INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

A Digital Watermarking Technique Using Discrete Wavelet Transform

Sneha Nargundkar
Assistant Professor, Shree Rayeshwar Institute of Engineering & Information Technology, Shiroda, Goa, India

Abstract:
The data embedded on digital media or distributed over the internet can easily be replicated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert a watermark into potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. Watermarking dependency on the original image increases its robustness but at the same time we need to make sure that the watermark is imperceptible. In this paper, we have presented a robust digital image watermarking scheme based on Discrete Wavelet Transform by embedding scrambled watermark in middle frequency subband. The imagescrambling is applied by Arnold Transform. The decomposition is done with Haar wavelet and direct weighting factor is used in watermark embedding and extraction process. The scheme results in exact recovery of watermark with standard database images of size 512x512, giving Correlation Factor equal to 1 with PSNR values in the range of 53-60dB.

Keywords: *Discrete Wavelet Transform, Image Scrambling, Arnold Transform, robustness, imperceptiility.*

1. Introduction

With the ease of editing and perfect reproduction in digital domain, the protection of ownership and the prevention of unauthorized tampering of multimedia data (audio, image, video, and document) have become important concerns. Data hiding, schemes to embed secondary data in digital media, have made considerable progress in recent years and attracted attention from both academics and industry. One way to protect multimedia data against illegal recording and retransmission is to embed a signal, called digital signature or watermark that authenticates the owner of the data. Watermarking is defined as adding a payload signal to the host signal. The payload can be detected or extracted later to make an assertion about the object i.e. the original data that may be an image or audio or video.

An effective watermarking scheme should have the following characteristics:

- Imperceptibility: A watermark embedding procedure is imperceptible if humans cannot distinguish the original data from watermarked data.
- Robustness: Watermark robustness accounts for the capability of the hidden data to survive both non-malicious manipulations, which do not explicitly aim at removing the watermark, and malicious manipulations, which precisely aim at damaging the hidden information. It has been argued that robustness can only be maintained if watermark is placed in perceptually significant regions of an image. But for the watermark to be imperceptible, it should be placed in perceptually insignificant regions of an image. They are two conflicting requirements.

Watermarking algorithms can be classified on several criteria [9]:

1. According to watermark detection and extraction: Blind and non-blind watermarking. Non-blind watermarking require that original image must exist for extraction whereas blind techniques do not require original image for watermark extraction.
2. According to ability of watermark to resist attack: Fragile, semi-fragile and robust watermarking. A watermark is fragile if the information hidden within the host data is lost as soon as any modification is applied to the host signal. Watermark is semi-fragile if it survives a limited well specified, set of manipulations, leaving the quality of the host document virtually intact. In robust watermarking it is required that the watermark is resistant against non-malicious manipulations.
3. According to visibility of embedded watermark: Visible and invisible watermark.
4. According to domain of watermark insertion: Spatial domain and transform/frequency domain watermarking. In spatial domain, watermark is embedded by directly modifying pixel values of original image. Ex: Least Significant Bit insertion. Such algorithms have low watermark information hiding capacity, less PSNR, less correlation between original and extracted watermark and less security, hence anybody can detect such algorithms. In frequency domain watermark is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against watermarking attacks because information can be spread out to entire image. Ex: Discrete Wavelet Transform, Discrete Cosine Transform, CDMA based Spread Spectrum Watermarking.

The rest of the paper is organized as follows: Section II focuses on survey of existing digital image watermarking algorithms. Section III focuses on importance of Discrete Wavelet Transform. In section IV, our watermarking methodology is given. Section V shows experimental results after implementation and testing and the conclusion is drawn in Section VI.

2. Literature Survey

A major breakthrough was achieved in the field of watermarking when Cox et al. proposed a secure spread spectrum watermarking technique for multimedia [6]. They proposed that a watermark should be constructed as an independent and identically distributed Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data which makes the watermark robust to signal processing operations and common geometric transformations provided that the original image is available.

K. Ramani et al. proposed a robust and imperceptible watermarking scheme for copy right protection [1]. The method is based on decomposing an image using the Discrete Wavelet Transform, and then embedding locations are generated from the low frequency sub-band by using secrete sort to improve the embedding intensity.

Wang Hongjun, Li Na have proposed a non-blind DWT based method [3] in which watermark was embedded in middle frequency coefficient using α as flexing factor with $\alpha = \beta |m|$,where m is mean value of all coefficients watermarking embedded. The mean value of many pixels in original image is used so that algorithm can produce favorable output for some different images. But this method doesn't provide enough security.

The method proposed in [3] using DWT was extended in [2] to enhance security of algorithm by using Arnold's Transform pretreatment for watermark. Arnold transform pretreatment eliminates spatial correlation and disperses the error bits among all pixels to make watermarking more strongly robust against cropping operation.

A digital image watermarking algorithm based on wavelet transform is proposed in [4] where Arnold transform is used to scramble the original watermark. In the embedding process two sub-bands which are in the same direction but in different resolution are selected when the carrier image is decomposed by two-layer wavelet transform. In the process of watermark extraction, the watermarks are detected by using the embedded position and scaling parameter after the wavelet decomposition of the watermarked image and the original image.

A strongly robust, non-blind algorithm is proposed in [7] based on DWT by embedding scrambled watermark in middle frequency sub band. The image scrambling is applied by Arnold Transform. The security levels are increased by generating PN sequence depending on periodicity of watermark image. The decomposition is done with Haar wavelet and the direct weighting factor is used in watermark embedding and extraction process.

3. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform offers multi resolution representation of an image and also provides perfect reconstruction of decomposed image. Discrete dyadic wavelet can be represented as

$$\psi_{j,k}(t)=2^{-j/2}\,\psi(2^{-j}t-k)\ j,\ k \in Z$$

When image is passed through series of low pass and high pass filters, DWT decomposes the image into sub bands of different resolutions. Decompositions can be done at different DWT levels.

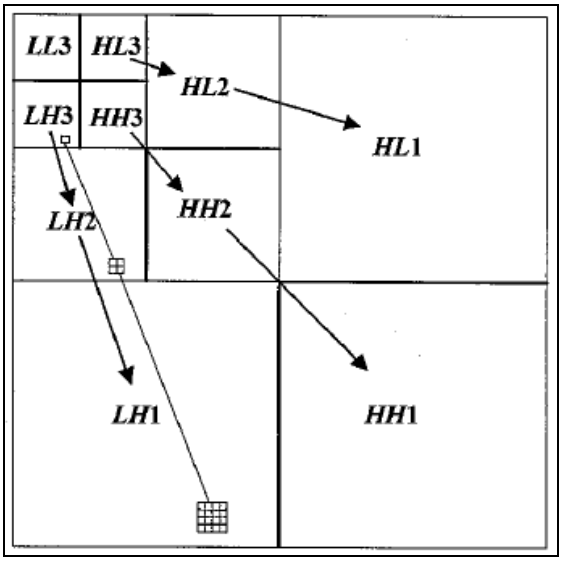


Figure 1: Three Level Image Decomposition

At level 1, DWT decomposes image into four nonoverlapping multi resolution sub bands: LLx (Approximate sub band), HLx (Horizontal subband), LHx (Vertical subband) and HHx (Diagonal Subband). Here, LLx is low frequency component whereas HLx,

LHx and HHx are high frequency (detail) components. To obtain next level wavelet coefficients, the subband LL1 is further processed until final N scale reached. At level N, we have 3N+1 subbands with LLx (Approximate Components.) and HLx, LHx, HHx (Detail components) where x ranges from 1 to N. Note that the arrow points from the parent subband to its children subband. The lowest frequency subband is at the top left and the highest frequency subband is at the bottom right. A wavelet tree consisting of all descendants of a single coefficient in the subband LH3 is also given.

Embedding watermark in low frequency coefficients can increase robustness significantly but maximum energy of most of the natural images is concentrated in approximate (LLx) subband. Hence watermark is not be embedded in LLx subband because it will cause severe and unacceptable image degradation. The good areas for watermark embedding are high frequency subbands (HLx, LHx and HHx), because human naked eyes are not sensitive to these subbands. They yield effective watermarking without being perceived by human eyes. But HHx subband includes edges and textures of the image. Hence HHx is also excluded. The rest options are HLx and LHx. We decide to perform watermarking in HLx region because Human Visual System (HVS) is more sensitive in horizontal than vertical. The image decomposition is done with Haar which is simple, symmetric and orthogonal wavelet.

4. Proposed Algorithm

4.1. Watermark Embedding

4.1.1. Watermark Pre-treatment

Watermark Scrambling is carried out through many steps to improve security levels. It makes sure that even if attackers intercepted the watermarking messages, they cannot get the exact secret messages. [9] We have use Arnold Transform for image scrambling which has a special property that image comes to its original state after certain number of iterations. These number of iterations are called 'Arnold Period' or 'Periodicity of Arnold Transform'.

Given an N*N image, the Arnold transform that is applied to every pixel in the image is given by

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod } N)$$

where, (x, y) ={0,1,.....N} are pixel coordinates from original image. Arnold transform will shift the value of the pixel at position (x,y) to position (xn,yn). The periodicity of Arnold Transform (P) is dependent on size of given image and is calculated using the following algorithm:

for n=1 to ….
xn=x+y;
yn=x+2*y;
if (xn mod N==1 and yn mod N==1) then
Arnold Peridicity (P)=n;

4.1.2. Embedding Algorithm

- Step 1: Perform a three-level decomposition of original image using Haar wavelet to find level 3 coefficients-LL3, HL3, LH3, HH3.
- Step 2: Find Arnold periodicity 'P' of watermark using the above algorithm.
- Step 3: Determine 'KEY' such that $0 \leq KEY \leq P$.
- Step 4: Find two scrambled images applying Arnold Transform on watermark with KEY1 and KEY2, where KEY1=KEY+Count, KEY2=KEY-Count; $KEY+Count \leq P$.
- Step 5: Take absolute difference of two scrambled images to get scrambled watermark.
- Step 6: Add scrambled watermark to HL3 coefficients of original image as follows:

HL3'(i,j)= HL3(i,j) + k*W(i,j)

where k is weighting factor, HL3'(i,j) are newly calculated level-3 horizontal coefficients, HL3(i,j) are level-3 horizontal coefficients of original image, W(i,j) is scrambled watermark.

- Step 7: Apply Inverse Discrete Wavelet Transform at level3, level2 and level1 sequentially to get watermarked image.

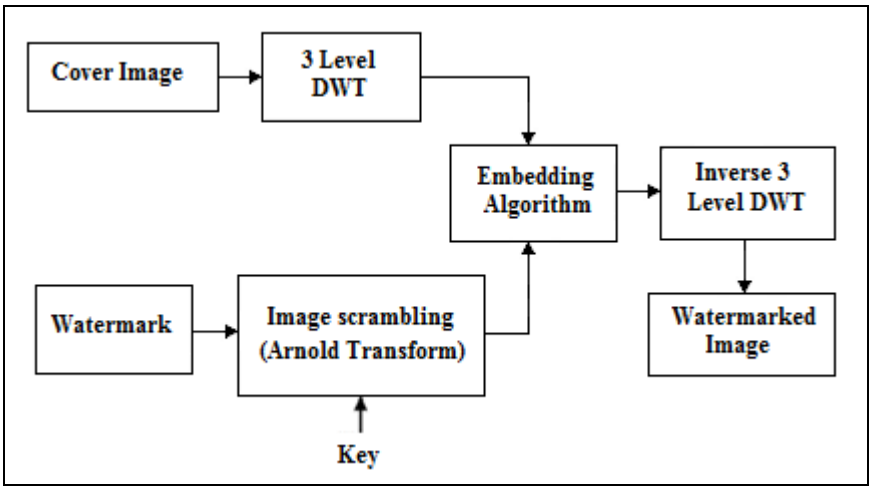


Figure 2: Watermark Embedding

4.2. Watermark Extraction

- Step 1: Decompose original image using Haar wavelet up to 3 levels to get HL3 coefficients.
- Step 2: Decompose watermarked image using Haar wavelet up to 3 levels to get HL3' coefficients.
- Step 3: Apply Extraction formula as follows:

Difference (i,j)=abs(HL3(i,j)-HL3'(i,j))/k
If Difference (i,j) < Threshold
then Extracted_Watermark(i,j)=0
otherwise Extracted_Watermark(i,j)=1

- Step 4: Perform image descrambling using Inverse Arnold Transform with the 'KEY' that we had used in embedding process to recover the watermark

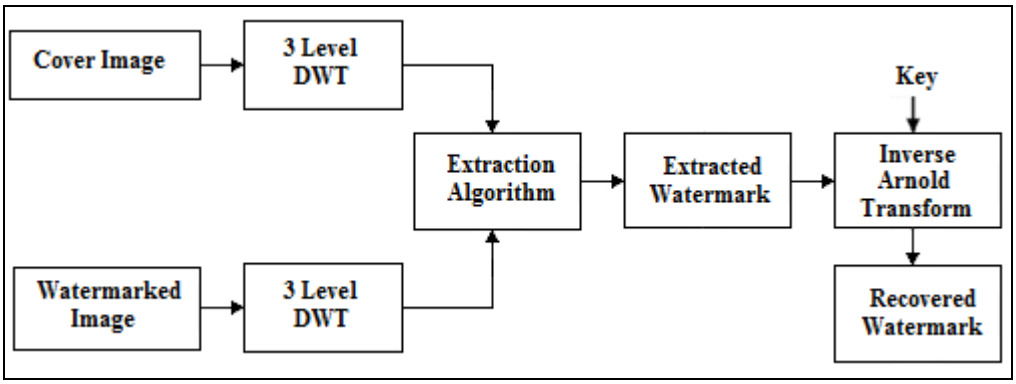


Figure 3: Watermark Extraction

5. Experimental Results

The technique was implemented in Matlab 7.10 and standard database images with 512x512 sizes as cover image and 64x64 size binary watermark images were used for testing. The performance Evaluation was done by two performance evaluation metrics: Perceptual transparency and Robustness.

Perceptual transparency means perceived quality of image should not be destroyed by presence of watermark. The quality of watermarked image is measured by PSNR. Larger the PSNR value, better is the quality of watermarked image. PSNR for image with size M x N is given by:

$$PSNR(dB)=10\log_{10}\frac{(Max_I)^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-g(i,j)]^2}$$

where f(i,j) is pixel gray values of original image, g(i,j) is pixel gray values of watermarked image. A PSNR value of at least 30dB is required for the watermarked image to be perceptually transparent.

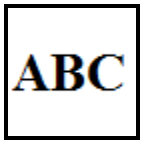
Robustness is a measure of immunity of watermark against attempts to remove or destroy it by various manipulations like compression, filtering, rotation, scaling, collision attacks, resizing, cropping etc. It is measured in terms of normalized correlation factor. The correlation factor measures the similarity between original watermark and extracted watermark. Its value generally varies from 0 to 1. Ideally it should be 1 but the value 0.75 is acceptable. Robustness is given by:

$$NC = \frac{\sum_{i=1}^{N} w_i \, w_i'}{\sqrt{\sum_{i=1}^{N} w_i} \sqrt{\sum_{i=1}^{N} w_i'}}$$

where, N is number of pixels in watermark, w_i is original watermark, w_i' is extracted watermark.
For standard 'Lena' image we get PSNR=53.9069 dB and NC=1, for weighting factor k=17. The PSNR and NC values for various standard database images with corresponding test images are shown in Table 1.

Figure 4. a) Original 'Lena' Image

b) Watermarked 'Lena' Image



c) Extracted Watermark

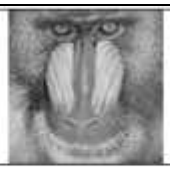
Images						
Weighting factor (k)	15	15	14	5	16	12
PSNR (dB)	53.9423	53.2825	54.2549	59.6757	53.6916	60.2555
NC	1	1	1	1	1	1

Table 1: Experimental results for standard database images with size 512x512

6. Conclusion

A robust algorithm of digital image watermarking based on DWT is introduced. Experiment results show that the algorithm realizes unobtrusiveness of watermark triumphantly to human visual system and keeps the quality of original image. Also the proposed method supports more security. One of the reasons, most of the research is focussed on Discrete Wavelet Transform is that JPEG2000 image compression standard is more suited to DWT than DCT. The presented Digital Image Watermarking methodology can be extended to color images and other multimedia for authentication and copyright protection.

7. References

i. Ramani K.; Prasad E.V, Varadarajan S.; Subramanyam A,"A Robust Watermarking Scheme for Information Hiding", Advanced Computing and Communications, 16th International Conference, 14-17 Dec. 2008, pp:58 – 64.
ii. Na Li; Xiaoshi Zheng; Yanling Zhao; Huimin Wu; Shifeng Li, "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform", International Symposium on Electronic Commerce and Security, 3-5 Aug. 2008, pp:942 – 945.
iii. Wang Hongjun, Li Na," An algorithm of digital image watermark based on multiresolution wavelet analysis", International Workshop on VLSI Design and Video Technology, Proceedings, 28-30 May 2005, pp: 272- 275.
iv. Vaishali C. Sanap, Aditi Jahagirdar and Meenakshi A. Thalor, "Data Hiding of Binary Image Using Discrete Wavelet Transformation", Journal of Global Research in Computer Science, Volume 1, No. 5, December 2010, pp:27-29.
v. Abu-Errub, A., Al-Haj, A., "Optimized DWT-based image watermarking", First International Conference on Applications of Digital Information and Web Technologies, IEEE, August2008,pp: 4-6.
vi. Ingemar J. Cox, Joe Kiliany, Tom Leightonz and Talal Shimon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing,1997,vol.6, issue.12, pp:1673-1687.
vii. B.L.Gunjal and R.R.Manthalkar, "Discrete Wavelet Transform Based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images", 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), Nov2010, pp:124-129.
viii. Zhao Rui-mei, Wang Mei, Hu Bo-ning, Lian Hua, "Digital Image Watermarking Algorithm Based on Wavelet Transform", Third International Symposium on Intelligent Information Technology Application, Nov2009, pp:437-440.
ix. Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics, August2005,pp:709-716