

Digital Image Watermarking using a Highly Secure Novel Hybrid Algorithm

Jobin Abraham
Department of Electronics,
BPC College, Piravom
Kerala, India

Abstract—Proposed here is an image watermarking scheme useable for authentication and copyright protection. A hybrid scheme that combines the advantages of DWT and DCT is devised and implemented. Here the whole of host image is not subjected to forward and reverse transform operations as done usually, instead the hosting image pixels alone are subjected to the two ways transform operation. Hence while operating on larger sized images, it is faster and more efficient as other pixels not used are left intact and untampered. The algorithm proposed is tested on numerous standard test images and the results are noted down. Common attacks that rupture the hidden watermark are also tested, to which a good level of robustness is obtained as demonstrated by the test results.

Keywords—watermark embedding; digital image watermark extraction; transform domain method; resilience to attacks

I. INTRODUCTION

Ownership protection or Copyright protection is a major concern in the digital world almost since the emergence of communication via Internet. With widespread employment of digital means of content storage and data transfer the concerns also grew bigger as the risks and challenges associated with safeguarding data became more challenging than ever before. As a solution to this anarchy, Watermarking schemes are recommended for protection of digital images from being misused by adversaries once they are available in the public domain. Though watermarking schemes were primarily developed for copyright protection, they are now put to use in several fronts relating to content safety. Recently watermarking schemes are also devised for various related applications such as fingerprinting the images, tamper detection and image recovery.

Digital watermarking is the mechanism for hiding a mark such as text or image in digital resources [1]. The watermark integration may be performed imperceptibly or visibly. Imperceptible means of marking is largely used for copyright protection on contrary visible schemes serve to advertise labels or pieces of information for the viewers cognizance.

The study in [2] establishes the field of digital image watermarking continues as a highly research area due its potential application in various areas such as data authentication, broadcast monitoring, copy control, fingerprinting and media forensics. For instance, by inserting the buyer details within a content the seller can keep a record of transaction which at the same time discourage and control

copyright breaches [3]. As a whole, application areas of watermarking are spread out to include areas such as, medical imaging, tamperproofing, audience measurement to law enforcement [4].

A major threat to digital watermarking is the targeted attacks that are designed to weaken the presence of embedded ownership information. Attacks can be intentional or unintentional. Intentional attacks can take any extreme form such as cropping or copy-pasting external image portions to make the hidden watermark undetectable. On the other hand, unintentional attacks are those actions enacted to enhance the image appearance or actions such as image compression that intends to save memory storage requirements. A variety of intentional and unintentional attacks are listed in [5].

II. LITERATURE SURVEY

Digital watermarking mechanisms can be broadly classified into spatial domain schemes [6, 7] and transform domain schemes [8, 10] based on the domain in which watermark integration with host image is performed. Invariably transform-based schemes are proven to be robust; hence such schemes are further investigated to enhance their deliverables by the researcher.

A review of various transform domain techniques used to embed watermark in host image is presented by [11]. Watermarking in frequency domain remains to be the safest scheme due to the possibility of imperceptibly scattering the watermark within host media and greater robustness to attacks [5].

A scheme using DCT transform is described in [12]. In this scheme, based on the size of the watermark random number of 8x8 blocks are selected from the host image for watermark embedding. Further, DCT of these blocks are computed and coefficients from row1, column5 and row5, column1 are used to setup two data sets. Then to embed the watermark, the coefficients are modified or set to zero depending upon the watermark bit. The deficiency of the scheme is that extraction of watermark under attacked scenario yields inferior output signal.

A color image watermarking in spatial domain is presented by [13]. For watermark embedding, all the three channels of color image are sub-divided into 4x4 non-overlapping blocks and DC coefficient of 2DFT is calculated only for the blocks

that are selected by hash pseudo-random scrambling algorithm. The DC coefficient of the block thus selected is modified to represent the watermark bit, 0 or 1. Though the scheme is fairly robust, the quality of the watermark image generated is comparably low registering a SSIM value of 0.9414. This degradation is largely due to use of DCC that literally spreads the external watermark bit to the whole of 4×4 block rather than localizing the variation to a specific portion.

A detailed study on hybrid watermarking schemes is done in [14]. The study underline hybrid methods are more robust and offer better imperceptibility compared to conventional spatial domain or transform domain watermarking schemes. [15] presents a hybrid scheme based on DWT-SVD. This method suggests the use of fourth level DWT decomposition of the host image and subsequent engagement of V matrix obtained from the SVD on two sub-bands, HH4 and LL4, for embedding the watermark. The scheme could accommodate high watermark payload as 3-level DWT decomposition of watermark is performed before they are integrated with the host image. However, as only LL3 and HH3 sub-bands are being used at the time of watermark embedding, the extraction phase fails to reproduce the precise watermark. Another side effect of increased payload is the watermarked image's quality degradation as indicated by comparatively lower SSIM values. [9] explains another hybrid watermarking using lifting wavelet transform (LWT) and discrete wavelet transform (DWT) for watermarking medical images.

A FDCuT-DCT based watermarking scheme primarily for medical image watermarking is discussed in [16]. FDCuT is applied on the host image to obtain three bands, Low Frequency, Middle Frequency and High Frequency bands. The scheme utilizes high frequency curvelet coefficients for DCT computation to get the mid-band where the watermark will finally be embedded. Two uncorrelated WGN (White Gaussian Noise) is engaged with a strength factor k to embed the bit; sequence 0 for bit 0 and sequence 1 to embed bit 1. Though the scheme is robust to several attacks, successful or precise extraction of hidden watermark is not possible even with zero tampering. Moreover, for improved robustness higher strength factor must be utilized which will obviously impair the quality of the watermarked image generated. Hybrid method presented in [17] uses DWT (discrete wavelet transform) and SVD (Singular Value Decomposition). SVD is applied at two levels and the watermark is embedded in LL4 sub-band. Encrypted watermark using Arnold map is used for embedding in the host image. The scaling factor is set as a trade-off between the desired imperceptibility and robustness.

III. PROPOSED METHOD

The method has two major phases. First, is the embedding phase where the watermark signal is integrated within the transformed domain coefficients of the host image. And the second phase is used mainly to establish ones claims on ownership by decoding his distinguishing signal from the hosting or disputed resource.

Significant edge pixels in an image are selected and used in the proposed method for embedding the watermark. For identifying the actual candidate edge pixels within an image,

the given host image is first subjected to two attacks that are very likely to be enacted by a receiver user sometimes casually to enhance the image. Here for the study, histogram equalization and jpeg compression is selected as both are very common and unintentionally attempted either to make the image appealing or performed non-maliciously to save on storage space. The details of the proposed procedure is shown in the block diagram in figure 1. Edge detection on actual image and its attacked versions are then analyzed for constructing a pool of unaffected pixels that will further be used for watermark signal insertion.

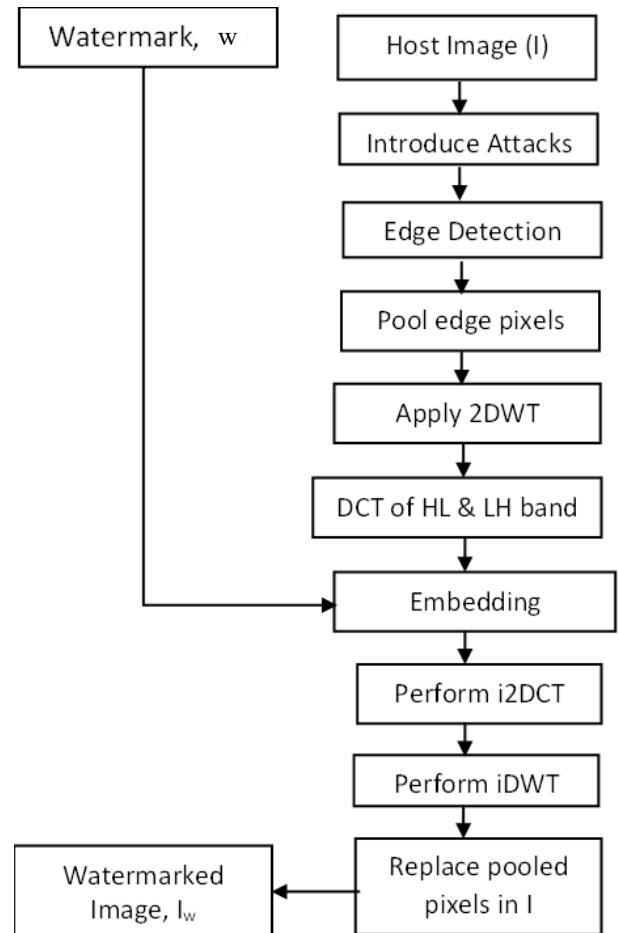


Fig. 1. Process of Embedding

A. Embedding Process

The steps involved in the Embedding process are explained below.

- Step 1: Input the host image I of size $N \times N$ and binary watermark image, w , of size $M \times M$. Convert watermark to a vector $w(k)$, where $k = 1, 2, \dots, Q$. The total length of the array $Q = M \times M$.
- Step 2: Enforce two candidate attacks a_1 , a_2 on I . Let the outcome from this exercise be I_{a_1} and I_{a_2} respectively for the attacks a_1 and a_2 .
- Step 3: Perform edge detection operation on all the version of the images, I , I_{a_1} and I_{a_2} .

Step 4: Compare the edge maps from the above and estimate the pixels that are still common. The results of above step are used to find invariant regions. Let R be count of this pixel train.

Step 5: Further, create a 2D sample image PI using the identified pixels. Perform the following to obtain an evenly sized 2D array, if R is not a perfect square.

Round the square root of pixel count R to nearest integer, $S = \text{floor}(\sqrt{R})$. If S is not even, decrement and reset as $S = S - 1$.

The outcome obtained from this stage is the pooled image PI of size $S \times S$.

Step 6: Decompose the 2D shaped pooled pixels image PI using 2DWT

$$[LL, LH, HL, HH] = \text{DWT}(PI)$$

Step 7: Compute DCT of HL band LH band to obtain D_{HL} and D_{LH} respectively

$$D_{HL} = \text{DCT}(HL)$$

$$D_{LH} = \text{DCT}(LH)$$

Step 8: Embed the watermark bit $w(k)$ in the mid-band coefficients (coef_{DHL} and coef_{DLH}) of D_{HL} and D_{LH} . Initialize, $k=1$.

If ($w == 1$), set ($\text{coef}_{DHL} < \text{coef}_{DLH}$)

If ($w == 0$), set ($\text{coef}_{DHL} > \text{coef}_{DLH}$)

Whenever not aligned as that of the above, modify coef_{DHL} and coef_{DLH} to reflect the required status by modifying as,

$\text{coef}_{DHL} = \text{coef}_{DLH} - \text{esr}$ for inducing ($\text{coef}_{DHL} < \text{coef}_{DLH}$) when ($w == 1$) and

$\text{coef}_{DLH} = \text{coef}_{DHL} - \text{esr}$ for ($\text{coef}_{DHL} > \text{coef}_{DLH}$) when ($w == 0$) where esr is a scalar value, known as embedding strength, used to ensure a desirable minimum difference between the two coefficients is always sustained.

Step 9: Increment, $k = k+1$; repeat step 8 until $k == Q$.

Step 10: After embedding all k watermark bits, perform i2DCT on D'_{HL} and D'_{LH} followed by i2DWT on $[LL, LH, HL, HH]$.

Step 11: Replace the embedded pixels back in host image in their original locations. Output the watermarked image, I_w .

B. Extraction Process

This stage decodes the embedded watermark from the host image. The host image is first used to generate the map required for identifying the pixel pool used for watermark embedding. The watermark containing pixels are retrieved or re-pooled from the watermarked image (I_w) with the assistance of aforementioned map and then watermark is decoded. The extraction algorithm is presented in the block diagram shown in figure 2.

The details of the steps involved are explained below.

Step 1: Input the watermarked image I_w and I.

Step 2: Perform the initial steps, steps 2 to 4 as performed during embedding process, for identifying the host pixels from I to form the edge map.

Step 3: Apply the edge map for pooling the corresponding pixels from the watermarked version the image I_w . The outcome obtained for this stage is pooled as image PI' of size $S \times S$.

Step 4: Decompose the pooled pixels image using 2DWT

$$[LL', LH', HL', HH'] = \text{DWT}(PI')$$

Step 5: Compute DCT of HL band LH band to obtain D_{HL} and D_{LH} respectively

$$D'_{HL} = \text{DCT}(HL')$$

$$D'_{LH} = \text{DCT}(LH')$$

Step 6: Extract the watermark bits from the mid-band coefficients of D_{HL} and D_{LH}

If ($\text{coef}_{DHL} > \text{coef}_{DLH}$), $w(k) = 0$ else $w(k) = 1$

Increment, $k = k+1$. Repeat the step until all watermark bits are read.

Step 7: Reshape the extracted values to form a two-dimensional image, w' of size $M \times M$.

These steps will recover the hidden watermark and could be used further for ascertaining the ownerships rights or to authenticate the image.

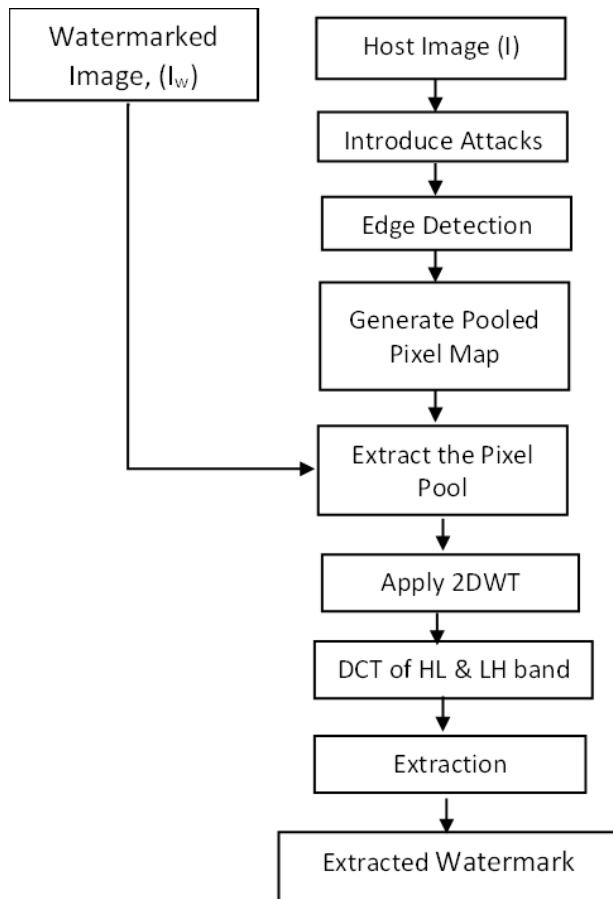





Fig. 2. Process of Watermark Extraction

IV. EXPERIMENTAL ANALYSIS

The proposed image watermarking method is developed using Matlab and tested on numerous standard and non-standard grayscale images. First, the process of embedding the watermark (w) is carried out and later, the counter operation to extract the hidden content is proceeded with. Both phases were extremely successful in that a high-quality watermarked image was obtained as the outcome from the phase one and also at the same time for phase two, the extracted watermark's bit error ratio results we obtained were all zeros. The grayscale images used for analysis were of size 512x512 and that of watermark is 32x32. Further, to qualitatively evaluate the scheme, methods discussed in [18] for accessing imperceptibility and robustness were engaged.

Host Image	Watermarked Image	Extracted Watermark
		

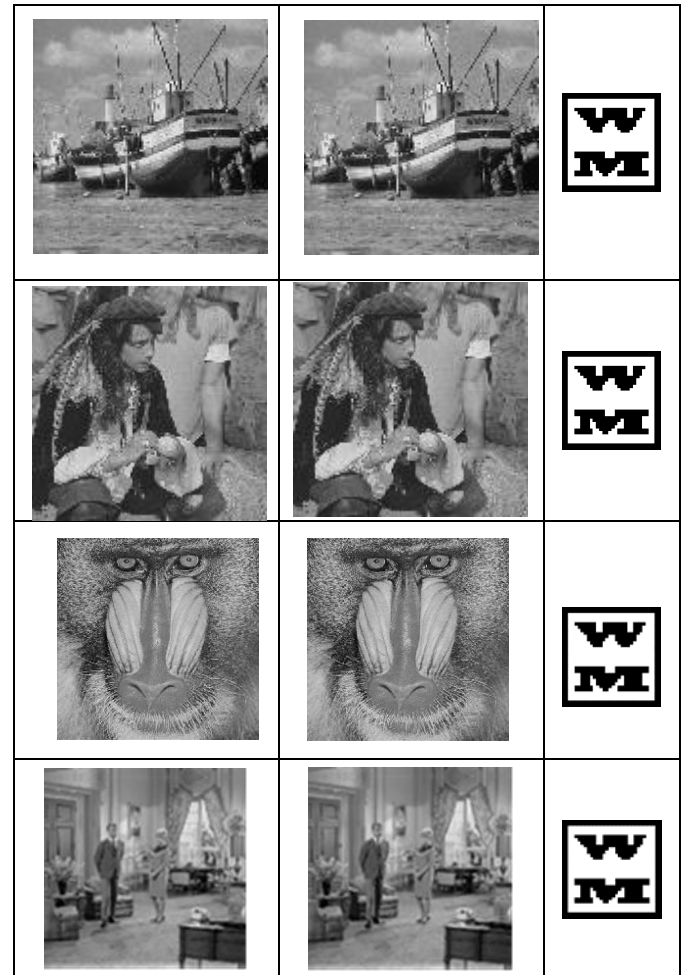


Fig. 3. Experimental Analysis of proposed method (Images: Lena, Boat, Pirate, Mandrill, Livingroom)

The experimental outputs are shown in figure 3. Watermarked image and the host images are shown side by side for easier comparison of the result generated. The process of extraction for all tested cases could successfully decode the hidden watermark and the NC values measured equals 1. A strength (esr) of 5 was used and for the livingroom image an esr of 10 was adopted. The readings for MSE, PSNR, SSIM, NCC and BER are presented in Table 1.

TABLE I. QUALITY MEASUREMENTS

Image	MSE	PSNR	SSIM	NCC	BER
Lena	4.06	42.05	0.9963	1	0
Boat	4.55	41.55	0.9971	1	0
Pirate	4.98	41.16	0.9954	1	0
Mandrill	2.17	44.76	0.9989	1	0
Livingroom	4.17	41.93	0.9968	1	0

TABLE II. RESILIENCE TO ATTACK MEASUREMENT

Attack Type	Lena Image		Boat Image		Pirate Image	
	NCC	BER	NCC	BER	NCC	BER
Salt & Peper	0.8471	0.1592	0.8445	0.1582	0.8429	0.1602
Histogram Equalization	0.9523	0.0488	0.8069	0.1963	0.9732	0.0273

Wiener Filtering	0.9693	0.0313	0.9750	0.0254	0.9532	0.0479
Contrast Adjustment	1	0	1	0	1	0
Image Sharpening	0.8437	0.1572	0.8323	0.1689	0.8751	0.1273
Poisson Attack	0.8462	0.1572	0.8354	0.1670	0.8407	0.1621



Fig. 4. Watermark Attack analysis (Salt & Pepper, Histogram equalization, Wiener filtering, Contrast adjustment, Image sharpening, Poisson attack)

Resilience of watermark to attacks of different kinds is an important prerequisite for the adoption of watermarking schemes [19]. Figure 4 shows the watermarked images that have undergone various attacks, mostly intentional to undo the presence of watermark signal from the host media. An embedding strength of $es=10$ is selected to generate the watermarked images for testing the attacks. The results observed shows the image could survive various attacks, and the embedded watermark could be detected with a profound similarity that makes them undeniable. Table 2. lists the NCC and BER measurement obtained after staging various attacks on three test images namely, Lena, Boat and Pirate image.

A Comparison of proposed method with few other existing methods is given in Table 3. The values illustrate the SSIM and NC is superior for proposed method in comparison with others. This indicates the imperceptibility and quality watermark extraction objectives stand accomplished.

TABLE III. COMPARISON WITH OTHER SCHEMES

Metric	Proposed	Sai Shyam Sharma	Fauzia Zameen	Qingtang Su et al
Domain	DWT-DCT	3-level DWT	4 -Level DWT - SVD	Spatial domain

Host image	512x512 grayscale image	64x64	512x512	512x512 color image
Watermark size	32x32	64x64	256X256	32x32 color watermark
Embedding band	Mid-freq bands	All sub-bands of 3-level DWT	Sub-bands – LL4 & HH4	Throughout, spread in 4x4 blocks
PSNR	42.05	29.78	43.84	38.05
SSIM	0.9963	0.9737	0.9909	0.9414
NCC	1	0.9984	0.9995	1

V. CONCLUSION

A novel watermarking scheme based on DWT-DCT is designed, implemented, and tested. The concept of pooled pixel region was used to incorporate the external watermark signal. After integrating the watermark, the pooled pixels are reassigned to their original positions so that the presence of the watermark is distributed throughout the image and is not highlighted to a noticeable level. In the second half of the work, the proposed method is tested and the performance is objectively analyzed. Testing under different watermark attack scenario is also undertaken to ensure the robustness of the design. The watermark could still be extractable with a comparatively high NCC value; which is sufficient to ascertain or confirm the content was watermarked by its producer owner beyond doubt.

REFERENCES

- [1] Prasanth Vaidya S, Chandra Mouli P.V.S.S.R (2015), Adaptive Digital watermarking for copyright protection of digital images in wavelet domain, Second International Symposium on Computer Vision and the Internet, Procedia Computer Science 58, pp233-240
- [2] Mahbuba Begum, Mohammad Shorif Uddin (2020), Digital Image Watermarking Techniques: A review, Information, 11, 110, doi:10.3390/info11020110
- [3] Shweta Wadhwa, Deepa Kamara, Ankit Rajpal, Aruna Jain, Vishal Jain, (2021), A Comprehensive Review on Digital Image Watermarking, Workshop on Computer Networks & Communications, Chennai, pp126-143
- [4] Kavitha Soppari, N Subhash Chandra (2019), Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks, International Journal of Computer Trends and Technology, 67(1), pp16-25
- [5] Basna Mohamad Salih Hasan, Sideeq Y Ameen, Omer Mohamad Salih Hasan (2021), Image Authentication based on Watermarking Approach: Review, Asian Journal of Research in Computer Science, 9(3), 34-51.
- [6] Soumya S, Sahana Karanth, Sharath Kumar (2021), Protection of data using image watermarking technique, Global Transitions Proceedings 2 (2021), 386-391
- [7] Zaid Bin Faheem, Mubashir Ali, Muhammad Raza, Farrukh Arslan, Jehad Ali, Mehedi Masud, Mohammad Shorifuzzaman , (2022), Image Watermarking Scheme using LSB and Image Gradient, Applied Science, DOI:10.3390/app12094202
- [8] Sara Helal, Nema Salem , (2021), A Hybrid watermarking Scheme using walsh Hadamard transform and SVD, Procedia Computer Science 194, pp 246-254
- [9] S Prasanth Vaidya , (2022), Fingerprint based robust medical image watermarking in hybrid transform, The Visual Computer, DOI: 10.1007/s00371-022-02406-4

- [10] Sai Shyam Sharma, Venkatachalam Chandrasekaran , (2021), A Novel 3-level DWT and CNN-based blind grayscale image watermarking for copyright protection against adversarial attacks, ICTACT Journal on Image and Video Processing, 11(03), pp 2460-2469
- [11] Sunil Gupta, Kamal Saluja, Vikas Solanki, Kushwant Kaur, Parveen Singla, Mohammad Shahid (2022), Efficient methods for digital image watermarking and information embedding, Measurement: Sensors, 24, doi.org/10.1016/j.measen.2022.100520
- [12] Sunesh, R Rama Kishore , (2020), A Novel and efficient blind image watermarking in Transform domain, International Conference on Computational Intelligence and Data Science, Procedia Computer Science 167, 1505-1514
- [13] Qingtang Su, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen, Tao Yao , (2019), New Rapid and Robust color image watermarking technique in Spatial Domain, IEEE Access, Vol 7, pp 30398 -30409
- [14] Mahbuba Begum, Muhammad Shorif Uddin , (2020), Analysis of digital image watermarking technique through hybrid methods, Advances in Multimedia, doi:10.1155/2020/7912690
- [15] Fauzia Yasmeen, Mohammad Shorif Uddin , (2021), An Efficient Watermarking Approach based on LL and HH Edges of DWT-SVD, SN Computer Science
- [16] Rohit Thanki, Surekha Borra, Vdvyas Dwiedi, Komal Borisagar , (2017), An efficient medical image watermarking scheme based on FDCuT-DCT, Engineering Science and Technology, an International Journal, 20, pp 1366-1379
- [17] Mahbuba Begum, Sumaita Binte Shorif, Mohammad Shorif Uddin, Alistair Barros, Md Whaiduzzama, Image Watermarking using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility, <https://doi.org/10.3390/a17010032>, 17, pp1-20, Algorithms, 2024
- [18] Yuanjing Luo, Xichen Tan and Zhiping Cai, Robust Deep Image Watermarking: A Survey, Computer, Materials & Continua, Vol.81, pp.133-160, 2024
- [19] Saif Aldeen S. Naem, Sarab M. Hameed, Digital Watermarking Techniques, challenges, and applications: A review, Mesopotamian Journal of Cybersecurity, 5(2), pp.453-476, 2025