*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834,p- ISSN: 2278-8735. Volume 8, Issue 1 (Sep. - Oct. 2013), PP 07-11*
*www.iosrjournals.org*

# Digital Image Watermarking Basics

Senthil Nathan.M[1] , Pandiarajan.K[2] , Baegan.U[3]
[1,2 & 3]*Student, III year Electronics & Communication,Karpagam College of Engineering,Coimbatore,India.*

***Abstract:*** *The increasing amount of applications using digital multimedia technologies has accentuated the need to provide copyright protection to multimedia data. This paper reviews one of the data hiding techniques - digital image watermarking. Through this paper we will explore some basic concepts of digital image watermarking techniques.Two different methods of digital image watermarking namely spatial domain watermarking and transform domain watermarking are briefly discussed in this paper. Furthermore, two different algorithms for a digital image watermarking have also been discussed. Also the comparision between the different algorithms,tests performed for the robustness and the applications of the digital image watermarking have also been discussed.*

## I . Introduction

There are three basic methods of secure communication available, namely, cryptography, steganography and watermarking [1]. Among these three, the first one,cryptography, deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange that deals with the content confidentiality and access control. By using cryptography, only authorized parties holding decryption keys can access the content (text or image). It provides the tools to secure sensitive information. Steganography, on the other hand, is a technique for hiding and extracting information to be conveyed using a carrier signal.

A watermarking system must allow for a useful amount of information to be embedded into the image. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content.

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 operations such as filtering, lossy compression,color correction, or geometric modifications. Security means that the embedded watermark can't be removed beyond reliable detection by targeted attacks. Imperceptibility means that 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 is used as a private key or public key function. Each of these properties must be taken into consideration when applying a certain digital watermarking technique [2]. Watermarking techniques can be classified according to the nature of data (text, image, audio or video), or according to the working (spatial or frequency) domain, also they can be classified according to the human perception (robust or fragile) [3]. In images, the watermarking techniques can be broadly classified into three types: (i) Visible watermark, (ii) Invisible fragile watermark and (iii) Invisible robust watermark [2], [3], which has wider currency and use. However all these mentioned classes can be applied by using software, hardware or both together. Fig. 1 illustrates a generic watermarking scheme.there are two watermarking techniques using software namely spatial domain and transform domain.

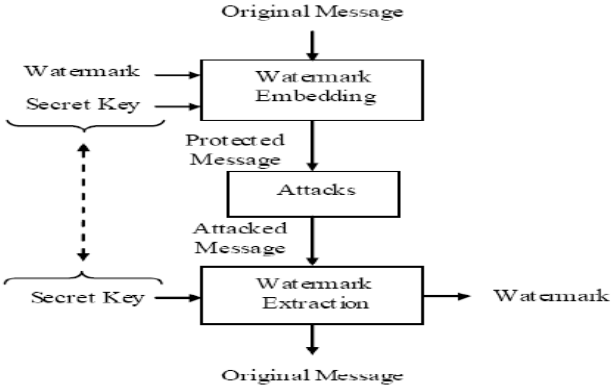


Fig .1. Generic watermarking scheme [14]

## II . Spatial Domain

An analogue image can be described as a continuous function over a two-dimensional surface. The value of this function at a specific coordinate on the lattice specifies the luminance or brightness of the image at that location. A digital image version of this analogue image contains the sampled values of the function at discrete locations or pixels. These values are said to be the representation of the image in the spatial domain or often referred to as the pixel domain. Spatial embedding inserts message into image pixels. The oldest and the most common used method in this category is the insertion of the watermark into the least significant bits (LSB) of pixel data [4][5][6].

In [7] they have implemented a simplest model of watermark technique. It has the ability to insert an invisible watermark into a spatial domain of a base-image. This technique yields marked-images with high imperceptibility and robustness quality. The algorithm provides high level of security by generating encryption key which is used to extract the watermark later; also, the algorithm is able to randomize the location of the watermark in different base-images.

## III . Transform Domain

Transform domain embeds a message by modifying the transform coefficients of the cover message as opposed to the pixel values. Ideally, transform domain has the effect in the spatial domain of apportioning the hidden information through different order bits in a manner that is robust. There are a number of transforms that can be applied to digital images, but there are notably three most commonly used in image watermarking. They are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

### A . DISCRETE FOURIER TRANSFORM

Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete valued function requires the Discrete Fourier Transform (DFT). In digital image processing, the even functions that are not periodic can be expressed as the integral of sine and/or cosine multiplied by a weighing function. This weighing function makes up the coefficients of the Fourier Transform of the signal. Fourier Transform allows analysis and processing of the signal in its frequency domain by means of analyzing and modifying these coefficients.

Pereira proposed a method for copyright protection by embedding a digital watermark in the DFT domain [8]. The properties of this technique based on polar maps for the accurate and efficient recovery of the template in an image which has undergone a general affine transform. In this technique, the watermark is composed of 2 parts: one is a template which contains no information in itself but can detect any transformations undergone by the image, and another one is a spread spectrum message that contains the hidden information. The length of the hidden information is supposed to be short and it is subjected to a preprocessing algorithm to produce the new message of length. Prior to embedding the hidden message, the luminance component of the cover image is extracted and is used to calculate the DFT coefficients. The hidden data and the template are then embedded in these coefficients. The template is embedded along 2 lines in the cover image which go through the origin and its purpose is to detect any attacks (transformation) the image has undergone

### B . DISCRETE COSINE TRANSFORM

Discrete Cosine Transformation (DCT) transforms a signal from the spatial into the frequency domain by using the cosine waveform. DCT divide the information energy in the bands with low frequency and DCT popularity in data compression techniques such as JPEG and MPEG.The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of the image. Here the middle frequency bands chosen such that they minimize to avoid the visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). FL is use to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is Chosen as the embedding region as to provide additional resistance to lossy compression techniques [9].

Chandra have proposed a robust watermarking method using MDKP [10].it has greatest robustness against various attacks and preserves the image quality after water marking. It embeds a watermark into an image in DCT domain. The image is divided into blocks and each block is processed using Multi Dimensional Knapsack Problem (MDKP) and in turn converts to spatial domain. The watermark is extracted from the image and compared with the original image. The measurement of quality of image is also concerned. this scheme exhibits better performance in robust digital watermarking.

**C . DISCRETE WAVELET TRANSFORM**

Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error. Since the bandwidth of the resulting coefficient sets is smaller than that of the original image, the coefficient sets can be down sampled without loss of information. Reconstruction of the original signal is accomplished by up sampling, filtering and summing the individual sub bands. The basic idea of discrete wavelet transform(DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district [11][12]. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two-dismensional image after three-times DWT decomposed can be shown as Fig.2. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, HH1. The low-frequency district information also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for *n* level wavelet transformation. The informaton of low frequency district is a image close to the original image. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image.

In [13] Shivani Garg proposed a new model for the DWT method of watermarking. The Proposed method decomposes cover image (original image), which is to be watermarked using DWT. The watermark is embedded to the specified DWT coefficient of the cover image. A new DWT based spread spectrum watermarking technique is proposed on the basis of embedding of various sequences in the DWT coefficients. The algorithm is Column wise DWT Coefficients Embedding Algorithm (CCE). In this method columns of DWT coefficients are taken for watermarking. The proposed algorithm is experimented on different sequences. Performance of the algorithm is analyzed by varying the gain factor and by inserting different sequences. Simulation results show that the proposed method achieves higher security and robustness especially in the case of Kasami sequence.

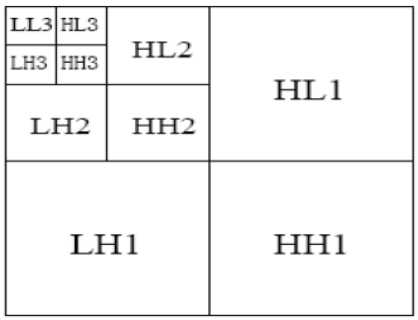


Fig . 2 sketch map of image DWT decomposed

## IV . Watermarking Algorithms

**A . SPATIAL DOMAIN ALGORITHM**

**Embedding algorithm** [14]

1) Reorganize size of the base-image to be [M × M].
2) Reset the contents of the LSB plane in the baseimage.
3) Reorganize color and size of the watermark to be [N × N] gray image.
4) Extract the all bit plane details from the watermark.
5) Shift the extracted values to right.
6) Add the shifted bit plane of the watermark into the LSB plane of the base-image.
7) Repeat steps (4th, 5th and 6th) m-times.
8) Finally, result is a watermarked-image.

Note that: watermarks' size should not exceed baseimages' size, e.g. *([N × N] = [M × M] / m)*.

**Extraction algorithm**

1) Extract the LSB bit plane from the marked image.
2) Shift the extracted contents by left.
3) Repeat 1st and 2nd steps, (m) times.

4) Result is watermark retrieved.

**B . FREQUENCY DOMAIN ALGORITHM**

**Embedding algorithm** [14]

1) Reorganize color and size of the base-image to be [M ×M] gray color.
2) Compute 2D wavelet transform for the base-image.
3) Initiate the weight of the watermarking.
4) Reorganize size and color of the watermark to be [M ×M] gray image.
5) Divide the transformed base-image into 4-blocks, namely, *LL, LH, HL and HH* respectively.
6) Multiply watermark by watermarking weight and then add the result to the blocks of the base-image.
7) The inverse wavelet transform is then taken to get the watermarked-image.

**Extraction algorithm**

On the other hand the extraction algorithm can be done by taking the forward wavelet transform of the watermarked image and then subtracted it from the base-image to get the watermark.

## V. Watermarking Robustness Test

Many different methods can be used to test whether a watermark can survive different changes to the image it is
embedded in. Here is a browsing of the popular of these methods [3]:

1) Horizontal Flipping**:** Many images can be flipped horizontally without losing quality. Few watermarks survive flipping, although resilience to flipping is easy to implement.

2) Rotation & Cropping: A small rotation with cropping doesn't reduce image quality, but can make watermarks undetectable as rotation realigns horizontal features of an image used to check for the presence of a watermark.

3) JPEG Compression/Re-compression: JPEG is a widely used compression algorithms for images and any watermarking system should be resilient to some degree to compression or change of compression level.

4) Scaling: Uniform scaling can increase/decrease an image by the same (%) rate in the horizontal and vertical directions. Non-uniform scaling can increase/decrease the image horizontally and vertically at different (%) rates. Digital watermarking methods can be resilient only to uniform scaling.

5) Dithering: It approximates colors by alternating two available similar colors from pixel to pixel. If done correctly this method can completely obliterate a watermark, however it can make an image appear to be "patchy" when the image is over-dithered.

6) Mosaic: A mosaic attack doesn't damage the watermarked-image or make it lose quality in any way, but still enables the image to be viewed in. To the viewer a "mosaic" image appears to look the same as the original. This means that the watermark cannot be detected, as a problem common to all image watermarking schemes is that they have trouble embedding watermarks into small images, (less than 256 pixels in height or width).

## VI . Comparision

**Advantages of DWT over DCT**:

Wavelet transform understands the HVS more closely than the DCT.

Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution [15].

**Disadvantages of DWT over DCT:**

Computational complexity of DWT is more compared to DCT'. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient.

**Advantages of DFT over DWT and DCT:**

DFT is rotation,scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions [15].

## VII . Digital Watermarking Applications

Digital image watermarking have a wide range of applications in the field of digital multimedia.The following are some of the applications of digital image watermarking [16].

**A . Copyright protection**: The most important application of watermarking is to provide copyright protection. Copyright protection requires high level of robustness so that the embedded watermark can not be removed without data distortion This watermark is extracted to show as proof if someone claims the ownership of the data.

**B . Finger Printing:** A robust watermarking algorithm is required for this application. Watermark is embedded in digital data to trace the source of illegal copies. Information related to customer like serial number or customer identity information is used as watermark.

**C . Content Authentication (integrity protection):** The objective of this application is to detect modification in data. To verify the authenticity of the received data watermark is embedded in host data. A fragile watermarking algorithm is required in this case.

**D . Broadcast Monitoring:**The main use of broadcast monitoring is to protect TV products like news items from illegal transmission . Watermark is embedded in commercial advertisements. Automated monitoring system can verify

whether the advertisements are broadcasted as contracted or not.

**E . Indexing:** Search engine use this technique to retrieve the required data in a short period of time and without any ambiguity. In indexing, Comments and markers or key information related to the data is inserted as watermark.

## VIII . Conclusion

This paper presents an overview of digital image watermarking. First we introduced the various watermarking techniques and classified them into three types: visible watermark, invisible fragile watermark and invisible robust watermark. Spatial domain and transform domain watermarking are briefly discussed here.Two different algorithms for the digital image waterwarking are also been discussed.Comparisions between the various watermarking technologies are also been reviewed.Thus the digital image watermarking proves to be a promising technology for the pupose of data hiding.

## REFERENCES


[1]. N. S. Kulkarni, I. Gupta, and S. N. Kulkarni "A Robust Image Encryption Technique based on Random Vector" , IEEE Computer Society. IEEE conference publications,in international conference on Emerging trends in engineering and technology (ICETET),pp. 15-19,2008.

[2]. P.B.Khatkale, D.G.Lokhande, Srescoe, "Digital Watermarking Algorithm for Color Images", IOSR Journal of Engineering (IOSRJEN) ,Vol. 3, Issue 3,pp. 01-09, Mar 2013.

[3]. S. Jayaraman, S. Esakkirajan, and T. Veerakumar. "Digital Image Processing", McGraw-Hill, 2009.

[4]. Cox.I, Miller.M, Bloom.J, Fridrich.J,Kalker. T "Digital Watermarking and Steganography", 2nd Edition. ISBN: 978-0123725851

[5]. Wang, R. Z., Lin, C. F., Lin, J. C. "Image hiding by optimal LSB substitution and genetic algorithm ", Pattern Recognition, vol. 34, pp.671- 683, 2001.

[6]. Swanson.M.D,Kobayashi. M, Tewfik.A.H. "Multimedia Data-Embedding and watermarking Technologies",in Proceeding of IEEE, vol. 86,no.6, pp.1064 – 1087, 1998.

[7]. Mustafa Osman Ali, Elamir Abu Abaida Ali Osman, Rameshwar Row, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization", International Journal of Engineering and Innovative Technology (IJEIT),Vol.2, Issue 5, pp.237-231,Nov 2012.

[8] . Pereira.S , Pun.T, "Robust Template Matching for Affine Resistant Image Watermarks ", IEEE Transactions on Image Processing, vol.9,issue.6,pp.1123-1129, 2000.

[9]. Keta Raval, Rajni Bhoomarker, Sameena Zafar "Implementation of Digital Watermarking For Image Security with EBCOT Algorithm and Error Correcting Codes",International Journal of Engineering and Advanced Technology (IJEAT), Vol.2, Issue.3, pp.281-285,Feb 2013.

[10] . A. Chandra,T. Kavitha , "Robust digital watermarking using MDKP", International Journal of Scientific and Research Publications, Vol.2, Issue 6, pp.1-4,Jun 2012.

[11]. Ghouti.L, Bouridane.A , Ibrahim MK, "Digital image watermarking using balanced multiwavelets" , IEEE Transactions on Signal Processing, vol.54,issue.4, pp. 1519-1536,2006.

[12]. Reddy A.A, Chatterji B.N, "A new wavelet based logo watermarking scheme" , Conference Pattern Recognition letters,vol.26,issue.7, pp. 1019-1027, 2005.

[13]. Shivani Garg, Ranjit Singh, "An Efficient Method for Digital Image Watermarking Based on PN Sequences", International Journal on Computer Science and Engineering, Vol. 4 No. 09,pp.1550-1561, Sep 2012.

[14]. Mustafa Osman Ali , Rameshwar Rao "Digital Image Watermarking Basics, and Hardware Implementation", International Journal of Modeling and Optimization, Vol. 2, No. 1,pp. 19-24, Feb 2012.

[15]. Prabhishek Singh, R S Chadha "Review to Digital Watermarking and a Novel Approach to Position the Watermark in the Digital Image",International Journal of Engineering and Advanced Technology (IJEAT), Vol.2, Issue.4,pp.24-27, Apr 2013.

[16] . Er. Jaspreet Kaur , Er. Karmjeet Kaur, "Digital Watermark: A Study" , International Journal of Advanced Research in Computer Science and Software Engineering,vol. 2,issue.8, pp. 159-163,Aug 2012.