A Multi-purpose Dual Watermarking Scheme

Jobin Abraham
Research Scholar, Mahatma Gandhi University,
Kottayam, Kerala, India

ABSTRACT
This paper proposes an image watermarking scheme that cater to multiple purposes of copyright protection and fingerprinting. For fingerprinting images, an ID number or a unique code pertaining to the buyer is hidden with in the digital resources at the time of resource transfer. For copyright protection of the resource, a unique signature such as a logo of the owner creator is integrated imperceptibly. In the proposed method these embedding operations are performed in the transform domain using discrete wavelet transform. The embedding algorithm works in two stages; hides the fingerprint using DWT inside the logo in the first stage and in second stage, integrates this secondary watermark in the base image to be watermarked.

Keywords
Digital images; watermarking; copyright protection; fingerprinting; discrete wavelet transforms (DWT)

1. INTRODUCTION
Watermarking is in fact a centuries old mechanism for copyright protection. Currency notes are watermarked for preventing forgeries. Recently, as analog technologies for data storage and transmission has become almost obsolete digital watermarking gained more significance and popularity. Digital technologies that are widely in use and have numerous advantages expect that they require stronger data protection mechanisms when compared to older analog systems. Digital Watermarking mechanisms can address several issues concerning data protection and preservation.

Digital Watermarking is defined as the process of imperceptibly hiding ownership information inside digital resource such as an image, audio or video. Such hidden information can be extracted later and verified to establish the owner creators' rights. Many consider steganography and watermarking to be the same. Though watermarking is similar to steganography in that information is hidden in images; differs greatly on the purpose of use or intention. In steganography the message to be transmitted is kept hidden within a cover image; hence the prime motive here is covert communication. In digital watermarking, the chief concern is copyright protection.

In addition to copyright protection, watermarking is proposed as an effective mechanism for several other applications as fingerprinting, tamper proofing, document labeling and broadcast monitoring [1, 2]. For copyright protection, a unique signature of the owner is integrated into the image. During the process of watermarking, the owner information is hidden in the digital resources to be protected using an embedding algorithm. These hidden information can be extracted later to establish the rightful ownership disproving fraud claims over ownership. The algorithm used is thus very important as it determines the robustness and strength of the encoding process that makes the decode ability or breakage of watermark impossible to illegal user.

Digital fingerprinting mechanisms can detect the source of unauthorized copying and illegal redistribution of the digital resources. To facilitate for this, whenever the original creator or legal owner sells a copy of his digital resource, some unique secret information such as customer ID or purchase number will be hidden in that document. Thus each copy at the time of distribution carries a unique code. This hidden information is the fingerprint that will help in locating the source of illegal copies and forgeries.

Watermarking methods can be classified into different types based on criteria's as the transformation operation used, visibility of the encoded watermark and on the ability of the embedded watermark to survive signal processing operations. Based on the transformation used there is spatial domain watermarking methods [2] and transform domain methods [3, 4]. The classification as visible watermarking and invisible watermarking schemes is based on visibility of the embedded watermark [5]. Robust watermarking and fragile watermarking is yet another classification indicating the resistance of hidden watermark to image processing operations such as contrast enhancement or histogram equalization.

Transform domain methods mostly uses discrete cosine transform (DCT)[3, 6], or discrete wavelet transform(DWT) [4, 7 ,8 9] for embedding the watermark signal in the images in frequency domain. A transform domain method that employees discrete wavelet transform (DWT) for watermark embedding is discussed in section II. DWT decomposes an image into four bands: a low frequency (LL) region, two mid frequency (HL, LH) region and a high level frequency (HH) component, as shown in figure.1. The most of the signal energy will be concentrated at the low frequency LL band and the higher frequency bands contain the edges and textures of the image.

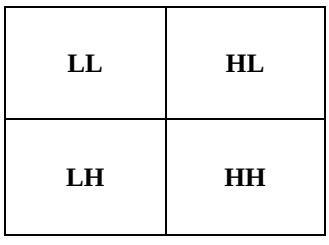


Fig.1 Discrete wavelet transform of 2-D image

In this paper, a method for embedding watermarks to establish ownership rights and also to fingerprint gray scale images is proposed. Section II describes the algorithm and section III is experimentation and testing of the proposed algorithm.

2. THE METHOD

Watermarking process comprises two key stages: Watermark embedding and Watermark extraction. The embedding stage integrates the watermark signal with in the base image. Watermark extraction is in fact the reverse process that attempts to decode the hidden watermark signal from the watermarked copy of the base image.

The algorithm accepts a base image of size N x N as input. Watermarking embedding is performed using an indexed logo gray scale image. Prior to this embedding, an index number is integrated with the logo image using DWT transform. Here the primary watermark is the gray scale coded number and the secondary watermark is the logo image.

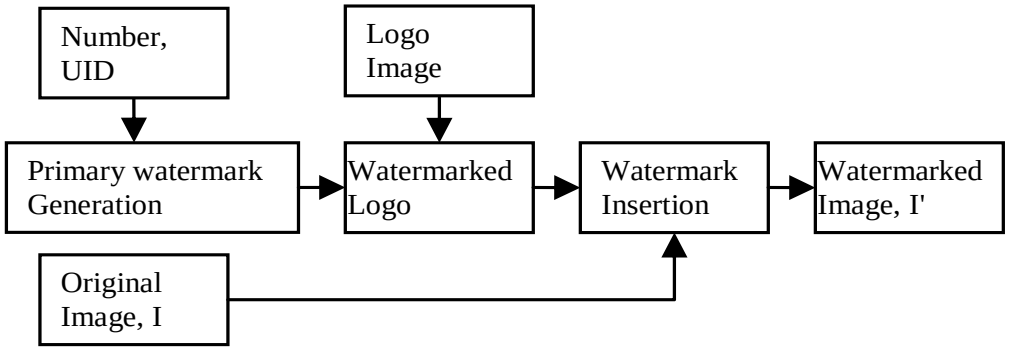


Fig.2 Process of Watermark Embedding

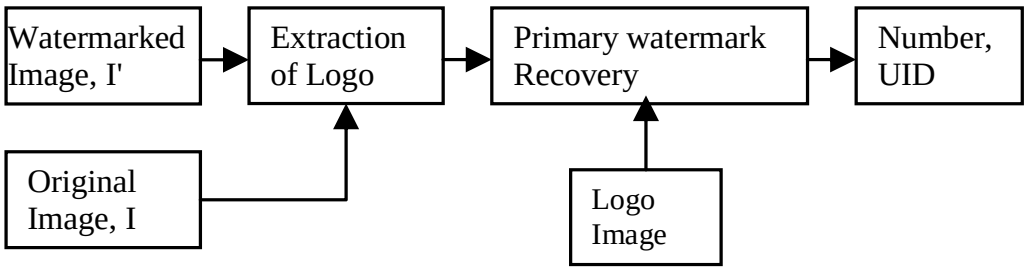


Fig.3 Process of Watermark Extraction

Figure 2 shows the stages in watermark embedding process. The UID representing a client is encoded as a gray scale image and is then embedded using DWT in secondary watermark. After hiding the grey scale coded index number in owner's logo image, apply inverse transform to generate watermarked secondary logo image. In next phase of embedding process, the base image I is watermarked using the above generated secondary watermark to produce the watermarked image I'.

Extraction process attempts to retrieve the logo of the owner as well the fingerprint code that identifies the legal buyer of digital resource. The original image I and the logo of the owner distributor are essentially required for decoding the hidden information from the watermarked copy. Block diagram of extraction process is shown in figure 3.

2.1 Embedding Algorithm

The watermark embedding algorithm comprises two stages. Stage1 is an encoding scheme, named as Jos coding, represents the number employed as primary watermark using gray scale values. In stage2, the encoded number from previous stage is hidden inside the grayscale logo image. This is the secondary watermark with which base image I is watermarked.

Stage 1: Encoding the UID number

The UID selected can be a 9-16 digit number. For representing this number, each digit in the number is to be encoded into a grayscale value. Encoding of the digits are based on a lookup table containing grayscale values to correspond for each digit in decimal number system.

Grayscale values are assigned for all digits in decimal number system, d = {0, 1, 2, 3….9} from a predefined look up table of equivalent grayscale values, say, gv = {25, 50, 75, 100 …225}. Now, any number may be encoded as a grayscale image using the following procedure.

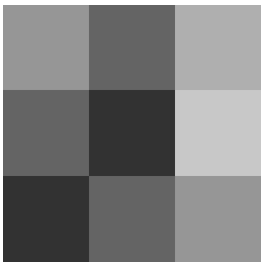


Fig.4 Primary watermark

1. Let n be a number and d a digit from n.
2. Substitute the corresponding gray scale value for the digit in hand from the look up table, $d_i = gv_i$, where i = 0,1…9.

3. Represent every digit d_i using a 4x4 block of gv_i, by repeating the grayscale value for that digit.
4. Repeat the steps above from (2-4) for converting all the digits in n.
5. Represent the blocks generated above as a 4r X 4r image where r^2 is the number of digits in n.

As an example, consider an UID, n, having nine digits, the above encoding steps will form a 12x12 block when the nine 4x4 sub-blocks are rearranged. The fig.4 below shows how the nine digit number, 536317135, shall appear after coding. This pattern is used as primary watermark by the embedding algorithm.

Stage 2: Watermark Embedding

In stage2 the fingerprint code generated in the previous stage is integrated to the secondary watermark. Base image I is watermarked as follows.

1. Input an image I of size NXN and a logo image I_L.
2. Apply DWT on logo image for watermarking the logo image I_L using Pw, generated in stage 1.
3. Select a sub-band, LL, for integrating Pw.
4. Compute, $y'_{LL}(i,j) = (1-sf)*y_{LL}(i, j) + sf*Pw(k)$, here sf is strength factor and $k = 16r^2$.
5. Repeat the above, step 4, for next i,j until all primary watermark coefficients are embedded.
6. Compute inverse DWT to obtain the watermarked logo image, Sw.
7. Use Sw as secondary watermark to a base image I.
8. Apply DWT on Sw and I.
9. Select the sub-band LL for embedding.
10. Compute, $I'_{LL}(i, j) = (1-sf)*I_{LL}(i, j) + sf * Sw_{LL}(k)$.
11. Repeat the above, step 10, for next i, j until all secondary watermark coefficients are embedded.
12. Compute inverse DWT to get I', the watermarked image.

The primary watermark is a grayscale 2D array consisting of 4x4 block per digit. Each 4x4 block thus in turn represents a digit from the number. Hence, to represent a 16 digit number sixteen 4x4 blocks will be used. DWT is applied on the 4x4 block number from primary watermark and also on the logo image for embedding the primary watermark. Inverse DWT is taken at the end to convert the coefficients back to produce the watermarked secondary image. The next process is to integrate the secondary watermark to original base image. DWT of image and watermarked logo is computed in the second level of embedding process to watermark the base image using secondary watermark.

2.2 Extraction Algorithm

Watermark extraction process involves two key tasks. First, the watermarked logo is extracted and in second, the primary watermark is extracted from the gray scale logo image. The algorithm requires the original non-watermarked images for decoding hidden contents. Such methods are generally referred to as non-blind watermarking techniques.

1. Input the images I, I' and logo image I_L.
2. Apply DWT on I and I'.
3. Compute the difference as, $Sy(k)=(I'(i,j)-(1-sf)*I(i,j))/(sf)$; for k=1..N/2.
4. Repeat the above step for next i, j until all embedded coefficients are extracted.
5. Using the extracted coefficients Sy, built the logo image I'_L by applying inverse DWT.
6. Compare the above, I'_L, with original logo image I_L
7. Apply DWT and extract the values for, $Py(k)=(I'_L(i,j)-(1-sf)*I_L(i,j))/(sf)$; for k=1..N/4.
8. Repeat the above step for next i, j until all coefficients are extracted.
9. Reshape the coefficients in Py as 4r X 4r gray scale image, where r*r is the number of digits in the original primary watermark, n.
10. Now to decode the digit d_i that corresponds each constituent 4x4 block by comparing the average pixel value computed for the block with the lookup table. Allow an error variation in a threshold range of $gv_i \pm 10$.
11. Decode all d_i digits by repeating step 10 to regenerate the hidden UID.

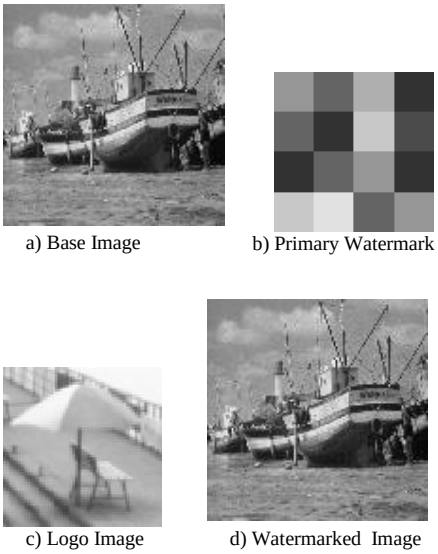
A potential problem due to forward and inverse transform operations carried out on base images during the process of watermarking; some value may vary from the actual during the conversion. These unintentional modifications can affect the extracted values. Hence to accommodate for these error variations the method uses an acceptable range of grayscale value at the time of digit estimation. Expression 1 is the employed in this method to allow for the transformation errors.

$$d_i = gv_i \pm 10 \qquad (1)$$

The range based estimation and highly redundant nature of the watermark signal used enhances the probability of accurate detection of hidden watermark codes**.**

3. EXPERIMENTAL ANALYSIS

The algorithm presented in section II is tested by implementing on various test images.



a) Base Image b) Primary Watermark

c) Logo Image d) Watermarked Image

Fig.5 Output images from watermarking process

Fig.5.a shows gray scale base images of size 512 x 512, which is watermarked using the logo of the owner is shown in fig 5.c. The secondary watermark is fingerprinted using a 16 digit number which is encoded using proposed Jos coding as shown in fig.5.b.

The algorithm was tested on more standard images and other gray scale images. Figure.6 shows few more examples and results for image watermarking.

a) Base Image b) Watermarked Image

Fig.6. Watermarking images

$$PSNR = 20Log\left[\frac{255}{RMSE}\right] \quad (2)$$

$$MSE = \frac{\sum(I(i,j) - I'(i,j))}{N * N} \quad (3)$$

Table 1. Peak Signal to Noise Ratio measurement

Image	Size of Watermarks: Pw, Sw	PSNR(dB)
Lena	16x16, 64x64	42.71
Boat	16x16, 64x64	45.86
Deer	16x16, 64x64	46.12

During the extraction stage the algorithm successfully retrieved the logo image from the watermarked image, from which the hidden numbers were also reproduced. Since the hidden watermark employed is highly redundant in nature, the extracted values matched the original integrated figures very closely.

The quality of the watermarked images is evaluated by measuring Peak Signal to Noise Ratio (PSNR). PSNR value for an image I of size N x N and its watermarked copy I' may be measured using equation 2 and 3. PSNR is expressed in dB. Higher PSNR values indicate that the image quality is higher. And a low PSNR is an indicative of greater difference between the two images compared. The table.1 lists the PSNR values obtained for various test input images. PSNR values were also observed for differently sized secondary watermark and primary watermark. For experimentation, a primary watermark of size 16x16 and secondary of size 64x64 is used.

4. CONCLUSION

A novel watermarking scheme for dual purpose of copyright protection and fingerprinting digital images is proposed. The method employs two different operations for hiding the creator owner information as well as the buyer information in the digital resources. This allows for establishing the rights of the distributor and also makes it possible to trace the source of illegal copies. In this method, DWT transform is employed twice, first on the grayscale logo image and then on the base image to be watermarked. During the process of extraction, the secondary watermark, the logo, is retrieved and then the fingerprint is decoded from the resulting secondary watermark. Due to the high redundant structure of the primary watermark, the digits were regenerated accurately. The embedding process when tested on various standard images performed watermarking imperceptibly and no visible traces or distortions could be noted in the resultant watermarked copies. For objective measurement of the quality of the watermarked images, PSNR was measured. And the results for various test cases showed that PSNR values are even better when fewer digits and smaller logos are used for fingerprinting.

5. REFERENCE

[1] I.J Cox, Mat M Miller, Jeffrey A Bloom, "Watermarking Applications and their Properties", IEEE ITCC, March 2000.

[2] Xin Liao, Qiao-yan Wen, jie Zhang, "A Steganographic method for Digital Images with four-pixel differencing and modified LSB Substitution", 2011.

[3] Tribhuvan Kumar Tewari, Vikas Saxena, "An Improved and Robust DCT based Digital Image Watermarking Scheme", International Journal of Computer Applications, June2010.

[4] Wai Chu, "DCT based Image Watermarking using Subsampling", IEEE Transactions on Multimedia, pp 34-38, Vol.5, March 2003.

[5] Vidyasagar m Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", IEEE Conference on Industrial Infomatics, pp 709-716, 2005.

[6] Latha Parameswaran, K Anbumani, "Content-based Watermarking for Image Authentication using Independent Component Analysis", Informatica 32 pp299-306, 2008.

[7] Qing Liu, Jun Ying, "Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis", IEEE Symposium on Electrical & Electronics Engineering, 2012.

[8] Nagaraj V Dharwadkar, B.B Amberker, " An Efficient non-blind Watermarking Scheme for Color Images using Discrete Wavelet Transform", International Journal of Computer Applications, May 2010.

[9] Chi-Man Pun, Xiao-Chen Yuan, "Geometric Invariant Digital Image Watermarking Scheme Based on Histogram in DWT Domain", Journal of Multimedia, Vol.5, pp 434-442, 2010.