

Combined DWT-DISB based image watermarking optimized for decision making problems

Ghassan N. Mohammed¹, Ahmed Abdul Hassan Al-Fatlawi², Ahmed Talal Kamil³

¹ Department of planning & studies, Ministry of Higher Education, Iraq

² Department of informatics system management, businesses informatics college, university of information technology and communications

³ Departement of Computer engineering, Engineering college, Aliraqia University

Article Info

Received Jul 15, 2019

Keyword:

Discrete Wavelet Transform
Robust
DISB
Digital Data
Watermarking
Imperceptibility

ABSTRACT

Currently, the protection of digital information, especially in the form of multimedia information such as images, video, text, and audio. The digital nature of the multimedia data has made it prone to misuse and attack, such as is of duplication, transformation, modification, and diffusion. In this sense, it is significant to create a system for protecting the intellectual property rights of the multimedia content. The system should guarantee copyright protection, authentication, and protection against duplication of the material. The drastic development in network multimedia system has made the development of these protection systems challenging. Numerous researches have proposed the use of watermarking to address these issues. The watermarking technique obscures vital information in the original multimedia data in which the hidden data is utilized for copyright protection and authentication. The primary need for any watermarking system should be to guarantee robustness against imminent attack while retaining the quality of the watermark images. This research presents a robust image watermarking technique used to hide details of the RGB Color elements. The proposed approach is an integration of the discrete wavelet transform (DWT) and the relatively new dual intermediate significant bit (DISB). The performance evaluation of the proposed approach produced quality watermarked images that are robust. The proposed method has a PSNR of 101.97 and an NCC of 0.9780 which compare considerable well with the individual techniques.

Corresponding Author:

Ghassan N. Mohammed¹
Department of planning & studies,
Ministry of Higher Education, Iraq.
Email: ghanm1971@yahoo.com

1. Introduction

The widespread use of digital multimedia data and processing tools has made image processing easy for the ordinary person who can obtain and modify the contents of images and other multimedia data [1]. Authentication of these digital data has thus become challenging to the content creator and the custodians. Generally, the digital watermarking skills can be categorized into two wide categories based on various application scenarios; fragile and robust watermarking [2]. In fragile watermarking techniques, the digital data is still susceptible to any form of modification; hence, are often applied in digital data tamper detection and restoration [1]. On the contrary, the robust watermarking approach is resistant to the standard form of attacks, and therefore, it is desired to use incorporate protection of digital data. The robust watermarking scheme is desired for watermarking for copyright protection because it guarantees imperceptibility and robustness [2]. In the robust watermark approach, the watermarked image or digital data can be easily extracted even from those

distorted attack. In the case of imperceptibility, the quality of the watermark image cannot be strongly affected, i.e., cannot be visibly observed by the naked eye. A watermark can be described as a recognizable pattern on an image, or a paper that appears has different shades of darkness or lightness when viewed against transmitted light, i.e., reflected light or a dark background [3]. Initially watermarks or produced by a mechanical process such as the complex cylinder mold and dandy roll process. Watermarks have been used over the years to improve the security characteristics of postage stamps, passports, banknotes, and other sensitive documents to curb counterfeiting [4]. Further, watermarks have been used in examination papers as they could provide dating, milling trademark, identification size, quality of paper, and locations [1]. Over the last decade, billions of multimedia data have been created which are easily copied and altered, increasing the need to protect the material and prove ownership. Digital watermarking has emerged as an approach for securing content and overcoming the shortfalls of the current copyright laws with regard to digital data. In digital watermarking, the specificity of the inscription should be that it retained intact covering the text even when copied or during transmission. Moreover, to prove the ownership of certain content, the watermark is traditionally removed, i.e., and tested [5]. Studies have proven that it is difficult for counterfeiters, cybercriminals, and malicious actors to remove and alter watermarks. Therefore, this gives the owner of the information autonomy over their content as well as safety and security [6]. Counterfeiters also attack the digital content, thus degrading its quality, but it has been proven that attacking watermarked images or videos becomes very difficult, especially in recovering the watermark. In case, the watermark has successfully extracted the counterfeiters cannot use it to prove ownership of the digital content.

In digital image watermarking techniques, the watermark was implanted in the information-carrying image [7]. Ideally it has been the practice that there is no discernible distinction between the watermarked and initial host image, and the watermark should be arduous to alter or extract without the decrease in the quality of the host image [8]. The watermark may be a binary sequence representation of a logo, serial number, signature, picture or a credit card number. In most cases, the watermark is used to prove ownership and secure the content of an image. The popularity of digital watermarking has increased with the proliferation of the internet as a crucial requirement for data security. Generally, watermarking entails watermark embedding and extraction [9]. The implanting process is performed by modification of the image features such as transform domain coefficients or luminance values. The selection of the coefficients is reliant on the perpetual criteria and the key instrumented permutation to increase the security and the robustness of the approaches used. Inserting of the watermark can be accomplished on an image independent or dependent additive manner or a variant of substitution mechanism [10]. Prior to divulging into the details of the proposed watermarking model it is vital to understand the bit-plane that characterizes the image.

The image bit-plane

The bit-plane of digital images describes a series of bits that occupy a similar location with regard to the relevant binary numbers. Traditionally, in grayscale images, has 8 bit-planes, where the first bit-plane is composed of the most significant bits (MSB) of the image whereas the 8th plane includes the least significant bits (LSB) [11]. The planes located in between are referred to as the intermediate significant bits (ISB), i.e., 2nd to 7th. Fig 1 below shows the location of each bit plane and the related pixel plane.

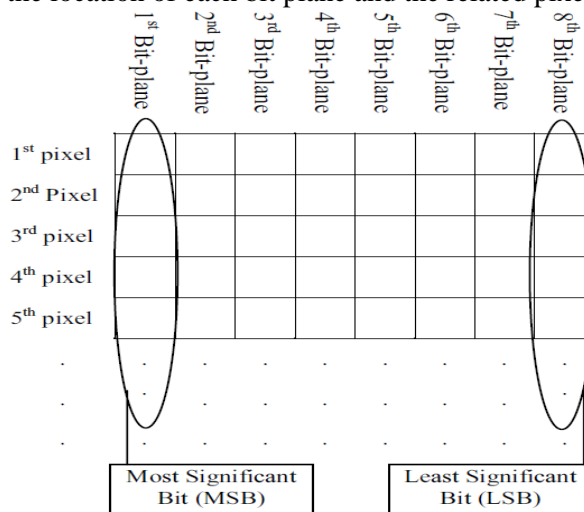


Figure 1. The bi-plane of the digital images

The value of the respective bits on the plane can be represented using the following notation 2^{n-1} where n denotes the order of the plane, i.e., 1-8 [11]. Using the notation above the bits add up to 255 as illustrated below.

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 = 255$$

The above computation shows that the maximum value that can fit in the 8 bits in the plane is 255 whereas the smallest value was 0. Modification of the 8 bit-plane results in the alteration of the pixel values in accordance with table 1 below [12]. When the alteration pixel value is minimal, the quality of the image was maintained at a very high value. In case, the change value is huge; then the image quality would be significantly degraded.

Table 1: The effect of modifying the 8 bit-plane

Bit position	Change in the pixel value
8 th bit-plane	± 1
7 th bit-plane	± 2
6 th bit-plane	± 4
5 th bit-plane	± 8
4 th bit-plane	± 16
3 rd bit-plane	± 32
2 nd bit-plane	± 64
1 st bit-plane	± 128

In this research, we aim to combine the discrete wavelet transform (DWT) and the relatively new dual intermediate significant bit (DISB) [11]. The combination of these two techniques would be aimed at enhancing the quality and the resilient of the watermarked image [10]. The combination of the DISB would alter the intermediate significant bits for the low-frequency approximation in the DWT domain for embedding the watermark in the image [11]. This combination applied the spatial and robust scheme which would enhance the undetectability, optimize the embedding of the watermark and security.

2. Related work

The most common classifications for the image watermarking are the frequency and spatial domain. This study evaluated the application of a robust approach for digital image watermarking in the frequency realm. The research would deal with a photo in the frequency dominion, which is watermarked at the varying potency in the intermediate subcategories [2]. The research compares the PSNR acquire from the combination of the two approaches with those obtained from individual techniques. The watermark was implanted in the image in the frequency section. Similarly, the watermark was extricated from the watermarked image to leave the host image, which can be accomplished by the intended user using a key from the sender [2]. This exercise prevented eavesdropping via extraction of information embedded in the watermark. Furthermore, the robustness of the technique was evaluated using the pseudo-random noise and NCC techniques. The first step was to assess the background of the two technologies and the essence of each in creating a robust technique [3].

2.1. Frequency domain

The image is a two-dimensional matrix of pixels in the spatial domain which is applicable in the signal processing domain. However, the array can be transformed into the frequency realm via the manipulation of the frequency domain representation or the use of the Fourier transform of the image [2]. In the frequency section, the image is represented using the frequency components such as the summation or superposition of the sinusoidal components [2]. The frequency representation of the image is in the form of spectrums. The DWT is a form of wave transformation of the image watermarking approaches.

2.1.1. Discrete wavelet transform (DWT)

In both functional and numerical analysis, the DWT describes a wavelet transformation where the waves are discreetly appraised [13]. DWT as a frequency domain technique has a key benefit over Fourier transform as it is capable of secular resolution, i.e., it records the location and frequency data [4]. The DWT is widely applicable in mathematics, computer science, science, and engineering. The DWT has been notably you for

signal coding in the representation of a discontinuous signal in more superfluous cases or as prerequisite for data compression [8]. In digital communication, the DWT of a signal x can be computed using a concatenation of filters. Initially, the samples are relayed via a low pass filter with impulse response y leading to a convolution defined as;

$$y|n| = (x \times g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n - k]$$

This signal was also decomposed simultaneously via the use of a high pass filter h [13]. The resultant outputs were the comprehensive and approximation coefficients [3]. The two filters must be correlated and are known as quadrature mirror filter based on Nyquist’s rule.

$$y_{low}|n| = (x \times g)[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n - k]$$

$$y_{high}|n| = (x \times g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n - k]$$

Where

x is the processing signal

y is the impulse response

The decomposition of the signal divides it into two the time resolution as half of the product of the filter formed part of the signal [14]. Nonetheless, the output would have half of the frequency cord of the input; thus, the frequency resolution was doubled for the sampled signal. Figure 2 below shows the filter analysis in DWT.

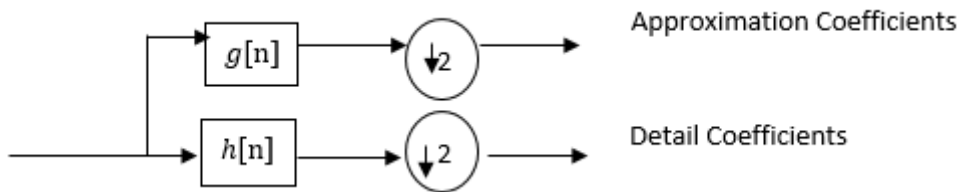


Figure 2. the filter analysis in DWT

Using the sub sampling operator \downarrow the expression for this section becomes

$$(y \downarrow k)[n] = y [kn]$$

The summation above can be summarized as

$$y_{low} = (x \times g) \downarrow 2$$

$$y_{high} = (x \times g) \downarrow 2$$

The downside to the DWT technique is that the computation of the complete convolution using the expression $(x \times g)$ waste a considerable amount of time [4]. The above analysis has shown that the wavelet transform is a multiscale signal analysis that employs Fourier transform fixed resolution approach for local signal analysis thus making it an ideal technique for signal processing and frequency analysis [3].

2.2. Dual intermediate significant bit (DISB)

The DISB is a relatively new watermarking model put across by Zeki et al. The technique considers the bit-plane in the digital images as a sequence of bits that have the paired location in the binary plane [5]. The intermediate bits, as noted earlier, are the bits that occur between the MSB and the LSB, i.e., 2nd to 7th-bit planes [1]. In ISB approaches the watermark is constantly repeated for a specific amount of time in the efforts to enhance the resistance of the watermarking technique [1]. This technique is primarily effective in watermark detection; thus, its algorithms are more resistant, especially in the case of geometrical transformation attacks. Further, the DISB enhances the quality of the watermarked image via the implantation of two bits into the respective pixel of the host image [11]. The remaining six bits are altered so that they can directly integrate the initial pixels. The approach creates high caliber watermarked images [12]. The embedding process commences with the preference of two bit-planes, i.e., 1 to 8, which are then denoted as (k_1, k_2) . The embedding process is expressed as.

$$L_{range} = 2K_2$$

Where the process is distinguished into periods where period one is located on the left, whereas period two on the right. Additionally, the duration of each period can be captured by dividing the scope by two.

$$L_{period} = \frac{L_{range}}{2}$$

The number of ranges (N) can be captured via the division of 256 by the length of the scope as shown below.

$$N = \frac{256}{L}$$

The computed implanted bits would be b_1 and b_2 which would be embedded into k_1 and k_2 respectively. The bit planes k_1 and k_2 was represented by Yk_1 and Yk_2 respectively in the binary numbers.

3. Proposed method

The DISB was used for embedding the image, enhancing the quality and the resilience of the watermarked image [3]. Alternatively, the DWT approach was used for the computation of the low-frequency variation of the ISB via the approximation of the low-frequency sequence (LL) [5]. The conventional design of DISB was used for the embedding process with the following ranges of the bit plane being utilized.

Table 2: The Ranges computed for each bit-plane

Bit-Plane	Number of the ranges (N)	Size of the Range (L)	Sample Ranges
1	2	128	0-128, 128-255
2	4	64	0-63, ..., 192-255
3	8	32	0-32, ..., 224-255
4	16	16	0-15, ..., 240-255
5	32	8	0-8, ..., 248-255
6	64	4	0-3, ..., 252-255
7	128	2	0-1, ..., 254-255
8	256	1	0,1,2, ..., 255

3.1. Embedding process

The embedding was completed for all the bit-planes using the bias values (X), which was vital for every embedding, quality, and resilience of the watermarked image [11]. The robustness of the DISB method was enhanced by applying the data encryption standard (DES) for securing the shared key [10]. The DWT technique was used to determine the number of alterations to be applied to be able to scramble the data and secure the data in the image [5]. The embedding position and the pixel bits for the host image would be determined randomly.

To substantiate the robustness of the proposed approach, the normalized cross-correlation (NCC) was used. NCC is a vital behavior parameter employed in extraction modules and is defined in the equation below.

$$NCC = \frac{\sum_x \sum_y W(x, y)W'(x, y)}{\sum_x \sum_y [W(x, y)]^2}$$

Where, $W(x, y)$ is the initial watermark image, $W'(x, y)$ is the extricated watermark image.

Table 3 below illustrated the various attack mechanism that were employed to analyze the robustness of the proposed method.

Attack Index	Parameter	Values
Salt and Paper Noise	Mean	0.005, 0.01
Gaussian Noise	Mean	(0,0.01)(0,0.005)
Scaling (Translation)	Displacement	(0.5,2)(2,0.5)
Filtering	Median, Average	(3x3)(5x5)
Brightness	Proportion	+50 +100

The caliber of the generated watermarked image was assessed using the peak signal to noise ratio (PSNR) as described in the equation below. An image is admissible to the human vision if the PSNR is higher than 30 dB [3]. A larger PSNR would mean a higher image quality.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{\frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (\alpha_{ij} - \beta_{ij})^2} \right) dB$$

Where

α_{ij} is the pixel of the original image

β_{ij} is the pixel of the watermarked image

(i, j) is the coordinates for the original image

(m, n) is the coordinates of the watermarked image

3.1.1. Embedding algorithm process

1. Color space transformation was implemented to the host image to alter the format from the conventional RGB to YIQ [14]. The luminosity component was extracted for element Y of the image. Further, the element (Y) was decomposed using the multi-level DWT technique for the low frequency sub-bands approximation maps (LL) as shown in figure below.

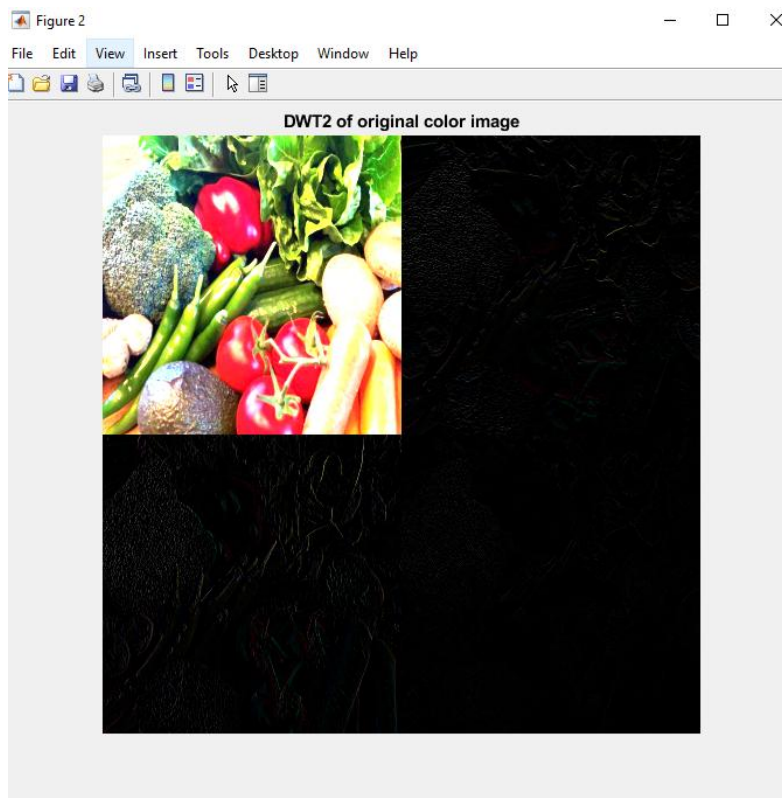


Figure 2. The result of performing multi-level DWT on the original image

2. DISB was performed on the sub bands that were created in step 1 above leading to creation of corresponding singular values.
3. Transformation was applied (τ) times on the watermarked image and then decomposed further by the application of single-level DWT to generate an LL or low frequency estimation sub-map.
4. The resultant singular values were modified in correspondence with the luminance element Y formed on the matrix coordinates of the watermarked image.
5. The component Y is combined with the YIQ design of the host image and then transformed to RGB to obtain the watermarked color image of the original image.

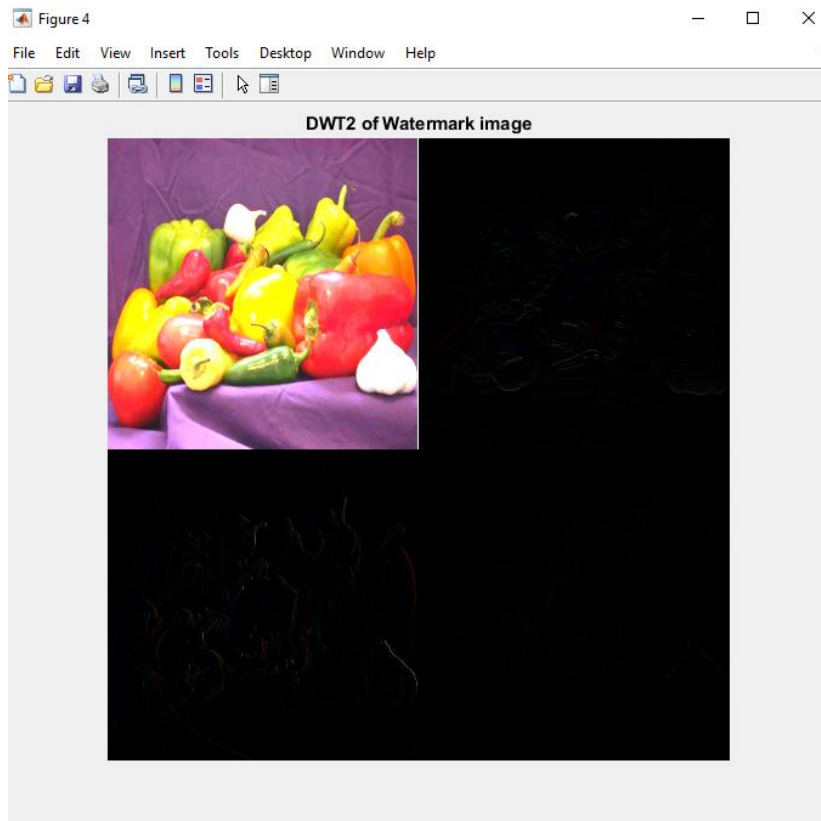


Figure 3: The result of performing multi-level DWT on the watermark image

3.1.2. Extraction algorithm process

1. The first two steps were similar to step 1 and 2 of the inserting process which was applied on the watermarked image that was decomposed into the arrays.

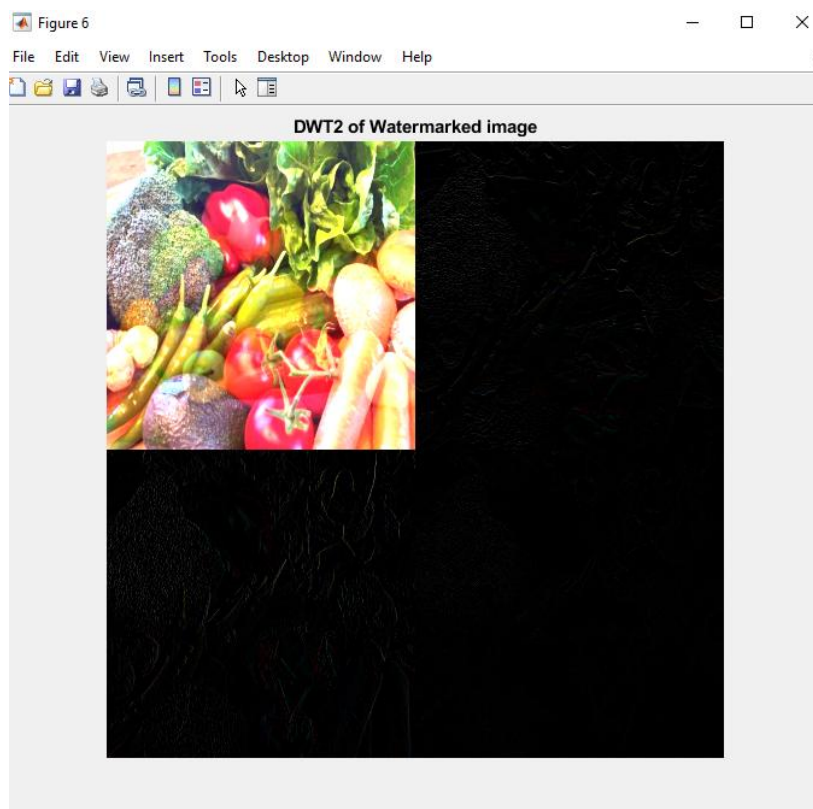




Figure 4: The result of performing multi-level DWT on the watermarked image

2. A modification corresponding to the singular value was completed with regards to the luminance component Y with an attack matrix being applied to create a new combined matrix while maintaining the scaling factor.
3. A single-level DWT was implemented on the new combined matrix then attacked by a specific image processing technique.
4. Transformation was used several $(T - \tau)$ times where T is the scrambling cycle to obtained the extracted watermarked image.

3.2. Designing of the technique

As earlier stated, the watermark was inserted in all the bit-planes of the original image. The NCC evaluation demonstrated that the robustness of the technique was resistant to the geometric attack [1]. The host and the watermarked image were downloaded from google bearing the following parameters.

Table 4: The parameters of the images used in the watermarking processes.

Role	Image	Parameters
Host		512x512 pixels
Watermark Image		512x512 pixels

4. Results

This part presents the simulation results of the several tests conducted on the proposed method to evaluate the quality and the resilience of the technique. The proposed model was implemented in the frequency domain with adequate distribution of details throughout the entire image. Both the host and the watermark images had 512x512 pixels.

4.1. Quality analysis

The PSNR was used for the evaluation of the image quality thus replacing the dimensions of the images into the PSNR equation defined above we obtained.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{\frac{1}{512 \times 512} \sum_{i=0}^{512} \sum_{j=0}^{512} (\alpha_{ij} - \beta_{ij})} \right) dB$$

The higher the value for the PSNR the greater the quality of the watermarked image [12]. The quality of the extracted watermark was compared with the original watermark as shown in figure 2 and 3 below

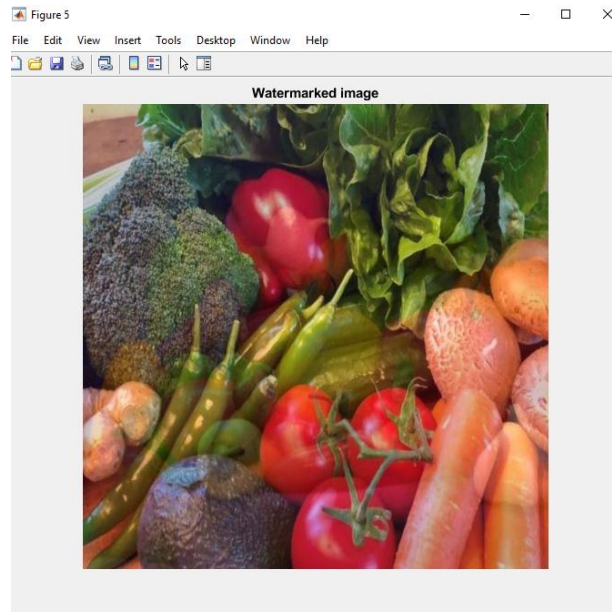


Figure 5: The watermark image that was created via the combination of the DWT-DSB technique.

The watermark image was inserted in the host image resulting the image above [2]. The changes and modification led to the improvement of the quality and the preservation of the initial image.

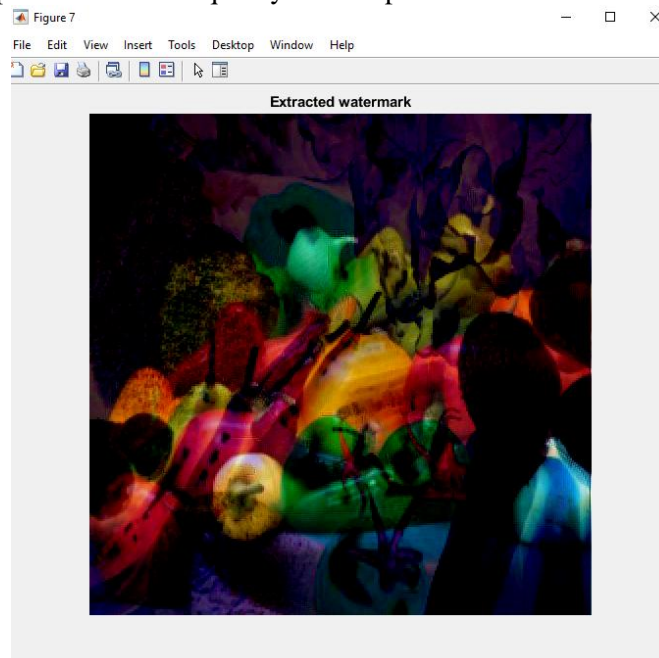


Figure 6. The extracted watermarked image from the host to compare the quality.

The extracted watermark was produced through the extraction process developed earlier [15]. The results for the analysis were compared inform of the PSNR to determine the performance of the proposed model against the other techniques. Table 5 demonstrate the comparison between the watermark and the extricated watermarked image.

Table 5: Results for the comparative analysis of watermark image and the extracted image

Parameter	DISB	DWT	Proposed Method
Watermark Image	Binary	Binary	Binary
PSNR (dB)	67.89	97.86	101.97
Capacity	32x32x4	32x32x2	32x32x2
NCC	1	0.9605	0.9824

4.2. Robustness evaluation

The robustness of the implemented technique was evaluated using multiple signal processing attacks that were applied on the watermarked image [16-18]. The attacks in table 3 were applied to the three techniques for comparative analysis. Furthermore, the value for NCC was recorded for the extricated watermarks under various signal breaches.

Table 6: The computed NCC parameters for the extricated watermarks under various attacks

Attack Index	Parameters	DISB	DWT	Proposed Method
Salt and Paper Noise	(0.005)	0.9678	0.9993	0.9988
Salt and Paper Noise	(0.01)	0.9158	0.9899	0.9958
Gaussian Noise	(0,0.01)	0.9995	0.8235	0.9992
Gaussian Noise	(0,0.005)	1	0.8706	0.9988
Scaling (Translation)	(0.5,2)	0.9103	0.9612	0.9687
Scaling (Translation)	(2,0.5)	0.9320	0.9601	0.9798
Filtering (Median)	(3x3)	0.9213	0.9524	0.9793
Filtering (Median)	(5x5)	0.8610	0.9623	0.9789
Filtering (Average)	(3x3)	0.8978	0.9739	0.9712
Filtering (Average)	(5x5)	0.8165	0.9658	0.9609
Brightness	+50	1	0.9667	0.9741
Brightness	+100	0.7589	0.9602	0.9707

The NCC values recorded above are averages of multiple iterations due to the randomness of the noise in the attacks. The values obtained for the NCC are typically greater or equal to those recorded for the independent DISB and DWT methods [3]. The NCC values in the experiment showed stability with the varying attack intensities. The above results have demonstrated that the proposed approach is considerably robust compared to the individual schemes.

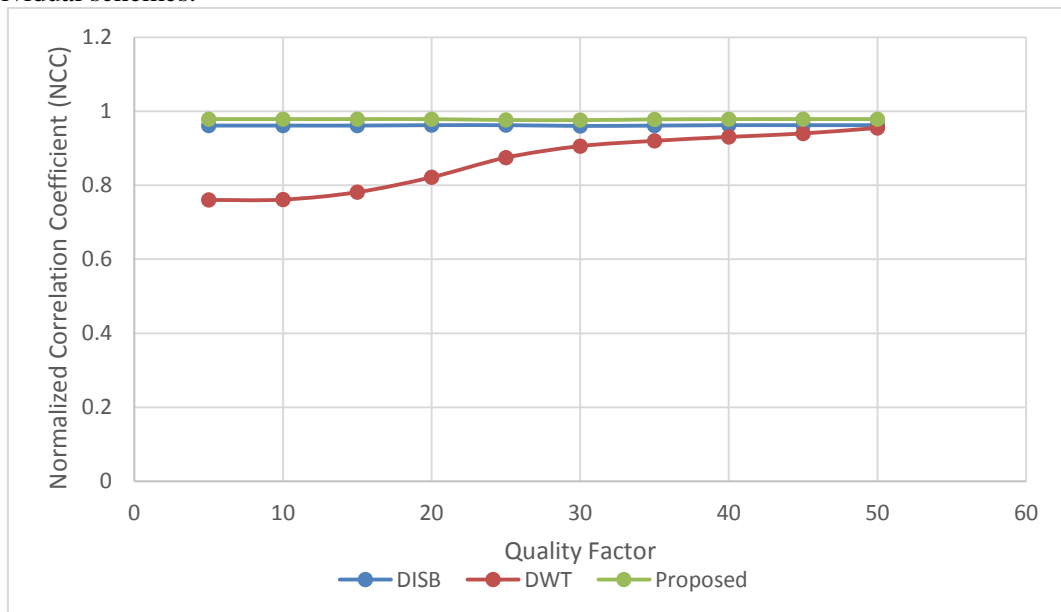


Figure 7. Comparative analysis for the different method NCC values for the various quality factors

The NCC values for different quality factors were used for comparative analysis. The data illustrated stability in the robustness and quality attained by each technique. The Proposed method achieved a mean NCC value of 0.9780 compared to 0.8649 and 0.9617 for DWT and DISB, respectively.

5. Conclusion

This study has presented a new technique that is a combination of the DISB and DWT in the frequency realm. The method has been proven to be a formidable watermarking algorithm. The proposed method utilizes the low-frequency accumulation of DWT to decrease the effect of watermark on implanting. The DISB component of the proposed approach ensures the quality of the watermarking via alteration of the ISB and robustness of the technique by introducing resistance to a variety of signal processing attacks.

References

- [1] S. E. Kaur and P. Matharu, "Robust Image Watermarking Based on Dual Intermediate Significant Bit (DISB) Invariant to Rotation, Scaling and Translation," *International Journal of Recent Research in Mathematics Computer Science and Information Technology*, vol. 3, no. 1, pp. 51-57, 2016.
- [2] X. Cui, Y. Niu, X. Zheng, and Y. Han, "An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image," *Plos One*, vol. 13, no. 5, p. e0196306, 2018.
- [3] X. Zhou, H. Zhang and C. Wang, "A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD," *Symmetry*, vol. 10, no. 77, pp. 1-14, 2018.
- [4] P. Kaushik, "Digital Image Watermarking using BFO Optimized DWT and DCT," *International Journal of Enhanced Research in Science Technology & Engineering*, vol. 3, no. 10, pp. 57-61, 2014.
- [5] A. M. Zeki and A. A. Manaf, "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit)," *World Academy of Science, Engineering and Technology*, no. 50, pp. 989-996, 2009.
- [6] R. K. Singh, D. K. Shaw and J. Sahoo, "A secure and robust block based DWT-SVD image watermarking approach," *Journal of Information and Optimization Sciences*, vol. 38, no. 6, pp. 911-925, 2017.
- [7] D. G. Savakar and A. Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3995-4008, 2019.
- [8] C.-C. Lai and C.-C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060 - 3063, 2010.
- [9] H. Lala, "Digital Image Watermarking using Discrete Wavelet Transform," *International Research Journal of Engineering and Technology*, vol. 4, no. 1, pp. 1682-1685, 2017.
- [10] M. Gupta, G. Parmar, R. Gupta, and M. Saraswat, "Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony," *International Journal of Computational Intelligence Systems*, vol. 8, no. 2, pp. 364-380, 2015.
- [11] A. Sharifara, G. Bin Sulong, and M. R. Seraydashti, "Digital Image Watermarking Using Different Levels of Intermediate Significant Bits with Zig-zag Embedding Approach," *International Journal of Image Processing*, vol. 7, no. 1, pp. 62-71, 2013.
- [12] A. U. Rahman, K. Sultan, D. Musleh, N. Aldhafferi, A. Alqahtani and M. Mahmud, "Robust and Fragile Medical Image Watermarking: A Joint Venture of Coding and Chaos Theories," *Journal of Healthcare Engineering*, vol. 2018, no. 8137436, pp. 1-11, 2018.
- [13] M. Haribabu, H. Bindu and V. K. Swamy, "A Secure & Invisible Image Watermarking Scheme Based on Wavelet Transform in HSI Color Space," *Procedia Computer Science*, vol. 93, pp. 462-468, 2016.
- [14] S. A. Parah, J. A. Sheikh, U. I. Assad, and G. M. Bhat, "Realisation and robustness evaluation of a blind spatial domain watermarking technique," *International Journal of Electronics*, vol. 104, no. 4, pp. 659-672, 2017.
- [15] A. Abbasi and W. C. Seng, "Robust Image Watermarking Using Genetic Programming," *Journal of Software and Systems Development*, vol. 2012, pp. 1-9, 2012.

- [16] N. Sinha and S. Gupta, "Digital Image Watermarking in Special and Frequency Domain," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 9, no. 6, 2019.
- [17] Abdullah, A.S., Abed, M.A., and Barazanchi, I. Al, 2019. Improving face recognition by elman neural network using curvelet transform and HSI color space. *Periodicals of Engineering and Natural Sciences*, 7 (2), pp.430–437.
- [18] B. Durakovic, "Design of Experiments Application, Concepts, Examples: State of the Art," *Periodicals of Engineering and Natural Sciences*, vol. 5, no. 3, p. 421–439, 2017.