An Improved Hybrid DCT-DWT Blind Watermarking Technique for Securing Multimedia Images

M. Hema
SRM University: SRM Institute of Science and Technology
Prayla Shyry S (praylashyry.cse@sathyabama.ac.in)
Sathyabama University https://orcid.org/0000-0003-0191-7534

Research Article

Keywords: Watermarking, DCT-DWT

Posted Date: February 22nd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1352507/v1

An Improved Hybrid DCT-DWT Blind Watermarking Technique for Securing Multimedia Images

M. Hema[1], Dr. S. Prayla Shyry[2]
Research Scholar[1], Professor[2]
m.hema23@gmail.com[1], praylashyry.cse@sathyabama.ac.in[2]
Sathyabama Institute of Science and Technology

Abstract- People are capable of manipulating and copying digital images. Protection and security must be given to the right property from piracy and illegal copies. To safeguard the intellectual property of digital images digital watermarking is used as a solution. Watermarking technique is prevalent due to an effective copyright protection method i.e., only the rightful owner can identify the signature that is embedded in a digital document. In this paper, a blind watermarking scheme is used which is dependent on the image content of certain specific DWT-DCT coefficients. The use of generalized Gaussian distributions helps in modelling the DCT-DWT coefficients of the Source image. The suggested system attained optimal PSNR, MSE and SSIM values and numerous attacks are resisted by an embedded watermark in the image watermarked as per the results of the experiment. Furthermore, the suggested system depicts far more robustness against numerous image processing attacks for example, scaling to 0.25 & 0.50, Cropping, and various types of noise attacks. Experimental results and numerical values of parameters confirms that the hybrid DCT-DWT blind watermarking technique is relatively efficient and also justifies the theoretical analysis.

Keywords - Watermarking, DCT-DWT,

1. INTRODUCTION

Internet technology has developed so much that a large amount of multimedia data is being transferred over the internet. Copyright protection is needed for transferring multimedia data over internet [2]. All kinds of data for example, video, image audio and documents could be transferred by people through internet network. Therefore, multimedia data must be protected in order to safeguard the distribution of intellectual property. This problem gives raise to develop a solution for copyright protection and image authentication. The most predominant media over the internet is the Digital image. It also acts as an efficient camouflage for hiding messages effectively [3]. Digital watermarking acts as an alternative solution for securing the patented and private property (In this case, images) from illegitimate users. Digital Watermarking is the method where sensitive private data is hidden in the type of a watermark into another signal [24]. This is termed as a host or cover where the embedded host signal's visual quality should not be lowered. For more effectiveness, extraction and detection of watermark needs to tested against a finite number of alterations and attacks that meets certain characteristics such as robustness, integrity & security [3][4].

There are certain properties to be fulfilled by a reliable digital watermarking scheme like, undetectability, security, imperceptibility, robustness, and blind extraction. Less distortion should be produced by embedding watermark into the original source image such that human visual system should not be able to detect the watermark effect [23]. The quality of the original host image and the image obtained after watermarking must be closer. There are recurrent signal processing and attacks for example, additive noise, filtering, cropping and modification of pixel values which must be resisted by the watermarks [2]. The watermark inward the image must be such that it is very difficult to be found and damaged by the intruders which is the main purpose of the watermarking method. In order to develop a robust and imperceptible

watermarking scheme which has very high security properties and has less complexity in computation which is always a major challenge.

During extraction process, classification of the watermarking schemes is based on how the original image is used. If the original image is required during the extraction process, then it is termed as non-blind watermarking [5]. On the other hand, if the original image is made unavailable during the extraction of the watermark, it is termed as blind watermarking. This paper focusses on the latter.

Robustness and quality camouflaging classifies the watermarking schemes into Discrete Cosine Transform (DCT) & Discrete Wavelet Transform (DWT) which relies on frequency domains. The embedding task could be completed with the aid of discrete cosine transform (DCT) & discrete Fourier transform (DFT) in the transformed domains [5][6]. According to the research, low and middle frequency coefficients are more sensitive to the human vision. Therefore, within the low frequency ranges, when the watermarks are embedded, operation methods of good performance in the transformed domains could be obtained [25][26]. Besides, the advantages of good energy compression, multi-resolution, and an imperceptible picture quality is obtained due to the DWT-based watermarking methods thereby, making it useful for image watermarking. Conversely, geometric attacks are irresistible while using the DWT-based watermarking [8].

The primary objective of the research lies in evaluating the performance of the given watermarking method in DCT-DWT domain by using a new analytical framework. It is possible to determine the amount of information anyone can hide for a specific probability of error using the achieved results from the hybrid method or properly deciding what could be the probability of a given image being watermarked. The combination of two or more transform domains forms a hybrid method that focuses discrete domain faults.

This research is planned as follows. Different watermarking schemes and its related works are presented in the Section II. Various watermarking methods are discussed in Section III. The suggested DCT-DFT watermark is represented in Section IV. Section V consists of the results of the experiments conducted and the conclusion is given in Section VI of the paper.

2. LITERATURE SURVEY

Ferda Ernawan et al. (Feb 2021) proposed a scaling factor that is flexible and relies upon specific DWT-DCT coefficients in comparison with the mean values of DWT-DCT coefficients. A proposed set of rules were used to embed the watermark image that followed flexible scaling factor. According to the experimental results, the suggested method could reach SSIM value of 0.987, PSNR value as high as 47dB and could provide an embedded watermark challenged with numerous attacks. The suggested watermarking methods was assessed under numerous attacks for robustness which is inclusive of filtered image, added noise, compression and geometrical attacks. The suggested method was also assessed for imperceptibility of watermarked pictures. According to the results, the suggested technique displayed very low BER value of the retrieved watermark even after subjecting to different attacks [1].

Baharak Ahmaderaghi et al. (March 2018) proposed a blind watermarking scheme that used Discrete Shearlet Transform (DST) as a field for embedding. A nonadditive method that depends on the statistical decision theory is used for new DST blind watermark detection system. The broadcast of original clean image is not needed here which is a major advantage

of the blind watermarking method. An investigation of scattered DST coefficients for various sub-bands and resolutions is done in order to achieve this. This model is proven to be simple and effective. The source image is not needed during the stage when detection occurs and also during various attacks, the parameters remain unchanged. Appreciable imperceptibility and improved payload are obtained from experimental results of DST based embedding [21].

Zakia Yahya et al. (Feb 2020) proposes “TDIAM”, a new method to transform-domain imperceptible attack in order to create attackers that are built on image steganography-method using a ``solitary cautiously watermark that is targeted". Three distinct frequency-domain methodologies, such as Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are practiced which makes it sturdy enough and requires less time to compute. While considering black box and white box attacks, the results display that the generated agitation vector positively dupes the convolutional neural network (CNN), LeNet-5 and AlexNet deep learning frameworks. Choosing between the three distress methods, DWT based distress shows more brighter results by effectively duping DNNs also confirming high imperceptibility [7].

Zhiqiang Zhu et al. (Dec 2019) suggested a new JPEG compression resistant image steganographic algorithm. The unaffected DCT coefficient signs are used before and after JPEG image compression. The distortion function determines the cost required for each candidate DCT coefficient. Lastly, the cover image is embedded with a message that is encrypted with a distortion that is minimum. The resulting image is dependent on both error-correction code and Syndrome-trellis codes. A typical steganographic system for images is suggested based on specific analysis where both the channels are addressed. A new algorithm based on steganography is developed which is robust and uses multiple quality factors which resists JPEG image compression. The suggested procedure has better undetectability performance when matched with DCRAS, FRAS and DMAS [17].

Ferda Ernawan And Muhammad Nomani Kabir (April 2018) presents a method that delivers robustness and high imperceptibility for protecting copyright information using Discrete Cosine Transform (DCT) psychovisual threshold using a reliable digital watermarking method. The DCT regions of a particular frequency are utilized by an embedding process in the watermarking method in such a way that the inclusion of watermark bits causes the minimum possible image alteration. For getting best quality of image, the proposed optimal psychovisual threshold is defined so that the watermark is embedded as a part of the source image. Additional security is provided by scrambling the watermark before embedding. For further verification, the technique is tested under numerous geometric attacks and signal processing. Results obtained experimentally reveal that the proposed technique is better in performance when compared to available methods in SSIM and NC values [22].

Rui Wang et al. (Oct 2020) suggests a new method of image zero-watermarking that protects from rotation attacks. It is centred on discrete cosine transform (DCT) and nonsubsampled pyramid decomposition (NSPD). According to the experimental results, the suggested method is very much robust against number of image processing attacks for example, filtering, scaling, rotation, translation, JPEG compression and Checkmark attacks. Many experiments were conducted to establish that in NSPD-DCT field, the AC coefficient signs of the image remains unchanged under different attacks. Also, before using zero-watermark detection, image rotation correction method was used to improvise robustness of the method against rotation attacks [9].

Junxiu Liu et al. (July 2019) recommends a unique image watermarking technique that is cantered on singular value decomposition (SVD), Hessenberg decomposition (HD) and discrete wave transformation (DWT). Initially, the raw source image is divided into number of sub-bands with the introduction of multilevel DWT which is termed as the embedding process. The subsequent coefficients are then used as the input for HD. The Fruit fly optimization algorithm (FOA) helps identify the optimal scaling factor accurately. With the aid of numerical simulation experiments, robustness and invisibility of the proposed technique is evaluated. Good visual quality, PSNR and SSIM are the results depicted by watermarked host images. The suggested technique's performance is much better and robust against various attacks [16][31].

Juan R. Hernández, Martín Amado, and Fernando Pérez-González (Jan 2000) analyses copyright protection of still digital images by using spread-spectrum-like discrete cosine transform domain (DCT) watermarking method. According to JPEG algorithm, DCT scheme is applied in blocks of 8 x 8 pixels. Illegal misuses could be easily tracked by encrypting information using watermarking. The ownership verification stage has two important tests: Initially the message embedded in the watermark is extracted using watermark decoding. Detection of the watermark determines whether the given input image holds a hidden watermark secured with a specific secret key. Secret key provides both security and robustness. The output achieved during the interleaving stage of the pseudorandom sequence generator and the pseudorandom sample permutation is determined with a secret key [29][32].

Amir Ansari, Genaro Saavedra, And Manuel Martinez-Corral (Nov 2020) suggests a new technique for light field watermarking with broad deliberation of the spatial and angular data. The suggested method's robustness is tested against common image processing attacks. A novel technique for LF watermarking is suggested in this paper. In order to improvise the performance of watermarking, large-scale intercorrelation and intra correlation of the LF has been introduced using 4D wavelet transform. The 3D perception of the watermarked LF is very well preserved which provides appreciable robustness against Guassian noise, median filtering, JPEG compression, and JPEG 2000. It was discovered that utilizing too few or too many DCT coefficients as well as too small block dimensions lowers the performance [12][33].

Alexia Briassouli and Michael G. Strintzis (Dec 2004) analysed the performance of nonlinear locally optimal blind watermark detection techniques that are transformed through DCT. ROC curves are compared in order to observe the effect of pre-processing using the LO Cauchy nonlinearities and Gaussian ZMNL both experimentally and theoretically. The performance is comparatively efficient than the finest generalized Gaussian detector through the usage of nonlinearities. Simplicity in implementation is an additional advantage of using nonlinear detectors. Also, with the existence of quantization, the performance of the suggested system is observed. Using the outcomes from the theory of dithered quantization, the effects of quantization on the detectors are examined [28][34].

TABLE 1
COMPARISON OF METHODS

R. NO	METHODOLOGY	ADVANTAGE	DISADVANTAGE
[1]	flexible scaling factor based on the image content's DWT-DCT coefficients	Robust under various attacks	Improved quality of watermarked image using optimization method

[21]	Blind Novel image watermarking using Discrete Shearlet Transform	Interceptibility and improved payload	Shortcomings in robustness against high compression levels
[7]	TDIAM method used on single selected targeted watermark	Robust and less computational time required	Practical threat to physical systems deployed in stable environments
[17]	Novel steganographic algorithm is designed for unchangeable image before and after JPEG compression	Better performance	Post processing attacks needs to be improvised
[22]	Image watermark by psychovisual method	High invisibility and robustness	Could not tolerate Guassian noise outbreak and histogram equalization
[9]	Unique zero watermarking method using NSPD-DCT	Robust against many image processing attacks	Not much robust against Checkmark attacks
[16]	Watermarking an image using DWT, SVD and HD	Very robust in order to secure noise, filter, sharpening and compression attack	Should be defending rotation attack and cropping attack. Performance could be increased using FOA algorithm
[29]	In order to have copyright protection, DCT is applied to still digital pictures	Robustness and more security is provided	Suitable coding methods are derived
[12]	4D wavelet transform is used for light field watermarking	Best watermarking performance is achieved	For avoiding intense attacks, integrity of various simulations is needed
[28]	Performance of Gaussian method and optimal Cauchy non linearity methods is analyzed traditionally and theoretically	Better performance than the existing detectors, simplicity in implementation	Noise statistics are unknown or inaccurate in nonlinear watermark detector

3. EXISITNG METHODOLOIGES FOR BLIND WATERMARKING SCHEME

3.1 Digital Image Watermarking

Digital image watermarking embeds a secret image into a carrier image for transmit of the secret image to a intended receiver [10]. The extraction process for any unintended receiver is made difficult or impossible. The method comprises of an effective embedding process and a

efficient detection process. Equation (1) represents the embedding process of any watermarking scheme. Equation (2) is used to compute original I_W when we have I_W'.

$$I'_w = F\left(S, I_{w,} k_p\right) \quad (1)$$

$$I_w = F^{-1}\left(S, I'_w, k_p\right) \quad (2)$$

Here,

I_w represents the original watermarked image
I_w' represents the processed watermarked image
F denotes pre-processing function
F^{-1} denotes the inverse pre-processing function
S denotes the size of the carrier image
K_p represents the private key used for embedding the watermark in C

The watermarked carrier represented by W_c is obtained using equation (3), where the original carrier image is represented by C and the encoding function is represented by E as indicated in equation (4). The exponent of the embedded image is denoted by $a \in [0,1]$ and embedding intensity is given by $\lambda \in R$.

$$W_c = E(C, I'_w) \quad (3)$$

$$E\left(C(x), I'_w(x)\right) = C(x) + \lambda\left(C(x)\right)^a I'_w(x) \quad (4)$$

Equation (5) represents the digital watermark extraction from the image which is watermarked, where extracted information is represented as $I_w*(x)$ whose position is given by x and the decoding function is provided by D and finally the carrier image is denoted by C and watermarked carrier image represented by W_c.

$$I_w * (x) = D\left(W_c(x), C(x)\right) \quad (5)$$

Digital image watermarking is classified into transform based on domain space and based on transform on transformation domain [11]. It is calculated based on the similarity and Peak signal to noise ratio (PSNR).

3.2 Discrete cosine transform (DCT)

Discrete Cosine Transform (DCT) is defined as an orthogonal transformation of image processing and signal processing. DCT provides high-computational complexity, low-error rate and high-compression ratio [13]. The compression performance of Discrete Cosine Transform on JPEG images is comparatively high and transforms the signal from one domain to another domain i.e., Spatial to frequency. Real data is transformed into real spectrum by DCT, which helps avoid redundancy [27][30]. DCT is applied to each section. This results in three frequency sub-bands namely high, mid and low frequency. DCT watermarking is based on two major key points [14][15]. First, the energy signal lies at very low frequency sub band that contains the key portions of the image. Second, the high frequency components are eradicated through noise and compression attacks.

DCT is classified into four major categories namely DCT I, DCT II, DCT III, and DCT IV. DCT II provides the base for compression of JPEG images. The common equation for 2D-DCT of an image of size XxY can be defined by equation (6):

$$h(u,v) = \left(\frac{2}{X}\right)^{\frac{1}{2}} \left(\frac{2}{Y}\right)^{\frac{1}{2}} \sum_{i=0}^{X-1} \sum_{j=0}^{Y-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.X}(2i+1)\right] cos\left[\frac{\pi.u}{2.Y}(2j+1)\right].f(i,j) \quad (6)$$

Where,

g (i, j) is the intensity of the pixel in row i and column j
h (u, v) is the DCT coefficient in row n1 and column n2 of the DCT matrix

The DCT image coefficients will be mostly zero. Low frequency parts of the image parts have larger value, whereas high and middle frequency areas of the image have higher and smaller value respectively. Digital watermarking is this performed in areas of image where frequencies are medieval or lower.

3.3 Discrete Wavelet Transform (DWT)

In image processing, a frequency domain technique is used which is called as Discrete Wavelet Transform (DWT). In this technique, image is decomposed into frequency channels having constant bandwidth. There are several image processing algorithms in DWT that provides: compression, reduction and noise edge detection [18].

Discrete wavelet transform desecrates an image into sub-images of independent frequency domain and spatial domain. After the application of DWT to the original image it is decomposed into four sub-bands: a single segment which has low frequency (LL) and three high frequency segments (HL, LH and HH). Table 1 depicts the decomposition of the original image after application of DWT [20].

LL	HL
LH	HH

Table 1. Wavelet Breakdown

A two-dimensional image is classified into four sub-bands, namely: LL, LH, HL and HH at level 1 DWT domain. Here the first letter stands for using high-pass or a low-pass frequency operation to the rows and second letter depicts the filter which is used at the columns. Until the required number of levels is reached, each sub-band is divided. The human chromatic system is very sensitive to the LL sub-band which depicts low frequency component and the digital watermarking is usually embedded in one or more of the other three sub-bands which have better image quality [19].

The high frequency sub-band of the image exhibits less energy which denotes the edge and texture of the original image. The low frequency sub-band is distributed across remaining parts of the image thus making it available for decomposition. The energy of the image is dispersed efficiently and the stronger image intensity can be embedded. Wavelet transform is used to decompose more levels of the image. Hence, as far as possible, it is better to adopt the wavelet breakdown levels in the algorithms.

4. PROPOSED DCT-DWT HYBRID WATERMARKING SCHEME

This section explores the possibility of improvements in the existing watermarking methodologies discussed in the previous section. Based on Hybrid DCT-DWT transform, a novel digital watermarking technique is proposed. The block diagram illustrates the steps involved in the novel technique. 2D-DCT is first applied to the source image, the output of which undergoes a series of DWT transformations. The embedding and extraction process are separately depicted in the proposed framework. Figure 1. depicts the series of steps involved in the hybrid proposed method.

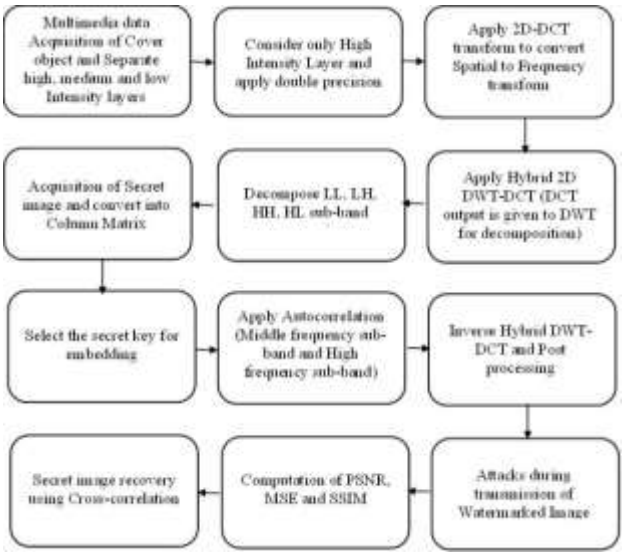

Fig 1: Proposed Hybrid DWT-DCT Scheme

Step 1: Acquisition of RGB cover image. Separate High, Medium and Low intensity layers and make resize it to standard 512×512. Consider only High Intensity Layer and apply double precision. Apply 2D-DCT transform to convert spatial to frequency transform

Step 2: Application of Hybrid DCT DWT transform over the cover image to obtain 4 sub bands: LL1, HL1, LH1 and HH1. The Image with 512×512 dimension converted into 256×256 sub band.

Step 3: Obtain a Secret image and convert the secret image into column matrix. The secret image is converted into binary format. Select the secret key for watermarking. The secret key is the image format that contains 0's and 1's.

Step 4: Apply the autocorrelation method for embedded secret image into covert object. Apply the iteration for embedding with respect to total number of matrix size of key. Estimate the high frequency inter block sequence using number of row and column of secret image. Apply the same for medium frequency for estimating inter block sequence. The scaling factor is applied to estimate final frequency coefficients.

Step 5: Estimate the mean value of the sub bands i.e. HL1, LH1 and HH1. The sub band which has the least average sub band is embedded first using the proposed method. 65536 elements are present in a single sub-band. In a single band, 768 watermark bits are inserted.

Step 6: 1×768 elements is taken into the sub-band and reformed into 256×3 portions and included in it. A single sub-band consisting of 256×256 = 65536 portions is obtained and a binary watermark bit consisting of 768 portions is included into the single sub-band.

Step 7: Apply post processing by applying Gaussian filtering, 2D median filtering to get quality image.

Step 8: Apply various attacks such as, image scaling 0.5 factor, 0.25 factor, image cropping, image noising using salt and pepper noise, Gaussian noise.

Step 9: Apply image recovery using cross correlation.

Different attacks on the watermarked image are employed and the watermarked image is assumed to be existing at the receiving end. The hidden watermark can be separated from the image using the following steps:

Step 1: Apply 2 Dimensional-DWT using Hybrid DWT DCT to the image which is watermarked.

Step 2: Evaluate the average of each sub bands i.e. LH1, HL1 and HH1.

Step 3: Take the sub band having the least average.

Step 4: Calculate the positions of the sub-band to be separated using steps (1), (2), (3) and (4).

Step 5: Separate the watermark bits from these positions from the least average sub-band. A binary matrix of size 256×3 is created.

Step 6: This matrix is reshaped into 1×768 binary matrix.

Step 7: The sub-band having the highest average is taken. Using the same method, separate watermark bits from it. A binary matrix of size 1×768 is formed.

Step 8: The three binary matrices are obtained and reshaped to 48×48. The required extracted watermark is obtained.

5. EXPERIMENTAL RESULTS AND ANALYSIS

To prove the robustness of the proposed hybrid DCT-DWT method, the blind watermarked image undergoes various attacks which proves that the proposed scheme is effective when compared with existing systems. Figure 2 shows a sample RGB source image that is acquired for blind watermarking using the proposed DCT-DWT watermarking scheme.

Fig 2: Input Source Image to be watermarked

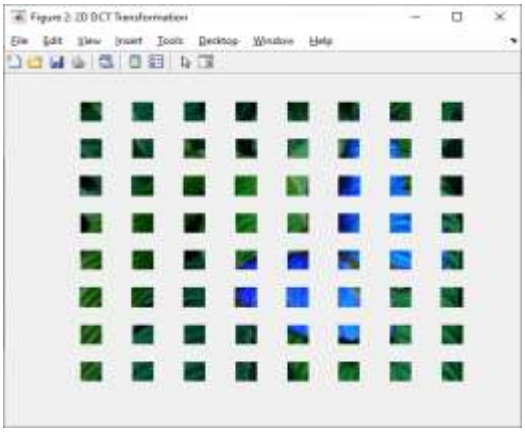

Fig 3. 2-Dimensional DCT Transformation of Source Image

The input source image is separated into 3 layers based on the intensity values associated with it. The low, medium and high intensity layers are separated from the source image. The various intensity layers are resized into standard 512x512 images. Images can be represented as single

or double precision numbers in the range 0 to 1. The operations on images are easier when they represented as floating point values. The higher intensity layers are only taken into consideration and double precision is applied to it. Each 512-image block is taken and 2D-DCT is applied to each block serially. Figure 3 illustrates the image after application of 2D-DCT to the source image. 2D-DCT converts the image from spatial domain to frequency domain.

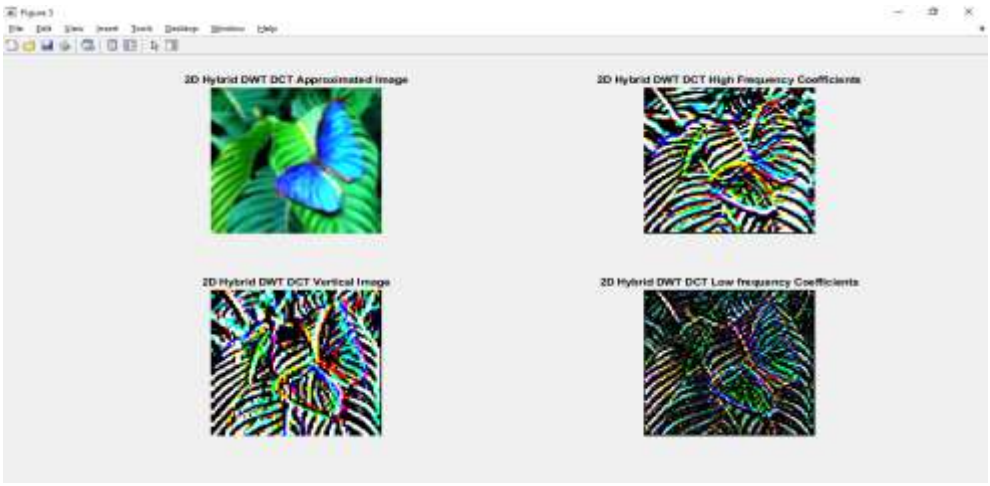

Fig 4. DWT Co-efficients into 4 Sub Bands

The source image is approximated using the hybrid DCT-DWT transform. Hybrid DCT DWT transform is applied on to the cover image to get four sub bands namely LL1, HL1, LH1 and HH1. Each 512×512 image is then converted into 256×256 sub band. Figure 4 illustrates the application of the hybrid DCT-DWT transform. The high frequency and low frequency coefficients are obtained using the hybrid method.

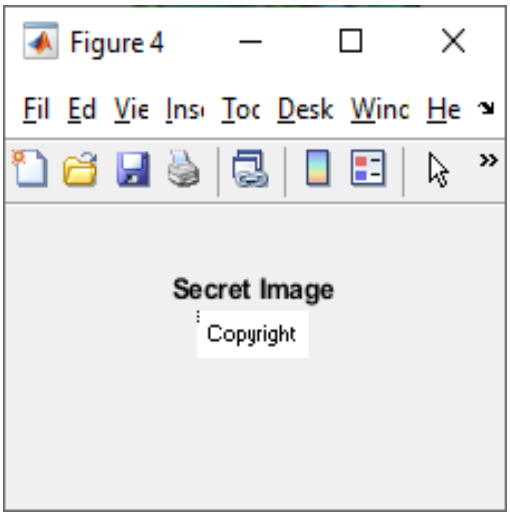

Fig 5. Secret Image to be Embedded

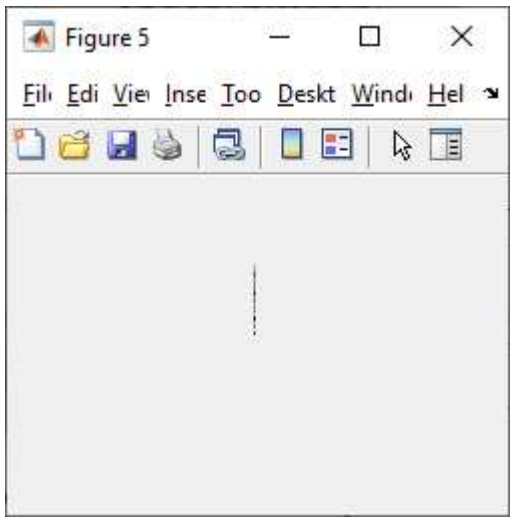

Fig 6. Random Key in Image Format

A secret image is taken for blind watermarking. The secret image is converted into a column matrix which in turn is converted into binary format. Figure 5 represents a secret Image that is selected for securing the watermarked secret image. The secret key is the image format that contains 0's and 1's. Figure 6 illustrates the secret image that is converted into a column matrix for further processing. Figure 6 illustrates the

application of the autocorrelation method for embedded secret image into a covert object.

Figure 7 represents the final raw image after embedding the DWT-DCT processed image with the watermark which is secured by the random key. The quality of the processed image is increased through the application of Gaussian filtering and 2D median filtering which is illustrated through Figure 8 and Figure 9.

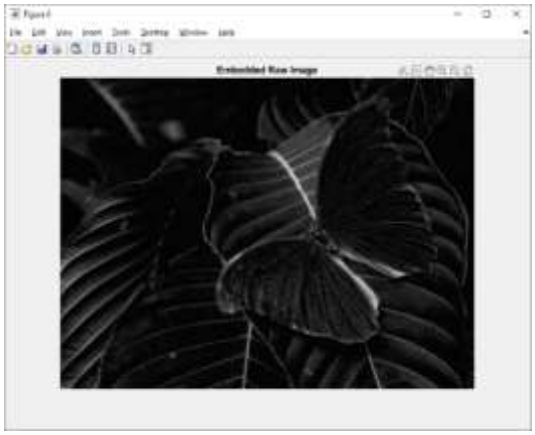

Fig 7. Embedded Raw Image in Grey Scale

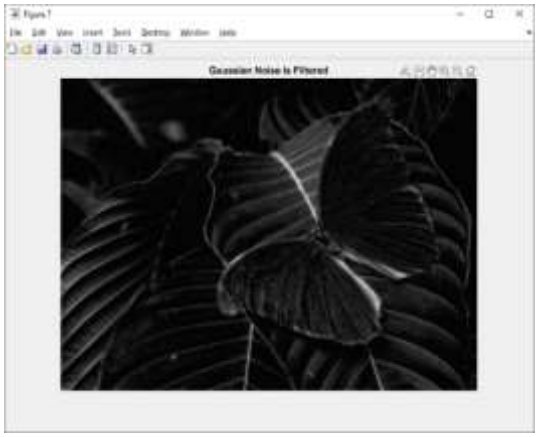

Fig 8. Embedded Raw Image with Gaussian Noise Filtered

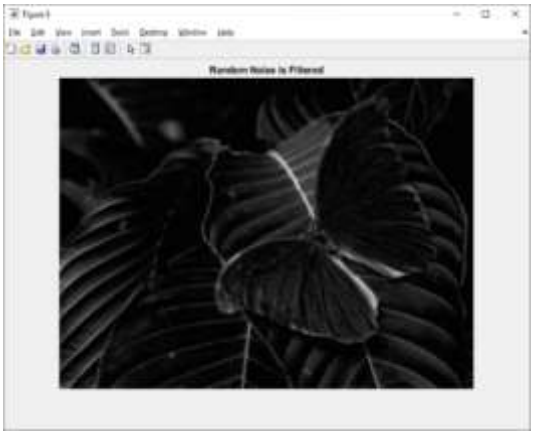

Fig 9. Raw Image with Random Noise Filtered

Fig 10. Filtered ROI Image

Figure 10 represents the pure filtered ROI image after removing the various associated noises with the application of Gaussian and 2D median filters.

Attacks on DWT-DCT Hybrid Watermarked Image

Once the watermarked filtered ROI image is obtained it is subjected to a serious of attacks to check the integrity of the watermark. Various attacks are made on the watermarked image such as image scaling to 0.5 factor & 0.25 factor, image cropping, image noising using salt and pepper noise, Gaussian noise.

In Figure 11 and Figure 12 the watermarked image is scaled down to 50% and 25% respectively. Downscaling the image is a type of attack on an watermarked image which checks whether the secret image is revealed. It is observed that scaling down the watermarked image does not reveal the secret embedded image.

Fig 11. Attack 1 – Image Scaled to 0.5

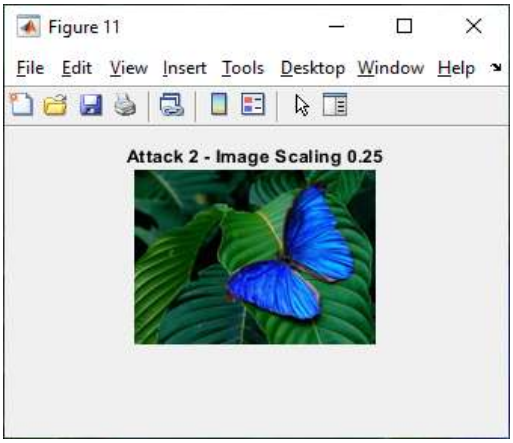

Fig 12. Attack 2 – Image scaled to 0.25

Fig 13. Attack 3 – Cropping of Image

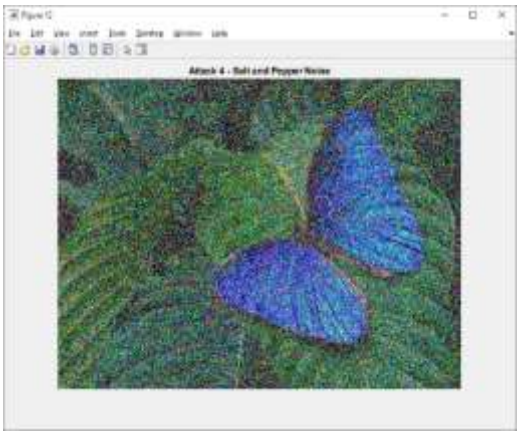

Fig 14. Attack 3 – Salt and Pepper Noise

In Figure 13 cropping is performed on the watermarked image. Cropping the image does not reveal the actual secret image or the watermark that is embedded in the source image. Thus the image is not susceptible to a cropping attack.

Fig 15. Attack 4 – Gaussian Noise

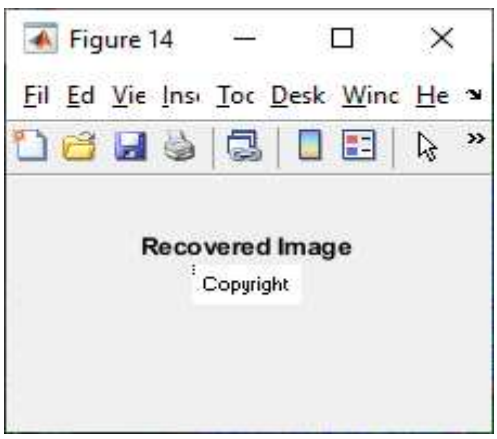

Fig 16. Recovered Image After Watermarking

Figure 14 and figure 15 introduces salt and pepper noise as well as gaussian noise into the watermarked image. The introduction of these noises which keeps the embedded quite intact and does not reveal the secret image embedded using the hybrid DCT-DWT transform. Figure 16, shows the image recovered using cross correlation.

Numerical Analysis of PSNR, MSE & SSIM

The results computed for the blind watermarking scheme based on the DCT-DWT hybrid scheme ae analysed based on three important parameters: PSNR, MSE and SSIM. Numerical values of all the 3 parameters are obtained for the watermarked image without any attack and also after application of 4 different types of attacks on the watermarked image. The following tables illustrate the above-mentioned numerical values:

Table 2: Parametric Values Without Attack

S. No	PSNR in dB	MSE	SSIM
1	59	0.0795	0.3298
2	53	0.0295	0.5847
3	52	0.0387	0.7768
4	49	0.3987	0.2676
5	58	0.0397	0.6878
6	51	0.0395	02485
7	47	0.3987	0.7878
8	41	0.3765	0.8878
9	48	0.3876	0.3942
10	57	0.3687	0.9575

Table 3: Attack 1 – Image Scaling of 0.5

S. No	PSNR in dB	MSE	SSIM
1	50	0.3983	0.3837
2	45	0.3987	0.4878
3	46	0.3876	0.4398
4	41	0.3487	0.5398
5	48	0.4787	0.4787
6	52	0.5789	0.5789
7	53	0.4579	0.5343
8	41	0.6348	0.7343
9	49	0.5678	0.5454
10	46	0.7838	0.2464

Table 4: Attack 2 – Image Scaling of 0.25

S. No	PSNR in dB	MSE	SSIM
1	45	0.9376	0.2333
2	49	0.3876	0.3876
3	41	0.7353	0.3755
4	46	1.0398	0.2567
5	52	1.1039	0.3423
6	53	1.2474	0.2342
7	50	1.2647	0.5676
8	46	0.2378	0.1453
9	42	0.3987	0.3422
10	42	0.5478	0.6423

Table 5: Attack 3 - Image Cropping

S. No	PSNR in dB	MSE	SSIM
1	39	1.2783	0.2783
2	40	1.298	0.2980
3	31	1.0578	0.0578
4	33	1.2783	0.2783
5	44	1.8476	0.8476
6	41	0.9387	0.4387
7	43	0.8398	0.2398
8	31	0.6469	0.5489
9	26	1.1101	0.3101
10	41	1.2098	0.3090

Table 6: Attack 4– Salt and Pepper Noise

S. No	PSNR in dB	MSE	SSIM
1	31	1.2000	0.1667
2	39	1.3000	0.2500
3	47	1.4000	0.3333
4	32	1.2500	0.2083
5	37	1.6000	0.5000
6	45	1.2000	0.1667
7	58	1.1000	0.0833
8	36	0.9387	0.1156
9	47	0.9376	0.2398
10	49	0.3983	0.3324

Table 7: Attack 5 – Gaussian Noise

S. No	PSNR in dB	MSE	SSIM
1	27	1.6000	0.6200
2	26	0.9000	0.1600
3	36	0.7000	0.2300
4	31	1.2000	0.3200
5	38	1.1000	0.1200
6	32	0.5000	0.5300
7	47	0.4000	0.4500
8	49	1.2000	0.2700
9	41	1.3000	0.3300
10	37	1.7000	0.7300

In Figure 16, PSNR in measured in dB and 10 different intensity images are considered. The PSNR has achieved high decibel in the case of without attack. The other attacks such as image scaling for 0.5 and 0.25, image cropping, image salt and pepper noise attack and Gaussian noise attack are considered as different attacks applied on the watermarked image. The PSNR in dB of image scaling 0.5 is reduced up to 10dB than without attack PSNR measure.

The image scaling 0.5 is reached 50dB. The PSNR in dB of image scaling 0.25 is reduced up to 5dB as shown in the figure. The PSNR in dB of image cropping varies from 25dB to 40dB. The PSNR in dB of salt and pepper noising varies from 30dB to 50dB. The PSNR in dB of Gaussian image noising varies from 27dB to 37dB.

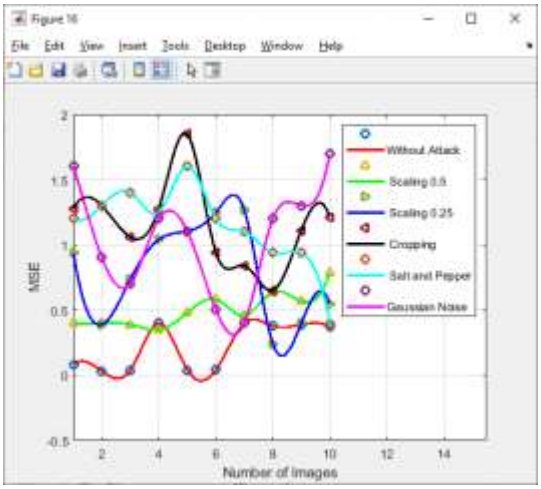

Fig 16. Comparison of PSNR – With & Without Attacks

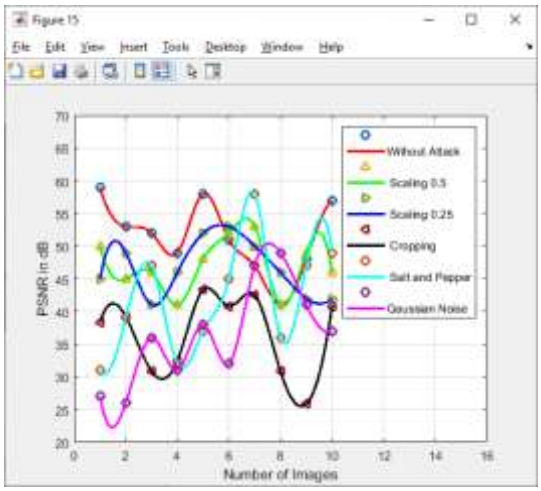

Fig 17. Comparison of MSE – With & Without Attacks

Figure 17 shows that Mean Square Error (MSE) of without attack is negligible. For the without attack image, the MSE value varies from 0.1 to 0.4. For the different attacks, the MSE value is increased as shown in the figure. The MSE of image scaling 0.5 varies from 0.4 to 0.8. The MSE of image scaling 0.25 varies from 0.6 to 0.9. The MSE of image cropping varies from

1.23 to 1.25. The MSE of salt and pepper noising varies from 0.4 to1.25. The MSE of Gaussian image noising varies from 1.6 to 1.8.

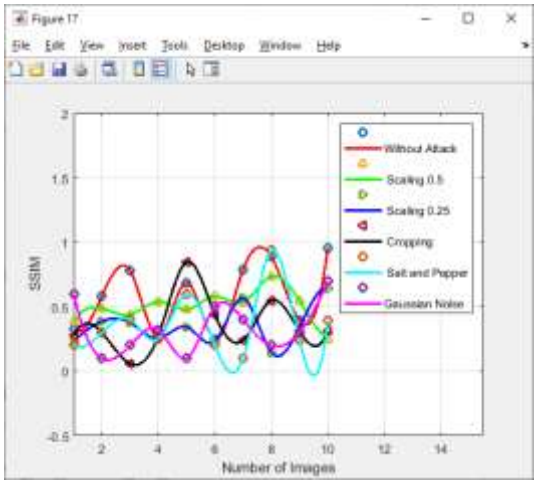

Fig 18. Comparison of SSIM – With & Without Attacks

In Figure 18, SSIM parameter of without attack is higher than other attacks. The SSIM of without attack varies from 0.3 to 1. The SSIM of image scaling 0.5 varies from 0.4 to 0.5. The SSIM of image scaling 0.25 varies from 0.2 to 0.6. The SSIM of image cropping varies from 0.2 to 0.3. The SSIM of salt and pepper noise attack varies from 0.1 to 0.3. The SSIM of Gaussian noise attack varies from 0.4 to 0.6.

CONCLUSION

In the suggested technique, novel hybrid DCT-DWT method was employed to obtain the robust feature of a host image in order to protect digital images. Many experiments were conducted to determines that even under numerous attacks there is nearly no change in the watermarked image. During numerous attacks, the proposed watermarking scheme's robustness was calculated. The attacks included scaling, cropping and introduction of various noises into the watermarked image. The watermarked image's imperceptibility was also a verification criterion in the suggested system. The transmission of original clean image is not needed in the blind watermarking which is its biggest advantage. The DST coefficients for various sub bands and resolutions are examined in order to achieve this advantage. According to the results obtained, the suggested scheme made High PSNR, low MSE and optimal SSIM values when subjected to various attacks. It is evidently a simple and effective method that allows the corresponding mathematical description of the full framework. In the future, for improvising the quality of the watermarked image, an optimization method could be used.

DECLARATIONS

Funding: The authors did not receive financial support from any organization for the submitted work.

Conflicts of interest/Competing interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Availability of data and material: 'Not applicable', Authors' contributions: 'Not applicable'

Code availability: 'Not applicable',

Consent to participate: ‘Not applicable’
Ethics approval: Compliance with Ethical Standards
Consent for publication: Authors give consent to the Journal to publish their article

References

1. F. Ernawan, D. Ariatmanto and A. Firdaus, "An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients," in IEEE Access, vol. 9, pp. 45474-45485, 2021, doi: 10.1109/ACCESS.2021.3067245.
2. A. Alzahrani and N. A. Memon, "Blind and Robust Watermarking Scheme in Hybrid Domain for Copyright Protection of Medical Images," in IEEE Access, vol. 9, pp. 113714-113734, 2021, doi: 10.1109/ACCESS.2021.3104985.
3. W. Sun, J. Zhou, Y. Li, M. Cheung and J. She, "Robust High-Capacity Watermarking Over Online Social Network Shared Images," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 3, pp. 1208-1221, March 2021, doi: 10.1109/TCSVT.2020.2998476.
4. A. Alzahrani and N. A. Memon, "Blind and Robust Watermarking Scheme in Hybrid Domain for Copyright Protection of Medical Images," in IEEE Access, vol. 9, pp. 113714-113734, 2021, doi: 10.1109/ACCESS.2021.3104985.
5. A. M. Cheema, S. M. Adnan and Z. Mehmood, "A Novel Optimized Semi-Blind Scheme for Color Image Watermarking," in IEEE Access, vol. 8, pp. 169525-169547, 2020, doi: 10.1109/ACCESS.2020.3024181.
6. X. Xi, X. Zhang, Y. Sun, X. Jiang and Q. Xin, "Topology-Preserving and Geometric Feature-Correction Watermarking of Vector Maps," in IEEE Access, vol. 8, pp. 33428-33441, 2020, doi: 10.1109/ACCESS.2020.2973458.
7. Z. Yahya, M. Hassan, S. Younis and M. Shafique, "Probabilistic Analysis of Targeted Attacks Using Transform-Domain Adversarial Examples," in IEEE Access, vol. 8, pp. 33855-33869, 2020, doi: 10.1109/ACCESS.2020.2974525.
8. O. S. Faragallah et al., "Efficient HEVC Integrity Verification Scheme for Multimedia Cybersecurity Applications," in IEEE Access, vol. 8, pp. 167069-167089, 2020, doi: 10.1109/ACCESS.2020.3019840.
9. R. Wang, H. Shaocheng, P. Zhang, M. Yue, Z. Cheng and Y. Zhang, "A Novel Zero-Watermarking Scheme Based on Variable Parameter Chaotic Mapping in NSPD-DCT Domain," in IEEE Access, vol. 8, pp. 182391-182411, 2020, doi: 10.1109/ACCESS.2020.3004841.
10. Y. Cao, F. Yu and Y. Tang, "A Digital Watermarking Encryption Technique Based on FPGA Cloud Accelerator," in IEEE Access, vol. 8, pp. 11800-11814, 2020, doi: 10.1109/ACCESS.2020.2966251.
11. X. Xi, X. Zhang, Y. Sun, X. Jiang and Q. Xin, "Topology-Preserving and Geometric Feature-Correction Watermarking of Vector Maps," in IEEE Access, vol. 8, pp. 33428-33441, 2020, doi: 10.1109/ACCESS.2020.2973458.
12. A. Ansari, G. Saavedra and M. Martinez-Corral, "Robust Light Field Watermarking by 4D Wavelet Transform," in IEEE Access, vol. 8, pp. 203117-203133, 2020, doi: 10.1109/ACCESS.2020.3035912.
13. Y. Cao, F. Yu and Y. Tang, "A Digital Watermarking Encryption Technique Based on FPGA Cloud Accelerator," in IEEE Access, vol. 8, pp. 11800-11814, 2020, doi: 10.1109/ACCESS.2020.2966251.
14. H. Fang et al., "A Camera Shooting Resilient Watermarking Scheme for Underpainting Documents," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 11, pp. 4075-4089, Nov. 2020, doi: 10.1109/TCSVT.2019.2953720.
15. M. Du, T. Luo, L. Li, H. Xu and Y. Song, "T-SVD-Based Robust Color Image Watermarking," in IEEE Access, vol. 7, pp. 168655-168668, 2019, doi: 10.1109/ACCESS.2019.2953878.
16. J. Liu et al., "An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain," in IEEE Access, vol. 7, pp. 80849-80860, 2019, doi: 10.1109/ACCESS.2019.2915596.
17. Z. Zhu, N. Zheng, T. Qiao and M. Xu, "Robust Steganography by Modifying Sign of DCT Coefficients," in IEEE Access, vol. 7, pp. 168613-168628, 2019, doi: 10.1109/ACCESS.2019.2953504.
18. D. O. Muñoz-Ramírez, V. Ponomaryov, R. Reyes Reyes, C. Cruz Ramos and S. Sadovnychiy, "Embedding a Color Watermark into DC coefficients of DCT from Digital Images," in IEEE Latin America Transactions, vol. 17, no. 08, pp. 1326-1334, August 2019, doi: 10.1109/TLA.2019.8932342.
19. S. P. Mohanty, E. Kougianos and P. Guturu, "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT," in IEEE Access, vol. 6, pp. 5939-5953, 2018, doi: 10.1109/ACCESS.2018.2795478.
20. N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," in IEEE Access, vol. 6, pp. 19876-19897, 2018, doi: 10.1109/ACCESS.2018.2808172.

21. B. Ahmaderaghi, F. Kurugollu, J. M. D. Rincon and A. Bouridane, "Blind Image Watermark Detection Algorithm Based on Discrete Shearlet Transform Using Statistical Decision Theory," in IEEE Transactions on Computational Imaging, vol. 4, no. 1, pp. 46-59, March 2018, doi: 10.1109/TCI.2018.2794065.
22. F. Ernawan and M. N. Kabir, "A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold," in IEEE Access, vol. 6, pp. 20464-20480, 2018, doi: 10.1109/ACCESS.2018.2819424.
23. Hina Lala, "Digital image watermarking using discrete wavelet transform", in IRJET, vol. 04 issue. 1, Jan 2017.
24. X. Liu, C. Lin and S. Yuan, "Blind Dual Watermarking for Color Images' Authentication and Copyright Protection," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 5, pp. 1047-1055, May 2018, doi: 10.1109/TCSVT.2016.2633878.
25. Amy Tun and Yadana Thein, "Digital Image watermarking scheme based on LWT and DCT", in IACSIT, vol. 5, no. 2, April 2013, doi: 10.7763/IJET.2013.V5.557
26. Gaurav Chawla, Ravi Saini, Rajkumar Yadav, Kamaldeep, "Classification of watermarking based upon various parameters", in IJCAIT, vol. 1 issue.2, September 2012.
27. Z. J. XU, Z. Z.WANG, Q.LU, "Research on Image Watermarking Algorithm based on DCT", in Elsevier, ESIAT 2011, 10 (2011) 1129 – 1135.
28. A. Briassouli and M. G. Strintzis, "Locally optimum nonlinearities for DCT watermark detection," in IEEE Transactions on Image Processing, vol. 13, no. 12, pp. 1604-1617, Dec. 2004, doi: 10.1109/TIP.2004.837516.
29. J. R. Hernandez, M. Amado and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," in IEEE Transactions on Image Processing, vol. 9, no. 1, pp. 55-68, Jan. 2000, doi: 10.1109/83.817598.
30. Xiang-Gen Xia, Charles G. Boncelet and Gonzalo R. Arce, "Wavelet Transform based watermark for digital images", Optical Society of America, vol. 3, no. 12, December 1998, OCIS codes: (100.0100).
31. Nirmalraj, S., and G. Nagarajan. "Fusion of visible and infrared image via compressive sensing using convolutional sparse representation." ICT Express 7, no. 3 (2021): 350-354.
32. Dhanalakshmi, A., and G. Nagarajan. "Group-normalized deep CNN-based in-loop filter for HEVC scalable extension." Signal, Image and Video Processing (2021): 1-9.
33. Nirmalraj, S., and G. Nagarajan. "Biomedical image compression using fuzzy transform and deterministic binary compressive sensing matrix." Journal of Ambient Intelligence and Humanized Computing 12, no. 6 (2021): 5733-5741.
34. Dhanalakshmi, A., G. Nagarajan, and L. Balaji. "SHVC performance enhancement using superior step search algorithm." ICT EXPRESS 5, no. 3 (2019): 206-210