Grenze International Journal of Engineering and Technology, June Issue

Digital Image Watermarking using the Discrete Wavelet Transform (DWT) for Robustness

Ms Gagana Deepa J[1] and Mrs Nalini H C[2]
[1-2]Assistant Professor Dept of ISE, Rajeev Institute of Technology, Hassan, Karnataka, India
Email: Email: jgaganadeepa@gmail.com, ,nalinihc@gmail.com

***Abstract*—Using DWT, the robustness and image watermarking in the transform domain is assessed. Using a bi-orthogonal wavelet transform, the cover image has four separate layers in it. To implant a binary watermark, a gain 2 factor and a random pseudonoise sequence are utilised. A random pseudonoise sequence is added to an image's medium frequency coefficients in order to include watermark information, the inverse DWT is then used to create the watermarked image. The concealed image is extracted using the same procedures as for embedding, and then the watermarked and original image coefficients will be compared. The performance evaluation is calculated using performance metrics like robustness expressed as MSE and PSNR. The imperceptibility measures for SSIM and Mean Correlation show good imperceptibility along with greater robustness against various noise attacks.**

***Index Terms*— Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Discrete Wavelet Transform (SS IM), and Structure Similarity Index (SSIM).**

I. INTRODUCTION

Nowadays, it's simple to acquire intellectual property because to the quick growth of multimedia and the broad diffusion of digital data through an internet network. To solve this issue, employ a technique known as digital watermarking.This method entails subtly changing a cover in order to include a message related to the image. Watermarking is the process of altering original multimedia files to incorporate watermark with significant data. The embedding technique of the original data remains unchanged, and the extraction technique can be applied to identify modifications.

Since the perceived quality of the original cover image is retained, watermarking enables the inclusion of secret information in hosted multimedia without impairing its visual appeal and makes it resistant to many types of attacks. During the digital watermarking process, the two- dimensional bi-orthogonal DWT is used for embedding in the PN sequence for both safety and extraction. Metrics that include robustness and imperceptibility are used to evaluate the performance associated with the watermarking process.

For image security, numerous watermarks are inserted; depending on chosen coefficients, various watermark producers are utilized. Cover image is chosen and then made into a grayscale version for further processing.

Direct pixel values in the spatial domain along with wavelet coefficients for the domain of frequency will be used for watermarking, depending on the working domain. Because it is a simpler but less reliable process, the original data is utilised in the spatial domain instead of this watermarked data.Utilising the discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT), the original image is converted into frequency wavelets in the frequency domain. A low-pass and high-pass filter is used to separate a

Grenze ID: 01.GIJET.9.2.406

two-dimensional DWT signal into its component portions in addition to the row and column directions, as shown in Figure 1.

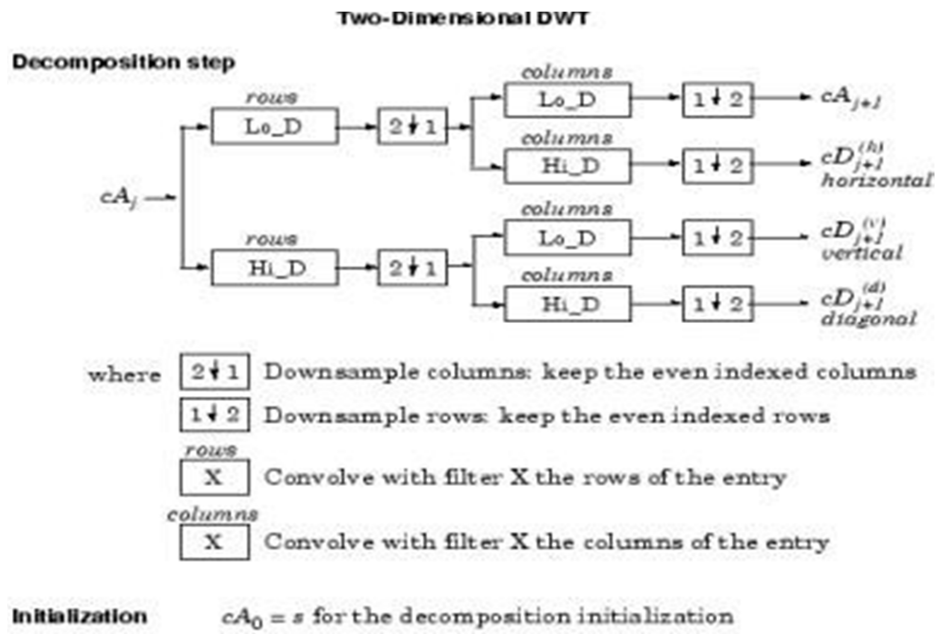

Figure 1: A 2-dimensional DWT with a single level

Any decomposition level's output is made up of four subbands, as shown in Figure 2: the initial subband (LL), three detailed subbands (LH, HL, and HH), that are referred as horizontal, vertical, and also diagonal subbands. The estimated sub-band is also used for the subsequent level of decomposition.

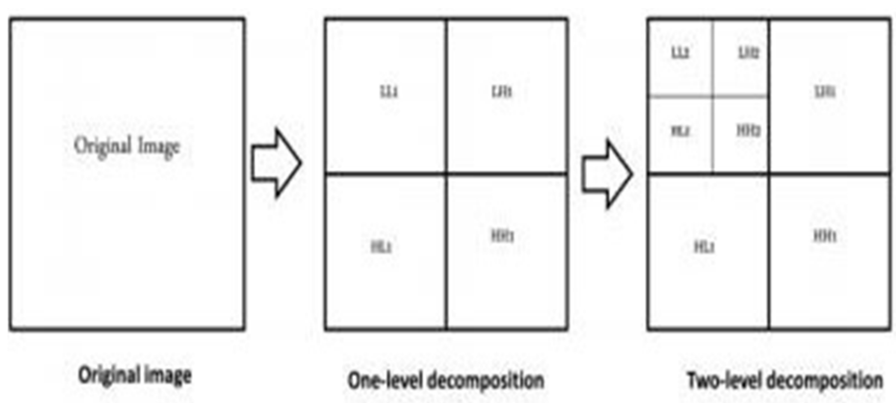

Figure 2: two-level decomposition of a two-dimensional signal using wavelet sub-bands

Since the advent of image manipulation software, it has become more difficult to distinguish an image's manipulation from its visual truth.

II. MOTIVATION

Digitization has a big impact on copyright issues, which makes it necessary to secure owners' information that is preserved in digital form. It is suggested to use digital watermarking to identify the owner and source of the content. Unlike encryption, it does not place limitations on who can view the data. Intellectual property rights have no further protection once encrypted material has been decrypted.

III. RELATED WORK

Ramani K. et al.'s[2] straightforward method, but not a safe one, uses a watermarking technique immediately. on the pixel using pseudo random generation depending on the user-provided key to take the Least Significant Bit (LSB). Digital watermarking technology based on discrete wavelet transforms has been created to address the drawbacks of this approach. The DWT multi watermarked system is built using the HH and LL sub-bands.

The integrated Watermark creates a solution has a lot of robustness on a big scale by combining the two sub-bands[3]. M. Chandra added watermark image bits to the cover image using a lower frequency range [4]. This approach is intended to be more dependable than alternatives. In order to remove the watermark afterwards, the DWT domain is purposefully used to include an invisible image inside the cover image. Images are the connected areas of a grayscale object with a similar texture. The analysis of images is best served by wavelet transforms. Sharp peaks and discontinuities in the signal are analysed using wavelet functions.

It is stated how the blind watermarking method that uses DCT-DWT and embeds a binary image within the grayscale photos leads to the DWT-DCT digital image watermarking method [1]. The watermark in the original cover image is included in the DCT blocks of the four chosen medium frequency sub-bands in the three-level DWT transformation. This outcome indicates the watermarked image is sufficiently imperceptible and that it is also resistant to the most of common noise attacks that occur during image processing.

IV. METHODOLOGY

A. DWT's Bi-Orthogonal Wavelet Transform

Using this method, the initial image intensities are transformed into coefficients. The process for converting a watermarked image to a marked image. The most effective transformation is DWT because it tells you the signal's frequency, amplitude, and application time. The orthogonal basis of a vector space is a wavelet. Two among the orthogonal functions which make up the basis set of the wavelet are the scaling function and the wavelet function. The translation and scaling of the two functions have been completed. The wavelets basis set consists of one scaling function with the wavelet functions shown in equation 1. The wavelet contains the difference information, while the scaling function contains the signal's average information.

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

The DWT function's coefficients are written as C_K, d_{jK}.

Equation 3 is used to represent fluctuations at different scales (LH, HL, and HH), while equation 2 is applied for describing an average component of the signal's details (LL). These are the traits that all wavelets share.

$$C_K = \int f(t)\varphi_K(t)\,dt \qquad \text{Eq 2}$$

$$d_{jK} = \int f(t)\psi_{jK}(t)\,dt \qquad \text{Eq 3}$$

Within each wavelet, there are different sub classes of wavelets dependent on the number of the coefficient values and the level of iteration. Decomposition of a two-dimensional, single-level wavelet.

For certain filters, including low pass or high pass, the estimated and complete coefficient matrices are computed using equations 4, 5, 6, and 7.

$$\Phi(t)=\sqrt{2}\sum_{n=-\infty}^{\infty} h[n]\varphi(2t-n) \qquad \text{Eq 4}$$

$$\Phi'(t)=\sqrt{2}\sum_{n=-\infty}^{\infty} h[n]\varphi'(2t-n) \qquad \text{Eq 5}$$

$$\psi(t)=\sqrt{2}\sum_{n=-\infty}^{\infty} h[n]\psi(2t-n) \qquad \text{Eq 6}$$

$$\psi'(t)=\sqrt{2}\sum_{n=-\infty}^{\infty} h[n]\psi'(2t-n) \qquad \text{Eq 7}$$

The DWT of a cover image is calculated to determine the robustness of the watermarking procedure. If the data is placed on a lower frequency band, data loss is possible; but, if the data is embedded within a higher frequency band, attack is far more likely. A medium frequency range of frequencies are hence selected for the hidden picture embedding. As shown in Figure 3, the secret image is placed into the fourth level in the cover image for security and robustness.

The medium range of frequencies is therefore selected for the secret image embedding and, as displayed in Figure 3, the secret image is added into the fourth level of the cover image for the security and robustness. The DWT within the cover image is calculated to assess the robustness of the watermarking process. If the data is inserted in a lower frequency band, data loss is possible. Additionally, if the data is inserted in a higher frequency band, attack is much more likely to occur.

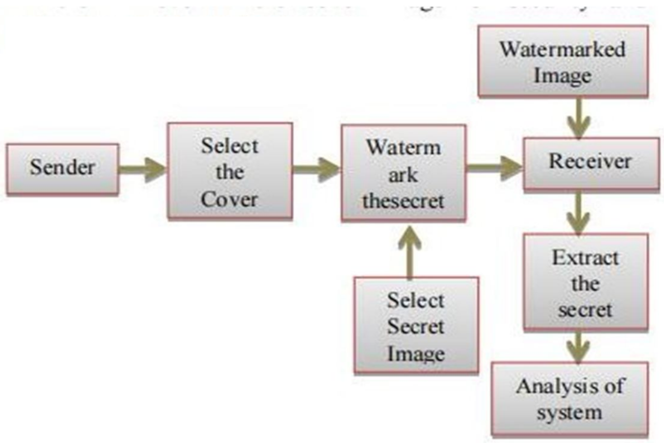

Figure 3: Architecture diagram of watermarking using DWT

B. Algorithm

Embedding Method

The suggested work does the following by embedding a cover image with a secret image using the DWT.

Step 1: Take into account the 256x256 grayscale cover image.

To obtain the wavelet coefficients as a matrix reflecting the estimated horizontal, vertical, and diagonal qualities as LL4, LH4, HL4, and HH4 sub-bands of size 16x16, conduct a 2-dimensional biorthogonal DWT across 4 levels in step 1.

Step 2: Produce a 16x16 random binary pseudonoise sequence. Step 3. Take into consideration the 16x16 binary secret image.

Add a binary pseudonoise sequence with a binary secret image for every distinctive element Step 4: The following information will be the last to be included.

Step 5: The total amount of the final embed data is multiplied by a predefined factor K to form a new wavelet coefficient matrix if the newly inserted binary watermark value is 1. The final embed matrix less the newly added wavelet coefficient matrix has been multiplied with a constant factor K if the additional binary watermark value is 0.

Step 6: To improve imperceptibility, change the midrange bands—the LH and HL subbands— using the justification provided. Consequently, the LH and HL bands have coefficients with watermarks.

Step 7: Using the same wavelet but with new values for the wavelet coefficients, perform an inverse two-dimensional DWT for 4 levels. A watermarked image is created as a result.

Extraction Method

The following is the procedure for extracting the hidden image from the watermarked image:

Step 1: Take into account the watermarked image and perform two-dimensional DWT using the identical embedding-related wavelet transform for the four levels

Step 2: Using the same wavelet transform, perform a two-dimensional DWT with four levels while taking into account the original cover image.

Step 3: Then examine the wavelet coefficients in the original and watermarked images, both of which were of equal length.

Step 4: Enter a value of 0 to the secret image if a watermarked image's transformed coefficient is less than or equal to the cover image's transformed coefficient, and a value of 1 if a watermarked image's transformed coefficient is higher than the cover image's transformed coefficient.

Step 5: Using the previously given reasoning, a binary secret image will be generated.

The reason that is a PN sequence with secret image added.

Consider the following if the modified wavelet coefficient is at a value of 15.

There won't be any changes to PN sequence 0. Therefore, as demonstrated in Table 1, this will present a greater level of unreliability during the extraction process. To solve this issue, include PN sequence together with a secret information.

TABLE I: 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

TABLE II: A PN SEQUENCE CASE STUDY

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

The hidden image value is zero if the new coefficient value is equal to or less than the previous coefficient, and one if the new coefficient value exceeds the old coefficient The perfect reconstruction produced by this technique is displayed in Table II.

It nevertheless maintains a higher level of imperceptibility and robustness even when a non-blind algorithm has been taken into account. The blind watermarking within an original cover image has proven to be far less accurate than the non-blind method.

Modulation Index

The level of imperceptibility and robustness is determined using the modulation index, a fundamental variable known as the K constant factor.The result may be altered in one of two ways by the wavelet coefficients of the transformation if K is greater.It is significantly simpler to repeat an extraction and much more resistant to varied noise or distortions if there have greater variations in the coefficients Visual quality along with imperceptibility both decrease when a coefficient deviates greatly from the genuine one.

C. Performance Evaluation

The analysis of watermarking algorithm's performance on an image takes into account a variety of variables, including security, resilience, imperceptibility, and hidden capabilities.

Imperceptibility

the variations between the watermarking process and prior.

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) measurements show these to be the visible variations.

The Mean Square Error over the cover image as well as the watermarked image is calculated using Equation 9.

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

where N is the number of pixels contained within each image and k is the total amount of pixels within the image.

For human eyes, the calculated PSNR from Equation 10 is equal to the watermarked images and the cover.

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

Robustness

When the embedded secret in a watermarking technique can be found and extracted after various forms of attacks. Filtering, compression, and distortions are frequent attacks on images. Analysis of the resilience is done using two separate performance criteria.

A measure of the resemblance between a cover image and a watermarked image (A and B pictures of size m x n) based on comparing their positions is called the correlation coefficient (CC).

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

The Structure Similarity Index uses equation 12 to calculate how similar the two images are to one another.

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

Where MAXI = maximum intensity across all pixels, C = hiding rate, and y = robustness.

V. RESULTS AND ANALYSIS

For an embedding procedure, a cover image is loaded, followed by the secret image and four levels of DWT along with the user-specified gain factor.

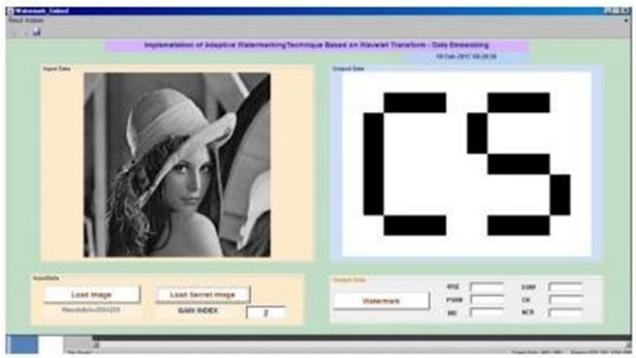

Figure 4: A cover image as well as secret image that were chosen for embedding

The secret picture is included into the cover image when the user hits the watermarking icon after importing the cover and secret images using the K value they've set, as seen in Figure 4.

Figure 5: The embedded cover image and watermarked image

Following the embedding process for different K values, the cover image as well as the watermarked image are shown in Figure 5.

Performance metrics are measured for different K values; the greater the K value, the more secure the watermarking process is.

The graphs in Figure 6, 7, and 8 show the quality metrics for the different values of K that have been recorded. Figure 9 shows the histogram analysis for the watermarked and cover image. More security is attained and image quality is maintained by increasing the K value. The quality metric is calculated for several K values in the table, including 2, 5, 10, and 15.

Performance metrics for various modulation index values are shown in Table III.

TABLE III: PERFORMANCE METRIC WITH INDEX VALUE

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

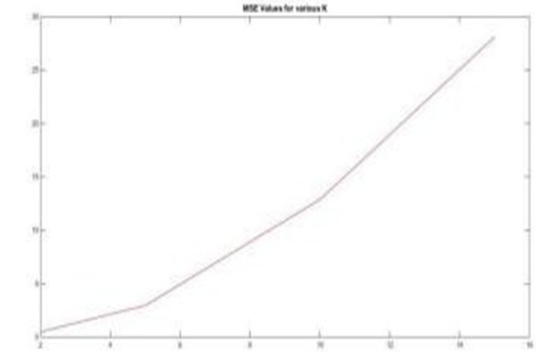

Figure 6: Shows the cover image's Mean Square Error for various K values

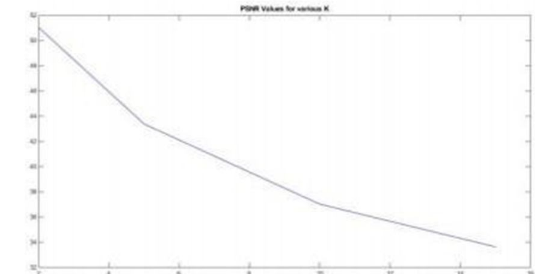

Figure 7: Shows the cover image's peak signal to noise ratio for various levels of K

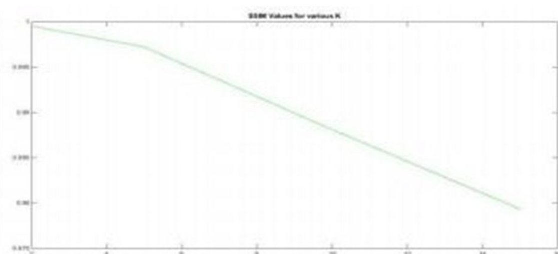

Figure 8: Shows the SSIM of the cover image for various K values

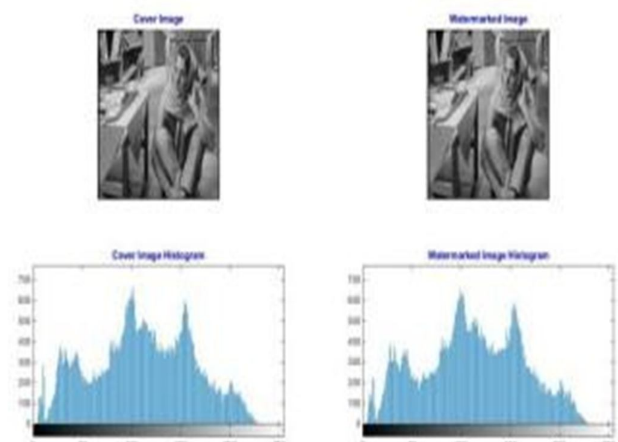

Figure 9: Analysis of the cover image's histogram and the watermarked image

VI. CONCLUSION

This study emphasises a strong imperceptibility, robustness, and immunity to many hazards. It was done using non-blind watermarking, which offers a high level of robustness and has a complete reconstruction under no attack. It's been altered to make it less perceptible. Security and invisibility are provided by a biorthogonal wavelet transformation and correlation for noise that varies with modulation index at particular time-frequency localization features.

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.