plus watermark) without an attempt to identify and isolate the watermark. Examples which include like compression (JPEG, MPEG), filtering, addition of noise, addition of an offset, cropping, (A/D) analog to digital conversion, and (D/A) digital to analog conversion.

4.2 Detection-disabling attacks:
Synchronization or Detection-disabling attacks are attacks that attempt to break the correlation and to make the recovery of the watermark impossible or infeasible for a detector watermark, mostly by the geometric distortion like a shift in (for video) direction, rotation, cropping, zooming, pixel permutations, sub band sampling, insertion or elimination of pixels or pixel clusters, or any other geometric transformation of the data.

4.3 Ambiguity attacks:
Ambiguity or deadlock attacks are attacks that attempt to confuse by producing fake original data or fake watermarked data. An example of an inversion attack that attempts to discredit the authority of the watermark by embedding one or several additional watermarks such that it is unclear authoritative which the first watermark was.

4.4 Removal attacks:
Removal attacks are attacks that attempt to analyze the watermarked information, which approximate the watermark or the original data. Removal attacks separated the watermarked data into original information and watermark, and the watermark is only rejected. For examples are like denoising, conspiracy attacks, certain filter operations, or determination attacks using synthetic modeling of the image.

5. CLASSIFICATION OF DIGITAL IMAGE WATERMARKING TECHNIQUES
A variety of techniques can be used to hidden message/logo/information in images and are classified as

5.1 Least Significant Bit Modification
The simpler method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object [9]. LSB substitution though has a lot of limitation present in it. The watermark accumulation by some of lossy compression or noise is likely to be prevailing over. If we simply set the LSB bits of each pixel to one the watermark obsolete with negligible impact on the cover object. A fundamental enhancement on LSB substitution would be to use a pseudo-random number generator to determine the
pixels to be used for embedding based on a given “seed” or key [9].

Precautions of the watermark would be enhanced as the watermark could no longer be easily viewed by intermediate unknown parties. The algorithm however would be still in risk to replacing the LSB’s with a constant.

**5.2 Correlation-Based Techniques**

Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise (PN) patterns as functional to an image. A pseudo-random noise sequence (PN) pattern watermark \( W(x, y) \) is to be added to the cover image which is \( I(x, y) \), which is given below in equation 1.1.

\[
I_w(x, y) = I(x, y) + k * W(x, y) \quad \ldots \ldots \cdot 1.1
\]

\( K \) denotes a gain factor value, and \( (I_w) \) is the resultant watermarked image. When the value of \( k \) rises then the roughness of the watermark is also increasing at the expense of the quality of the watermarked image.

The watermark is to be retrieve, the same pseudo-random noise generator algorithm is seeded then the same key and then the correlation of the noise pattern and possibly computed watermarked image. If the correlation exceeds a definite value of threshold \( T \), then the watermark is detected and a single bit is to be set. Correlation-based method can be modestly comprehensive to a multiple-bit watermark by the image dividing up into blocks, and each single block is performing the above process autonomously. A number of ways this fundamental algorithm can be improved. First, the threshold notion can being used for determining a logical “1” or “0” can be eliminated by means of two dissimilar part of pseudo-random noise patterns. One sample is selected a logical “1” and the other a “0”.

The above course of action is then performed once for each pattern and the higher resulting correlation pattern is to be used. This method raises the probability of an accurate detection, still after the image has been issue to the attack. Then this type of scheme can be advances further by pre-filtering the image before applying watermark. If we can be decreasing the correlation between the PN sequence and the cover image, we can raise the resistance of the watermark to the noise. The edge enhancement filter by applying it given in equation 1.2 given below, the stiffness of the watermark can be improved with no loss of capacity and very little reduction of image quality.

\[
F_{edge} = \frac{1}{2} \begin{bmatrix} -1 & -1 & -1 \\ 1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix} \ldots \ldots \cdot 1.2
\]

**5.3 Frequency Domain Techniques**

Here we can insert the watermark in DCT, DFT, and FFT transform domains technique etc. The main potency offered by transform domain techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features. The toughness and quality both of the watermark could be improved if the properties of the cover image could correspondingly be exploited. It is regularly preferable for the case to hide watermarking information at corner of the images, noisy regions, but not in an uncomplicated region. The benefit is two-fold; deformation in smoother regions of an image is more perceptible to the HVS and becomes a prime aim for lossy compression method.

Taking these aspects into consideration, whose transform domain technique working in some sort becomes very attractive. The mainly popular domain system for image processing is that of the Discrete Cosine Transform (DCT). The Discrete cosine transform (DCT) allows an image to be broken up into different frequency bands coefficients, which manufacture it much easier to initiate the watermarking information into an image in the middle frequency bands. The middle frequency bands are selected such that they have minimize they evade the most visual significant parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a discrete cosine transform (DCT) block. The middle band frequencies (\( F_m \)) of an 8x8 DCT block can be define here as shown below in figure 1.2.

\( F_L \) is used to indicate the lowest frequency band components of the block, while \( F_H \) is used to signify the higher frequency components. \( F_M \) is taken as the embedding region so as to provide additional resistance to lossy compression methods, while considerable modification is to be overcome of the cover image [10].
Next two DCT Bₖ (u₁, v₁) as well as DCT Bᵢ (u₂, v₂) position of the Fₘ segment is taken out comparison. These locations are by chance choosing rather than, extra robustness to compression can be achieved if we base the choice of coefficients on the recommended JPEG quantization table shown below in table 1. If two locations are to be chosen such that they have identical quantization illogical values, we can think with assurance that any scaling of one coefficient will scale the other by the same factor…preserving their comparative size. Based on the table, we can detect that coefficients (4, 1) along with (3, 2) or (1, 2) along with (3, 0) would make appropriate candidates for taken out comparison, as their random quantization standards are to be identical. The DCT block will be encode (0) if Bᵢ (u₁, v₁) < Bᵢ (u₂, v₂), or else it will encode a (1).

The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded. The substitute of such transform coefficients should not alter the watermark image significantly, as it is generally believed that discrete cosine transform coefficients of middle frequencies have magnitudes similar. The watermark robustness can be improved by introducing a watermark strength constant k, such that Bᵢ (u₁, v₁) - Bᵢ (u₂, v₂) > k. Coefficients transform is such that in which this criteria cannot be meet are modified though the use of random noise as to then satisfy the relationship. By increasing the value of gain factor thus which decreases the chance of detection errors at the expense of additional image degradation quality [10]. Another achievable technique is to insert a PN sequence W into the middle frequencies of the DCT block. We can modulate a given DCT block (x, y) using equation 1.3 given below:

\[
I_{W,x,y}(u,v) = \begin{cases} 
I_{x,y}(u,v) + k \times W_{x,y}(u,v), & u,v \in F_{M} \\
I_{x,y}(u,v), & u,v \notin F_{M}
\end{cases}
\]

For each 8x8 block x, y of the image, the block of the DCT is first calculated. In that block, the middle frequency components Fₓ are added to the pseudo random sequence W, which multiplied by a gain factor k. Coefficients in the low frequencies and middle frequencies are copied over to the transformed image which is unaltered. Each one block of the image is at that moment conversely transformed to give us our final watermarked image (Iₓ). The watermarking procedure can be made somewhat more adaptive by slightly altering the embedding process to the method as given in equation 1.4.

\[
I_{W,x,y}(u,v) = \begin{cases} 
I_{x,y}(u,v) + (1+k \times W_{x,y}(u,v)), & u,v \in F_{M} \\
I_{x,y}(u,v), & u,v \notin F_{M}
\end{cases}
\]

This slight modification scales the strength of the watermarking based on the size of the particular transform coefficients are being used. Larger k’s value is thus used for transform coefficients of higher magnitude in consequence increase the watermark in regions that can afford it; deteriorating it in those that cannot. The image is broken up into those same 8x8 blocks for the purpose of detection, and a DCT performed. The same (PN) sequence is to be then compared to the middle frequency values of the transformed coefficient block. If the correlation among the sequences 1 is to be detected then that block exceeds some threshold T; 0 is to be detected otherwise here. Once more the effectiveness of the watermarking is denoting with k, where increases the
robustness by rising the value \( k \) of the watermark at the expense of quality.

5.4 Wavelet Watermarking Techniques

Another possible domain for embedding watermark is that of the wavelet domain transform. The Discrete Wavelet Transform (DWT) method divide an image into a lower resolution estimate image (LL) as well as horizontal resolution (HL), vertical resolution (LH), as well as diagonal resolution (HH) sub-band detail of components. It is an easy to apply and can efficiently decreases the computation time. The process can then be repetitive to computes various “scale” wavelet component decomposition, as in the 2 scale wavelet composition transform shown below in figure 1.3.

Many advantages over the wavelet transform is that it is believed to more accurately model aspects of the human visual system (HVS) as compared to the fast Fourier transform (FFT) or Discrete cosine transform (DCT). This allows user to use high energy watermarks in regions that the HVS is known to be less prone to, such as the aspect of the bands by high resolution band like

![Wavelet Transform Diagram](image)

(LH, HL, and HH). Watermarks embedding in these regions permit us to enhance the robustness of the watermark, no additional impact on the image quality. One of the easiest methods is to use a similar embedding technique to which used in the DCT, the inserting of a sequence of CDMA in the detail bands according to the given below in equation 1.5.

\[
I_{W_{u,v}} = \begin{cases} 
W_i + \alpha |W_i|x_i, & u, v \in HL, LH \\
W_i & u, v \in LL, HH 
\end{cases}
\]

\[\text{Figure 1.3: 2 Scale 2-Dimensional Discrete Wavelet Transform}\]

Where \( W_i \) denotes the transformed coefficient of image, the \( x_i \) is the bit of the watermark to be embedded, moreover \( \alpha \) a scaling factor. The watermark to be detected we generate the same pseudo-random sequence used in CDMA generation and determine its correlation with the two transformed detail of transform coefficient bands. If the correlation exceeds some threshold \( T \), the watermark is to be detected.

This can be easily extended to multiple bit messages by embedding multiple watermarks into the digital image. In the spatial domain version, a separate seed is used for each pseudo-random sequence (PN) which is then added to the detail transform coefficients as given equation 1.5 given above. If the correlation exceeds \( T \) for an exacting sequence a “1” is recovered; and a zero otherwise during detection. The procedure of recovery subsequently iterates throughout the entire PN sequence until all the bits of the watermark have been improved. Furthermore, as the insertion uses the standards of the transformed value in embedded, the process of embedding should be somewhat adaptive, the majority of the watermark storing in the larger coefficients. The author [11] should claims that the method should prove opposed to scaling, JPEG firmness, cropping, rotary and a different typical attack.

6. CONCLUSION

We survey and review number of techniques for the watermarking of digital images, and compares their potential and restrictions. We provide the concise interpretation of digital image watermarking and it was still enough to draw several conclusions about digital watermarking. LSB substitution is the simplest method in the LSB substitution but not a very good candidate for digital watermarking due to its lack of strength. The watermarks implanted in the LSB method can be detached easily or altered without degrade the quality of image. It appears that LSB would be left behind in watermarking due to its tremendous information capacity. Most of the distortion-based watermarking techniques mainly aim at protecting the ownership, where distortion-free watermarking techniques mostly are fragile and aim at maintaining integrity.

ACKNOWLEDGMENT

The author wants to thanks to guides who help in study about all these related things.

REFERENCES


www.ijsret.org
Natural and Applied Sciences, The Middle East Technical University, pp 2–8, Sep 2002.


