Watermarking for Robustness of Digital Images Based on Discrete Wavelet Transform (DWT)

Gagana Deepa J[1]
Student,(M.Tech)
Dept of CS&E,
Adichunchanagiri Institute of Technology,
Chikkmagaluru

Darshan L. M[2]
B.E, M.Tech,
Dept of CS&E,
Adichunchanagiri Institute of Technology,
Chikkmagaluru

***Abstract*—Arobustness of image watermarking in transform domain using DWT is evaluated. The coverimage is decomposed in to 4-levels using Bi-orthogonal wavelet transform. Binary Watermark is embedded using random pseudo noise sequence and gain factor. For embedding watermark information a random pseudo noise sequence is added in the medium frequency coefficients of an image and then use inverse DWT to forman watermarked image. To extract the secret image same procedures as the embedding process is used and then compare the watermarked coefficients with original image coefficients. The performance evaluation is calculated using the performance metrics such as robustness in terms of MSE and PSNR. Imperceptibility in terms of SSIM and Mean Correlation these shows good imperceptibility and higher robustness against various noise attacks.**

Keywords*—Structure Similarity Index (SSIM), Discrete Wavelet Transform (DWT),Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR).

1. INTRODUCTION

Now a days a rapid development of multimedia and widespread distribution of digital data over a internet network this become easy to obtain a intellectual properties. To overcome this problem using a approach called digital watermarking. This is the practice of imperceptibly altering a cover to embed a message about that cover image. The process of original multimedia data modified to embed a watermark with key information is watermarking process. The method of embedding of original data is unchanged and the impose of modifications can be identified using the extraction method.

Watermarking will embed the secret data in host multimedia without affecting the visual quality and robust against various types of attacks with preserving the perceptual quality of original cover image.The digital watermarking uses the two dimensional bi-orthogonal DWT for embedding along with the PN sequence for security and extraction process the performance of the watermarking process is calculated using metrics like robustness and imperceptibility.

A multiple watermarks are embedded for image security where, depending on the selected coefficients, multiple of watermark producer is used. The cover image is selected then converted to grayscale image for future process.

According to working domain, Watermarking can be done for spatial domain a direct pixels values is considered or in frequency domain a wavelet coefficients are considered. In spatial domain the watermarked data is replaced by the original data, as this is simple method but less robust. In frequency domain the original image is transformed into frequency wavelets by using Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). A two-dimensional DWT signal is decomposed along the row and column directions by using a low and high-pass filters as shown in Figure 1.

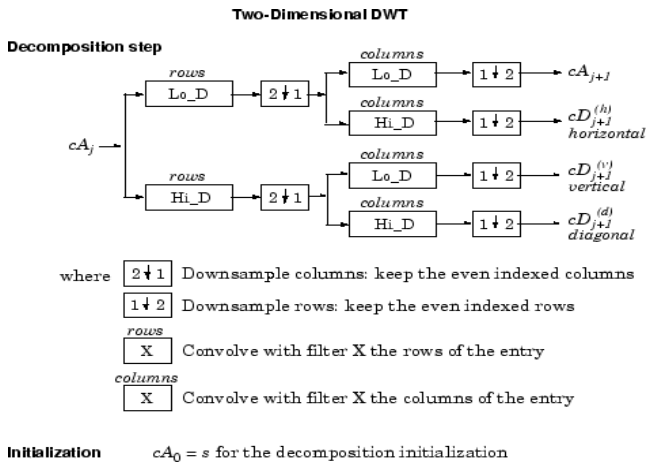

Figure 1: Single level 2-dimensional DWT.

In any decomposition level the output consists of four sub-bands: an approximate sub-band (LL), and three detailed sub-bands (LH, HL and HH) that are called the horizontal, vertical, and diagonal sub-bands as shown in Figure2. The approximate sub-band is further used for next level decomposition.

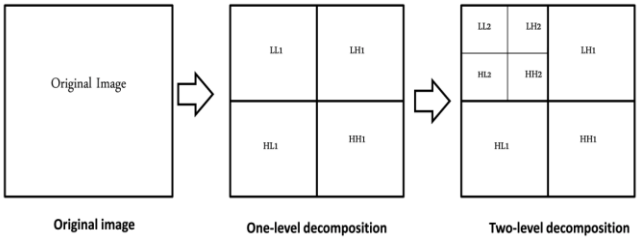

Figure 2:Wavelet sub-bands with 2-level decomposition of a 2-dimensional signal.

2. MOTIVATION

However, in recent years, digital technology for manipulating images had made difficult to distinguish the visual truth of image. Besides, the characteristics of digitising bring significant effect on copyright issues, this create an urgent need to protect intellectual property on the digitally recorded owners information. Digital watermarking is proposed to claim the ownership of the source and owner. Unlike encryption, it does not restrict access to the data. The intellectual property rights is no longer protectedonce encrypted data is decrypted.

3. RELATED WORK

The Least Significant Bit (LSB) based on watermarking technique directly the the pixel is used with the pseudo random generation based on the user given key is a straightforward method proposedby Ramani K. et al.[2], but this method not a secured algorithm. To overcome the shortcomings of this method, the digital watermarking technique based on Discrete Wavelet Transforms has been presented. The HH and LL sub-bands are used for the construction of DWT multi watermarking scheme. The combining of the two sub-bands for embedding the watermark provides a system with good robustness in a large scale[3]. M. Chandra has used middle frequency band to add watermark image bits in the cover image [4]. To make this method is more robust compared then other method. By using DWT domain that imperceptibly embeds the secret image in the cover image such that watermark can be extracted later. Images are the region of similar texture that are connected and gray scale that forms the object. For image analysis Wavelet Transform are best suited. To analyze sharp spikes and discontinuities of the signal wavelet functions are used.

The combined DWT-DCT digital image watermarking method [1] is evaluated a blind watermarking uses DCT-DWT that embeds a binary image into the gray images is presented. Watermark is embedded in the DCT blocks of the selected four medium frequency sub-bands of three-levels DWT transformed of a original cover image. This results shows that the imperceptibility of watermarked image is acceptable but the results shows the robust for most of common image processing noise attacks.

4. METHODOLOGY

A. Bi-Orthogonal Wavelet Transform in DWT

In this technique the original image intensities are transformed to coefficients. The inverse transform of marked coefficients to watermarked image. DWT becomes the most suitable transformation it gives the information about frequency, amplitude along with time information at which time signal is applied. A Wavelet is an orthogonal basis of vector space. Wavelet has basis set of orthogonal functions, scaling function φand wavelet function ψ. The translation and scalingof the two functions get complete basis sets. The wavelets basis set contains one scaling function and all other are the wavelet functions shown in equation 1. The scaling function has the average part of the signal information and the wavelet hasa difference information.

$$f(t)=\sum^{\infty}_{K=-\infty} C_K\varphi_K(t) + \sum^{\infty}_{j=-\infty}\sum^{\infty}_{K=-\infty} d_{jK}\psi_{jK}(t) \quad \text{Eq 1}$$

C_K ,d_{jK}– Coefficients of the DWT function f(t).

Where C_K represents a average part of signal information (LL) uses equation 2 and d_{jK} represents the variationsat different scales (LH, HL, HH) uses equation 3. These arecommonfeatures for all wavelets.

$$C_K = \int f(t)\varphi_K(t)\,dt \quad \text{Eq 3}$$

$$d_{jK} = \int f(t)\psi_{jK}(t)\,dt \quad \text{Eq 4}$$

Within each wavelet, the subclasses of wavelet are differed by level of iteration and by count ofcoefficient values.A single level 2 dimensional wavelet decomposition with respect to particular filters, low pass or high pass and computes the approximate and detail coefficients matrices uses the equations 5, 6, 7, 8.

$$\Phi(t)=\sqrt{2}\sum^{\infty}_{n=-\infty} h[n]\varphi(2t-n) \quad \text{Eq5}$$

$$\Phi'(t)=\sqrt{2}\sum^{\infty}_{n=-\infty} h[n]\varphi'(2t-n) \quad \text{Eq 6}$$

$$\psi(t)=\sqrt{2}\sum^{\infty}_{n=-\infty} h[n]\psi(2t-n) \quad \text{Eq 7}$$

$$\psi'(t)=\sqrt{2}\sum^{\infty}_{n=-\infty} h[n]\psi'(2t-n) \quad \text{Eq 8}$$

The DWT of cover image is computed for the robustness of watermarking process. If the data is embed in the lower frequency band then there are chances of losing of data and if the data is embed in the high frequency band are very prone to attack. So the medium frequency band is selected for embedding secret image. The secret image is embedded in the 4th level in the cover image for security and robustness as shown in Figure 3.

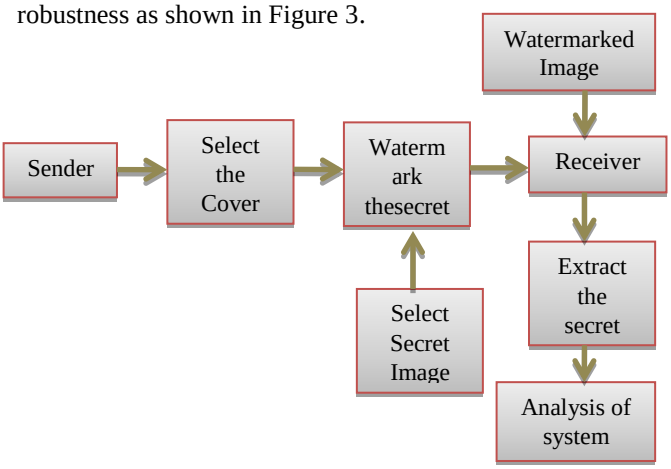

Figure 3: Architecture diagram of watermarking using DWT.

The embedding process uses the PN sequence that is randomly generated and the K is a modulation index.In this a biorthogonal wavelet transform is used to transfer the image values from spatial to frequency domain by this 4 sub-bands will be formed this process is done for 4 levels. The medium frequencies are selected to embed the secret image in a cover image by sender and inverse DWT is applied for 4 levels to get watermarked image. At the receiver side comparing the medium frequencies of watermarked and cover image to extract the secret image. Then the performance evaluation is done for different noise attacks.

B. ALGORITHM

Embedding Method

The proposed work uses the DWT for embedding a secret image in a cover image as follows

Step 1: Consider the cover image of size 256x256 of gray scale.

Step 2: Apply 2-dimensional biorthogonal DWT at 4 levels to get the wavelet coefficients of matrix defining the approximate, horizontal, vertical, and diagonal details as LL4, LH4, HL4 and HH4 sub-bands of size 16x16.

Step 3: Generate the random binary pseudo noise sequence of size 16x16.

Step 4: Consider the binary secret image of size 16x16.

Step 5: Add binary pseudo noise sequence with binary secret image by every individual element. This will be the final data to embed.

Step 6: If the added binary watermark value is 1 then, a new wavelet coefficient matrix is the sum of final embed data multiplied by constant factor K. If the added binary watermark value is 0 then, the new wavelet coefficient matrix minus of the final embed matrix is multiplied by a constant factor K.

Step 7: Changing the medium bands that is LH and HL sub bands by using above logic for a better imperceptibility.Hence the LH and HL bands has watermarked coefficients.

Step 8: Performing inverse two dimensional DWT for 4 levels using same wavelet but with a new wavelet coefficients values. This generates a watermarked image.

Extraction Method

The process of getting the secret image from the watermarked image as follows

Step 1: Consider the watermarked image and perform two dimensional DWT for four levels using a same wavelet transform as of embedding process.

Step 2: Consider the original cover image and perform 2 dimensional DWT for four levels using a same wavelet transform.

Step 3: Now compare the wavelet coefficients of watermarked image and original image where both having of same length.

Step 4: If a transformed coefficient of watermarked image is lesser or equal to the transformed coefficient of cover image place a value 0 for the secret image and if the transformed coefficient of watermarked image is greater than the transformed coefficient of a cover image place value 1 for the secret image.

Step 5: By using above logic a binary secret image is formed.

Reason for adding a PN sequence and secret image.

Suppose consider the transformedwavelet coefficient of value 15. Following can be happen.

Table 1: A case study on PN sequence

PN-sequence	Watermark	Result (k=2)
0	0	15-0=15
0	1	15+0=15
1	0	15-2=13
1	1	15+2=17

For PN sequence 0 there will be no changes. So this will pose a greater unreliability at the time of extraction process as shown in Table 1. So add PN sequence with the secret information to eliminate this problem.

Table 2: A case study on PN sequence

PN-sequence(p)	Secret image(w)	Embedded data(p+k*w)	Result (k=2)
0	0	0+2*0	15
0	1	0+2*1	17
1	0	1+2*1	13
1	1	1+2*2	19

So if a new coefficient value is less than or equal to the old coefficient then secret image value is 0 and if the new coefficient value is greater than the old coefficient then secret image value is 1 so by this a perfect reconstruction is done as shown in Table 2.

Though a non-blind algorithm is considered but it retains the property of imperceptibility and robustness to a higher degree.The non-blind watermarking is a method extraction of the blind watermarking of a original cover image and has proved to be much more robustness.

Modulation Index

The K is a constant factor which is an important value called modulation index and it is used to determine the degree of robustness and the imperceptibility. If a value K is more then, more the transform wavelet coefficients can change a result in two situations.If there is more changes in the coefficients easier to reconstruct an extraction and is much more immune to various noise or distortions.If a coefficient aremore different than the actual one has a high qualityvisual degradation and imperceptibility be compromised.

C. PERFORMANCE EVALUATION

The analysis of the image performance using watermarking algorithm includes various metrics such as imperceptibility, robustness, the hidden capability and security are different for different situations.

1. Imperceptibility

The changes before and after the watermarking process. This is the visible changes can be measured in Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

The Mean Square Error between the watermarked image and cover imagethe is calculated using equation 9.

$$MSE=1/N\sum (I0\ [j, K] - IW\ [j, K])^2 \qquad \text{Eq 9}$$

whereN=number of pixels in each image and k =sum of all pixels in the image.

The PSNR is visually indistinguishable by human eyes of cover and the watermarked images calculated by using equation 10.

$$PSNR= 20\ \log_{20}(MAX_I/\sqrt{MSE}) \qquad \text{Eq 10}$$

2.Robustness

In watermarking scheme if the embedded secret can be detected and extracted after different types of attacks. The common attacks on a image includes filtering, compression and distortions. The robustness calculation is analysis using two different performance metrics.

The Correlation Coefficient(CC) is the resemblance between cover and watermarked image (A and B images of size m x n) according to matching their positions and measured using equation 11.

$$CC=\frac{\sum m\sum n(Amn-A\prime)(Bmn-B\prime)}{\sqrt{[\sum m\sum n(Amn-A\prime)][\sum m\sum n(Bmn-B\prime)]}} \qquad \text{Eq 11}$$

The Structure Similarity Index is measure of the similarity between 2 images measured using equation 12.

$$PSNR=20\ \log(MAX_I/[\sqrt{C((1/y)-2)}]) \qquad \text{Eq 12}$$

Where MAX_I= all pixels maximum intensity, C= hiding rate, y= robustness.

5. RESULTS AND ANALYSIS

For a embedding process an cover image is loaded and apply 4 levels of DWT with the gain factor set by the user then load the secret image.

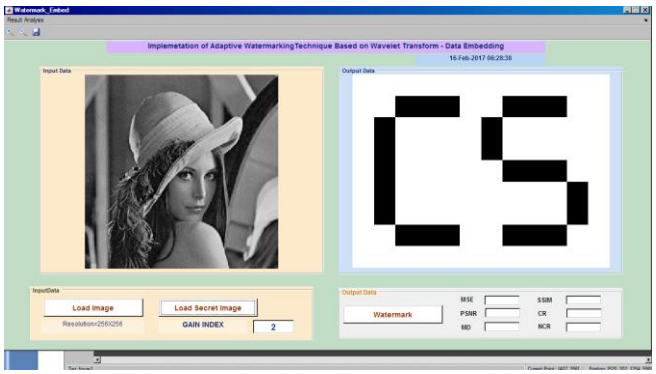

Figure 4: The cover image and secret image selected for embedding.

When the cover and secret image is loaded by the user with the K value set by the user click on watermarking button the secret image will embed in the cover image as shown in Figure 4.

Figure 5: The cover image and the watermarked image after embedding.

The Figure 5 shows the cover image and watermarked image after embedding process for different values of K. For various values of K the performance metric are measured a higher value of K more secure is the watermarking process.

For different value of K the quality measures are recorded as shown in the Table 3 and graph are shown in Figure 6, 7, 8. Figure 9 shows the histogram analysis of cover and watermarked image. By setting greater the K value the quality of image is maintained and more security is achieved. In table the quality metric is measured for different K values 2, 5, 10, 15.

Table 3: Performance metric for different values of modulation index.

Performance Metric	Modulation Index			
	K=2	K=5	K=10	K=15
MSE	0.13672	3.3359	28.8004	56.5184
PSNR	56.7725	42.8986	33.5368	30.6089
SSIM	0.99986	0.99667	0.9787	0.96298

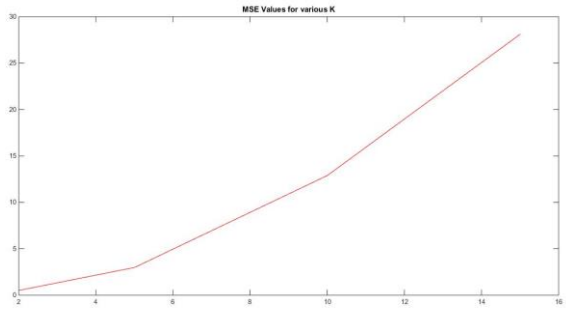

Figure 6: The Mean Square Error of cover image for different values of K.

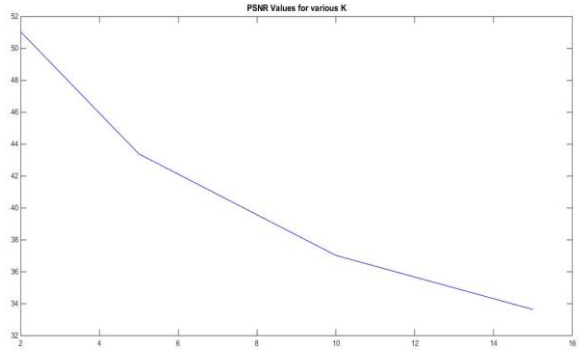

Figure 7: The Peak Signal to Noise Ratio of cover image for different values of K.

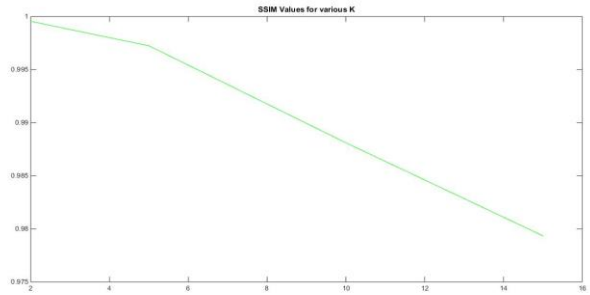

Figure 8: The SSIM of cover image for different values of K.

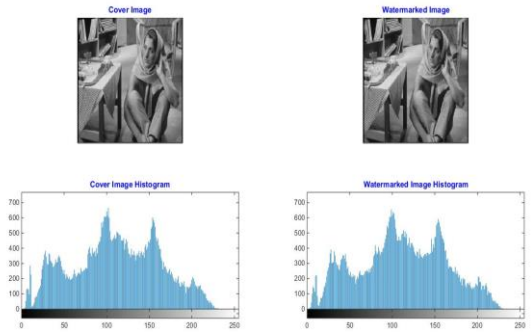

Figure 9: Histogram analysis of cover image and watermarked image.

6. CONCLUSION

In this paper a good imperceptibility, robustness is retained and immunity to different attacks is noticed. Since implementation of non-blind watermarking is used that provide a high robustness and had a perfect reconstruction at no attack. The gain factor is tuned for more imperceptibility. A biorthogonal wavelet transformation with correlation for noise differ with modulation index at unique time-frequency localization property gives the security and invisibility.

AUTHORS ACKNOWLEDGEMENT

I am thankful to my sir Darshan L.M B.E, M.TECH, assistantProfessor department of CS&E,Adichunchanagiri Institute of Technology, chikmagaluru-577102 for his consistent support and guidance.

REFERENCES

[1] ShvetiSejpal, Dr. Nikesh Shah "Performance Analysis for Authentication in Digital gray scale image using DWT domain"International Journal Scientific and Research Publications, Volume 5, Issue 12, December 2015 338 ISSN 2250-3153

[2] Ramani K., Prasad E.V, Varadarajan S.; Subramanyam A,"A Robust Watermarking Scheme of Information Hiding", Advanced Computing and Communications, 16th International Conference, 14-17 pp : 58 – 64, Dec. 2008.

[3] RavalMehul, RegePriti, "Discrete wavelet transform based on multiple watermarking schemes", Conference on convergent technologies for asia-pacific region, vol. 3, pp. 935-938, 2003.

[4] Munesh Chandra, ShikhaPandey, "A DWT Domain Visible Watermarking scheme for Digital Images", 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).

[5] Anumol Joseph, K. Anusudha, "Robust watermarking based DWT SVD", International Journal of Signal & Image Processing, Issue. 1, Vol. 1, October 2013

[6] Swapnil R. Suke, Dr.Prof. VibhaVyas, "RobustMedical Image Multiple Watermark using 4-level DWT," International Journal of Advanced Computing and Electronics Technology (IJACET)ISSN:2394-3408,VOLUME-2,ISSUE-4,2015

[7] Gupta, Raval "A robust and a secure watermarking scheme based on a singular values replacement." Indian Academy of Sciences Vol. 37, Part 4, August 2012, pp. 425–440.

[8] Santi P. Maity et. al "Design ICVG of A Robust Spread Spectrum Image Watermarking Scheme". GIP, 2011.pp 145-150.
[9] OthmanO.Khalifa et. al "Performance Evaluations of A Digital Watermarking Systems" 8th International Conference on ICIDT, Vol.3, 2012, pp 533-536.

BIOGRAPHIES

Ms. Gagana Deepa J is a student of Computer Science, Adhichunchanagiri Institute of Technology, Chikkamagaluru,pursuing M.Tech (CS) from this college. Received B.E from Adhichunchanagiri Institute of Technology, affiliated to VTU University, Chikkamagaluru in the year 2015.

Mr. Darshan L.M B.E., M.Tech., is working as assisstant professor, Department of computer science & Engineering, AIT college, Chikkamagaluru.