# DIGITAL IMAGE WATERMARKING FOR COPYRIGHT PROTECTION

*Nandhini S*
*Assistant Professor Mr.R.Ambikapathy.,M.C.A.,M.Phil.,*
*Department of MCA,*
*Krishnasamy College Of Engineering and Technology,*
*Cuddalore*

**Abstract**

Digital Watermarking is the process of embedding data called watermark or signature or label or tag into a multimedia object (image or audio or video) so that the watermark can be extracted for ownership verification or authentication. In image watermarking, the hidden information is embedded into cover media to prove ownership. The secret key encryption algorithm is used for embedding the watermark using LSB technique. Copyright abuse is the motivating factor in developing new encryption technologies. One such technology is digital watermarking. The focus of this proposed research work will give emphasis on detail digital image watermarking techniques and its applications in various fields. Areas that will be covered are definition of digital watermarking, purpose, techniques, and types of watermarking attacks and its applications in digital image processing.

KEYWORDS-Digital Watermarking, Secret key, Encryption, Decryption, Least Significant Bit

## 1.INTRODUCTION

Digital watermark was first discovering in 1992 by Andrew Tirkel and Charles Osborne. Watermark is derived from the german term “Wessmark. The first watermarks devolved in Italy during the 13th century, but their use apace spread across Europe. Watermarking can be measured as special techniques of Steganography where one message is embedded in another and the two messages are related to each other Digital Watermarking is the process of embedding data called watermark or signature or label or tag into a multimedia object (image or audio or video) so that the watermark can be extracted for ownership verification or authentication. During the last years, the world is rapidly becoming digital in many aspects. Among the most interesting of these aspects is multimedia. Many new technologies have come into our lives along with multimedia and one of the most recent is watermarking. Digital technology has offered users easy ways to create, process, and distribute digital assets. This technology is becoming important due to the popularity of usages of images on web. Digital signature is also a verification scheme that is used for verifying the reliability and authenticity of the image content. In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security. A digital signature can be either an encrypted or a signed hash value of image contents and image characteristics. In Visible watermarking watermark appears visible to

a casual viewer on a careful inspection. The invisible-robust watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark.

## 2. Proposed System

The proposed watermarking system could be described by the block diagram .The watermark embedding unit and watermark security unit form two important sub-systems of the proposed system. The watermark security unit is aimed at improving the security watermark so as to make it impossible for an adversary to get the exact watermark even if it has the knowledge of embedding algorithm. Chaotic theory and Arnold encryption have been used to achieve a better security. The mathematical preliminaries of Chaos and Arnold encryption are presented
in the following sub-section.

## 3. WATERMARK:

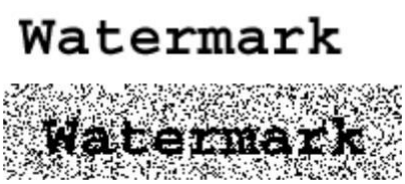
A **watermark** is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light or when viewed by reflected light, at a darkbackground, caused by thickness or density variations in the paper. Encoding an identifying code into digitized music, video, image or other file is known as a digital watermark. Digital watermarking technique is thus implementing the concept of watermarking in digital media

### 3.1 WATERMARKING AND CRYPTOGRAPHY

Watermarking and cryptography are nearly related techniques but watermarking is discrete from encryption. In the digital watermarking system, it is containing information carrying the water is embedded in an original image. The watermarked image is transmitted or stored and then decoded to be determined by the receiver. Cryptography scrambles the image so that it cannot be implicit. In Figure 1 explain the principal of cryptograph, in which plain text encrypted in to cipher text which is then decrypted into plain text. The objective of watermarking is not to limited access to the original image, but to ensure that embedded data remain recoverable the input to the watermarking algorithm is the image which is to be watermarked and is encrypted by public or secret key which will produce watermarked image.

### 3.2 Digital Image Watermarking Techniques

The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification. Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, color correction, or geometric modifications. Security means the embedded watermark cannot be removed beyond reliable detection by targeted attacks. Imperceptibility means the watermark is not seen by the human visual system. Complexity is described as the effort and time required for watermark embedding and retrieval. Lastly, verification is a procedure whereby there is a private key or public key function (Dittmann, Mukherjee, & Steinebach, 2000). Each of these properties must be taken into consideration when applying a certain digital watermarking technique. The following sections describe a few of the most common digital watermarking techniques.




## 4. Applications Of Digital Watermarking

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Annotation of digital photographs with descriptive information is another application of invisible watermarking. Digital watermarking may be used for a wide range of applications, such as:

**Copyright 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.

**Broadcast Monitoring:**

This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

**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.

## 5. Characteristics of Digital watermarking

There are a number of important characteristics that watermark can exhibit, Jalil and Mirza (2010), Bandyopadhyay and Paul (2010). The main characteristics of digital watermarking are classified into major categories as follows.

- **Robustness**: The watermark should be capable to resist after normal image processing operations such as image cropping, transformation, compression etc.
- **Imperceptibility**: The watermarked image should appear like same as the original image to the ordinary eye. The observer cannot detect that watermark is embedded in it.
- **Security**: An unauthorized someone cannot detect, retrieve or change the embedded watermark characteristics of digital watermarking
- **Transparency**: Transparency relates to the properties of the human sensory. A transparent watermark causes no artifacts or feature loss.
- **Capacity**: Capacity describes how many information bits can be fixed. It addresses also the possibility of embedding multiple watermarks in one document in parallel. Capacity requirement always effort against two other important requirements, that is, imperceptibility and robustness. A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.

## 6. Attacks on Digital Watermarking

There are various possible malicious intentional or unintentional attacks that a watermarked matter. The accessibility of wide range of image processing soft ware's made it possible to achieve attacks on the robustness of the watermarking systems. The aim of these attacks is foil the watermark from performing its intended

purpose. A brief introduction to various types of watermarking attacks is follows.

• **Removal Attack**: In this attacks mean to remove the watermark data from the watermarked object .

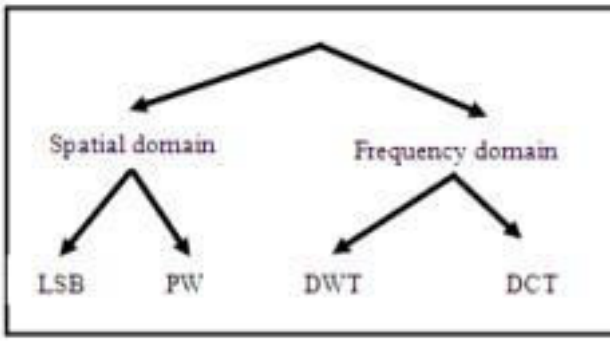
•**Geometric attack**: All manipulations that distress the geometry of the image such as flipping, rotation, cropping, etc. should be detectable [11].

• **Protocol Attack**: In this attacks do neither mean at destroying the embedded information nor at disabling the detection of the embedded information

•**Cryptographic attacks**: It is deal with the brilliant of the security.

## 7. Classification of Watermarking Techniques

Watermarking is the method of hiding the secret information into the digital media using some strong and suitable algorithm. Algorithm plays an essential role in watermarking as, if the used watermarking technique is capable and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information. There are some various algorithms are used to hide the information.




**Spatial domain:** Algorithms directly load the raw data into the original image [2]. Spatial watermarking can also be applied using colour separation. In this way, the watermark appears in only one of the colour bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing.

**Least Significant Bit:** Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks . LSB is very sensitive to noise and common signal processing and cannot be used in practical applications.

**Patchwork Algorithm:** Patchwork is a data hiding technique developed by Bender et al. and published on IBM Systems Journals. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution .

**Frequency domain:** Compared to spatial-domain methods, frequency domain methods are more commonly applied. The aim is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain, that is the characteristics of the human visual system (HVS) are better captured by the spectralcoefficients.

**Discrete cosine transforms (DCT):** DCT represents data in conditions of frequency space relatively than an amplitude space. It is useful, because that corresponds more to the way humans observe light, so the part are not supposed can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc.

However, they are difficult to implement and are computationally more costly.

**Discrete wavelet transforms (DWT):** Wavelet Transform is a recent technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal

### *8. Watermark Embedding Algorithm*

The watermark embedding process is stated in the following algorithm-

(1) Consider an image X in which the watermark to be inserted and M be a message (owners information's).

(2) Let H (.) be a cryptographic function such as MD5or SHA-1 [2]. The Message digest is computed as-

H(M)=(P1,P2,P3……Ps)

Where Pi denote the output bits of hash function and s is the size of the hash value that depends upon the type of the hash function such as s=128 for MD5 and s=160 bits for SHA-1.

**(3)** The Image hash is computed as-

(a) First the Binary image B is crated from the original image X.

(b)Then Image hash is computed using hash function such as MD5 or SHA-1 i.e. I = H(X)

**(4)** Then watermark W is generated by encrypting message digest Ps using symmetric key cryptosystem as:

W= EK (Ps )

Where E(.) is an encryption function of the symmetric key system and K is the secrete key.

(5) Embed the watermark bits and Image hash into LSB of original Image X.

(6) Finally obtain the watermark image Xw

### 8.1Watermark Extraction Algorithm

The watermark extracting process is stated in the following algorithm-

(1) Extract encrypted Message digest and Image hash from LSB of watermark Image Xw.

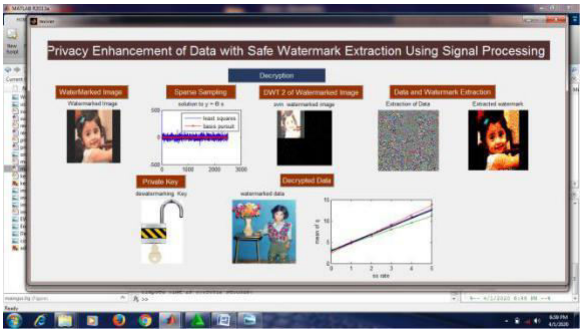
(2) Obtain the hash value using symmetric key algorithm

P's = DK(W')

Where D(.) is an decryption function and K is the owners secrete key.

(3) Compare P's with recomputed hash value of message to prove the ownership of the image.

(4) Similarly the Image hash is recomputed and compare for temper detection.

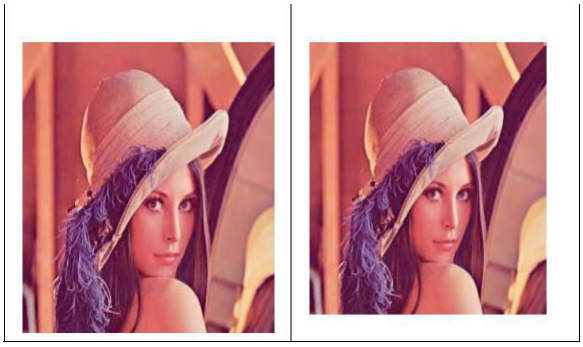



## 9. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed idea is implemented using Java development kit (JDK1.6). The cryptographic primitives are implemented using JCA. JCA provide a set of classes for the implementation of cryptographic function such as encryption, decryption and hash. The original image is being watermarked using this proposed scheme

The proposed algorithm is tested for different payloads. The quality of the watermark image against the embedding payload is tested in terms of three parameters: Histograms, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Larger is the PSNR better is the

quality of image and smaller is the MSE better is quality of image. If we look the histograms of watermark images with payload 2kb, 5kb, 10kb and 14kb (as shown in fig. 5 to 9) and histogram of original image, we find that both are almost same. The experimental results with respect to Peak Signal to Noise Ratio and Mean Square Error are shown in table1. It is clear from the results that the PSNR value is greater than the acceptable values i.e. 30dB and MSE values are also in acceptable range.



a.original image b.watermark image

## 10. Conclusion

The Digital Watermarking technology is becoming important due to the popularity of usages of images on web. In invisible watermarking technique the watermark is embedded in such a way that the modifications made to the pixel value is perceptually not noticed and it can be recovered only with an appropriate decoding mechanism. This paper presented invisible watermarking scheme for copyright protection of images. The watermark is generated by
encrypting the message digest using symmetric key algorithm. Then the generated watermark along with the image hash is embedded into LSB of original image. The verification process uses the same key as in encryption and hence it can be used for the copyright protection of the images. During the verification process the received hash is compared with the recomputed hash to prove the ownership. Similarly the image hash is compared with the recomputed image hash for detecting any modifications made in the image pixels. This technique provides high capacity and minimum computations. Further we can improve this method by embedding the watermark into DCT coefficients.

## References:

1] Mohanty, Ramakrishnan “A Dual Watermarking Technique for Images “http://citeseer.ist.psu.edu/mohanty99dual.html
[2] R. L. Rivest, “The MD5 message digest algorithm." Internet RFC 1321, April 1992.
[3] R.L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, vol. 21, pp. 120{126, February 1978.
[4] W. Diffie and M. E. Hellman, “New directions in cryptography," IEEE Transactions on Information Theory, vol. 67, pp. 644{654, November 1976.