Multimedia Tools and Applications (2020) 79:501–554
https://doi.org/10.1007/s11042-019-08087-x

Analysis of frequency domain watermarking techniques in presence of geometric and simple attacks

Anshul Chopra[1] · Shailender Gupta[1] · Sangeeta Dhall[1]

Received: 6 December 2018 / Revised: 5 April 2019 / Accepted: 6 August 2019 /
Published online: 2 September 2019

Abstract
Protection of manuscript accessible online is always an apprehension for researchers. Many ideas had come up for copyright protection and authentication of such documents. One of the admired keys to provide safety to the owner's data is digital watermarking. It is the process of hiding the secret message (text, audio, image, logo, signature) into the document for providing authentication. A watermarking mechanism is said to be effectual if it offers high imperceptibility, robustness against attacks, security and last but not the least has the high correlation value of extracted watermark with the original one. Numerous survey papers are available in literature taking only a few techniques or parameters into account, but this paper takes almost all frequency domain (standalone and hybrid) methods in absence and presence of geometric and simple attacks and does an exhaustive analysis on the same. MATLAB software is used for implementation. Results illustrate the superlative technique under the influence of simple attacks is DWT-FFT, and under geometric attacks DWT-SVD is preeminent.

Keywords Digital watermarking · Geometric attack analysis · Simple attack analysis

1 Introduction

With the advancement in the internet and digital technologies, availability of online texts, images, sound or diagrams in digital form is on augment. Once digitalized the different

✉ Anshul Chopra
Chopraanshul80@gmail.com

Shailender Gupta
Shailender81@gmail.com

Sangeeta Dhall
Sangeeta_dhall@yahoo.co.in

[1] Department of Electronics Engineering, J.C.Bose University of Science and Technology, YMCA, Faridabad, India

elements such as images are all ‘equivalent’ and can be manipulated, merged, altered or mixed to create an endless variety of new works. This gives rise to problems of unauthorized access, copyright protection and exploitation of documents. As per the statistics provided by Online Copyright Infringement Tracker Latest wave of research (March 2018) from Intellectual property office [38] shown in Table 1, infringement on different types of content was recorded. According to the facts, the contravention of books and TV contents is escalating annually. To counter these intimidations, numerous techniques have been developed to do digital works challenging to copy, distribute and access without obligatory consent. These techniques are roofed under the head of Digital Rights Management (DRM).

Digital Rights Management comprises of techniques which are developed to keep a check over duplication, modification, and distribution of original works. Several DRM techniques are; employing access and copy control software’s, encryption techniques and digital watermarking. Access and copy control software facilitates the originator to keep a check on the free and illegal misuse of their work. These techniques ensure that only paid users should have a right to access the product. Encryption techniques provide procedures in which the message is altered into another form so that it can’t recite or recognize by the unauthorized person. Its goal line is to avert the interceptor from the acquisition of any information about the plain text from cipher text. Digital watermarking is the technique of hiding the special feature like a logo, signature, symbol, etc. in original work (Image, Video or Audio) so that unauthorized access of contents can be traced.

The Digital watermarking system comprises of embedding and detection part. [19] The embedding part receives the original image and watermark image, perform the embedding process and provide the watermarked image at the output. This process is described in Fig. 1(a). This image is sent at the sender side where the extraction process is applied to it, as shown in Fig. 1(b), which results in getting the watermark image. It offers ownership security of document, data and provides protection. [49]

Watermarking techniques can be classified on a different basis like working domain, human perception, application areas, type of document, etc. By domain, these are classified as spatial [64] and frequency domain. Spatial Domain Techniques work on the pixel value of the media or cover image. [57] The watermark is embedded as a result of modifying the pixel value of the cover image. LSB substitution is one of the simplest and most popular spatial domain methods. Frequency Domain Techniques embed a watermark by modifying the transform domain coefficient. These coefficients are created by transforming the detailed cover image into the frequency domain. [35] There can be various types of transformations such as Discrete Cosine Transform (DCT), Discrete

Table 1 Infringement by content type, based on consumption in the past 3 months

↑ Sign Increase (From last year) ↓Sign Decrease (from last year)	Music	Films	TV	Software	Books	Video-games	Sport Content	Any
2018	19%	19%	23%	20% ↓	13%	16%	21%	25%
2017	18%	21%	22%	26% ↑	11%	16%	NA	25%
2016	20% ↓	24%	20%	19%	12%	18%	NA	25%
2015	24%	23%	21%	20%	11%	18%	NA	27%

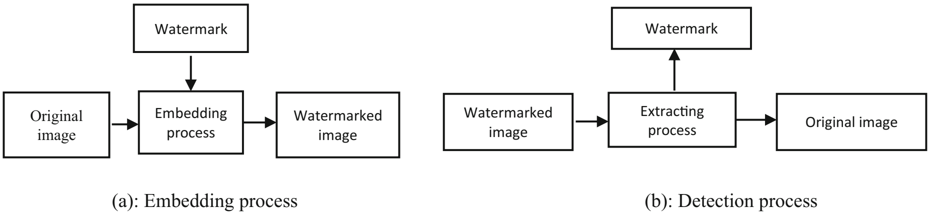


Fig. 1 (a): Embedding process (b): Detection process

Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Fractional Fourier Transform (FrFT), Hadamard transform, Singular Value Decomposition (SVD), Stationary Wavelet Transform (SWT), Lifting Wavelet Transform (LWT), and numerous amalgamation of these techniques. [11]. Former Techniques have various disadvantages such as attacks on the watermarked image can devastate the watermark image, sensitive to filters, suffers from signal compression and hostile attacks. [20] Latter are more robust against attacks in comparison to previous. Some of the desirable features of good watermarking schemes are enlisted below:

- Imperceptibility: It evaluates the quality of the watermarked image concerning the cover image after the insertion of a watermark. Visual inspection or qualitative analysis of snapshots of images before and after embedding is the measure of this property.
- Robustness: It is an important parameter to judge the watermarking technique, and it can be computed by the most probable attacks such as noise attack, removal attack, inversion attack, Gaussian attack, etc. The Peak Signal to Noise Ratio (PSNR), Mean Absolute Error (MAE) and Mean Square Error (MSE) are its measures. Also, Bit Error Rate (BER) is calculated which tells the number of bits to change before and after the attack in the host image.
- Security Analysis: The security analysis of a technique is done by comparing the pixel values, probability distribution and histograms between the cover and watermarked - image. A histogram is a graphical representation of the distribution of the data. Various parameters used to measure the security are Jaccard index, UIQI, Bhattacharya coefficient, etc.
- Data Extraction: It weighs the correlation between the extracted and original watermark. Bit Error Rate (BER) is its measure. It tells the number of bits changed between original and extracted watermark.

For a technique to be secured these parameters should have typical values or values close to the ideal values which imply decidedly less change in both images. This paper surveys various frequency domain watermarking schemes available in literature and does an exhaustive analysis by the parameters mentioned above.

The entire paper is organized as follows: Section II provides motivation and contribution by the author, Section III gives the description of frequency domain techniques with block diagrams, Section IV describes Performance metrics, Section V gives Snapshots along with results and Section VI draws the conclusion which is followed by references.

2 Motivation and contribution

Digital watermarking is one of the essential mechanisms for DRM; consequently, many researchers have implemented and published various algorithms. Due to the profusion of these techniques exhaustive survey of algorithms is sternly desirable. Numerous review papers are available in the literature describing the comparison of available methods based on various performance parameters; some of them are listed here.

As seen in Table 2, available papers in literature have given limited details of frequency domain watermarking techniques. Thus, this paper aims for the following contributions.

- An effort is made to cover almost every frequency domain watermarking techniques in different levels, i.e., standalone, two-level and three-level (the amalgamation of 2 or 3 technologies) to upsurge security of image.
- Comparison of methods is made on two different bases. First, without considering any attack and second by examining the most likely attacks such as simple attacks (Salt & Pepper, Gaussian, Poisson) and Geometric attack (Rotation attack).
- Numerous performance metrics are used for different types of analysis to get the best technique even in boisterous channels. Security analysis (Jaccard Index, Correlation coefficient, Intersection Coefficient, Bhattacharya coefficient, UIQI), Robustness analysis (MSE, MAE, PSNR, Bit- error) and Attacks (Salt & Pepper, Gaussian, Poisson, Rotation attack) are executed for comparison.
- After analyzing all parameters best technique is identified in absence as well as the presence of seizures. Results are presented for the ideal as well as realistic conditions.

3 Frequency domain watermarking techniques

The following symbols are used to describe the frequency domain watermarking techniques.

I = cover image	EW = extracted watermark
W = watermark image	EI = extracted cover image
WI = watermarked image	α = scaling factor

1) **DCT (Discrete Cosine Transform):** It is used to transform the image from the spatial domain to the frequency domain. This transformation is done in various steps [44] which includes division of the image into blocks of 8*8 as shown in Fig. 2 which is followed by reduction of dynamic range by subtracting value 127 from each pixel value so that new range lies between [−128, 127] instead of [0255]. These new values are then transformed into the frequency domain using a discrete cosine transform. This transformation divides the whole image into different frequency bands (low, medium and high) as shown in Fig. 3. Watermark is embedded in the middle frequency because visibility of image remains unaffected. Low subband contains the visual part of the image; high-frequency subband is removed by the quantization process. [63] Final step is quantization process, which is applied on the block due to given fact "human eye is fairly good at observing the small difference over a large area but not so good in case of high-frequency brightness operation". [1] For this process JPEG compression table is used, which is predefined and makes all high-frequency values rounded to zero and rest component values small in number.

Table 2 Survey papers in literature

S.NO	AUTHOR/YEAR	TECHNIQUES SURVEYED	ATTACKS	Comparison Criterion (out of four)
1.	Md. Asikuzzaman and Mark R. Pickering(2018) [7]	Four techniques are taken into account (SVD,DFT,DCT,DWT-SVD)	Four types of attack (cropping,Rotation, Gaussian, salt & pepper) for robustness analysis	Robustness -PSNR, Bit-Error and NC
2.	Khalid A. Al-Afandy and et.al (2018) [3]	Frequency domain-DWT,SVD,DCT and DSWT	Rotation, Gaussian, resizing, blurring	Robustness-PSNR and NC
3.	K. Sreenivas, V. Kamkshi Prasad (2018) [54]	Frequency Domain-DCT	No Attacks applied	Robustness- PSNR, NC security- UIQI, SSIM
4.	Snehlata Maloo1, N. Lakshmi and N.K. Pareek(2017) [53]	Frequency domain techniques-DCT,DWT,SVD	Gaussian, scaling and Rotation attacks	Robustness-PSNR
5.	G. Dinesh Kumar, Dontoju Pranay Teja, Sykam Sreekar Reddy, N. Sasikaladevi *(2017) [15]	Key generation algorithm	Noise test – Salt & pepper	Security analysis- Histogram, key analysis, correlation Robustness- PSNR, MSE
6.	H. R. Fazlali & S. Samavi & N. Karimi & S. Shirani 2(2017) [18]	Frequency domain-DCT,CT	Cropping attack, Gaussian	Robustness-PSNR,SSIM
7.	Sonam Tyagi and et.al (2016) [60, 46, 47]	Spatial Domain (LSB) and Frequency domain (DCT,DWT and DFT)	Discussed various attack: removal, interference, passive etc.	Robustness-PSNR,MSE,SNR,BER
8.	Qiudong Sun · Liandong Wang · Yufeng Shao · Jiancun Zuo(2016) [55]	Frequency Domain-DCT	Salt& Pepper, Gaussian Noise	Robustness-PSNR,BER
9.	Margarita Favorskaya,Eugenia Oreshkina(2015) [17]	Frequency domain-DCT,SWT	Geometric Attack	Robustness-PSNR,BER,NC
10.	Shahid Bashir Dar, Aasif Bashir Dar (2014) [12]	FFT, DCT and DWT	No Attacks applied	Others: Multi resolution and HVS characteristic

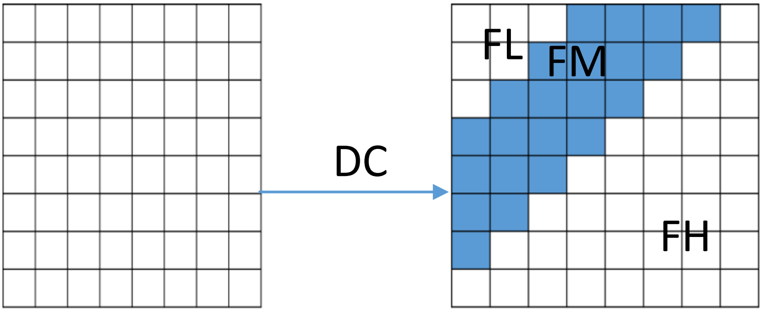


Fig. 2

Fig. 3

Fig. 2 and 3 Image is divided into 8*8 block. Different frequency band

Application: Used in pan card, I card of the employee of the company, fingerprint, medical imaging where low cost is required.

Where FL is low frequency sub band, FM is middle frequency sub band; FH is high frequency sub band.

3.1 Embedding process in DCT

In DCT algorithm, the cover image I and watermark image W are inputs and transformed into grayscale as shown in Fig. 4. On these images different steps are performed, initiating from division of image into blocks trailed by reduction of dynamic range by subtracting 128 from each pixel, in subsequent step 2-D DCT is applied, concluding step is quantization which is done by dividing each pixel block with the standard quantization Table (QI)/ (QW). [9]

For embedding the watermark, addition approach is used in which watermark (QW) is added with cover image (QI) after multiplication with scaling factor (α). To obtain watermarked image inverse quantization process is performed followed by inverse DCT and then adding 128 to each pixel. In this way, the watermarked image (W) is obtained.

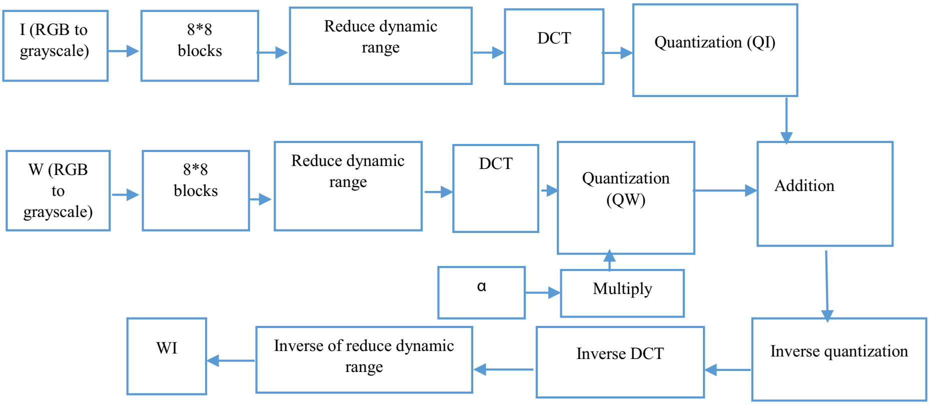


Fig. 4 Embedding process of DCT

3.2 Extraction process in DCT

This process is shown in Fig. 5. The watermarked image (WI) is divided into blocks, and the dynamic range is reduced by subtracting 128 from every pixel, DCT is applied then quantization process (QWI) is performed. Next Subtraction operation is performed between the watermarked quantization value (QWI) and cover image quantization value (QI) to retrieve the watermark. This difference is divided by the scaling factor followed by inverse quantization, inverse DCT, and inverted dynamic range to extract the watermark image (EW). Similarly, the cover image will be obtained by subtracting extracted watermark (EW) from quantization value of the watermarked image (QWI) and then an inverse process is performed to retrieve the cover image *(EI)*.

2) **DWT (Discrete Wavelet Transform):**

The Wavelet transform is an extensively used technique in image processing, watermarking, etc. Wavelets are oscillations which are rapidly decaying like waves having mean value zero and consist of finite duration. [23] Wavelet can be of two type's continuous and discrete wavelet. In continuous wavelet, the analyzing function is wavelet which compares the signal to shifted or compressed or stretched wavelet. Stretching and shrinking the message concerning time is called scaling. The relation between scaling and frequency: large scale factor-low frequency and vice versa. DWT performs wavelet decomposition using wavelet filters such as Daubechies, Haar, coiflets. The filter used for watermarking is Haar DWT which consists of two operations vertical and horizontal. DWT decompose the image into three spectral directions, i.e., horizontal, vertical and diagonal. Image of DWT is analyzed by allowing it to pass through the analysis filter followed by downsampling. Analysis filter bank consists of low pass and high pass filters at the decomposition stage. [58]

The procedure for Haar –DWT is as follows:

Step 1: Pixels are scanned left to right in the horizontal direction as shown in Fig.6, performing addition with neighboring pixel and store result in the left side. The difference operation result is stored on the right side. Low-frequency part (L) is represented by pixels' addition while high-frequency part (H) by pixel difference.

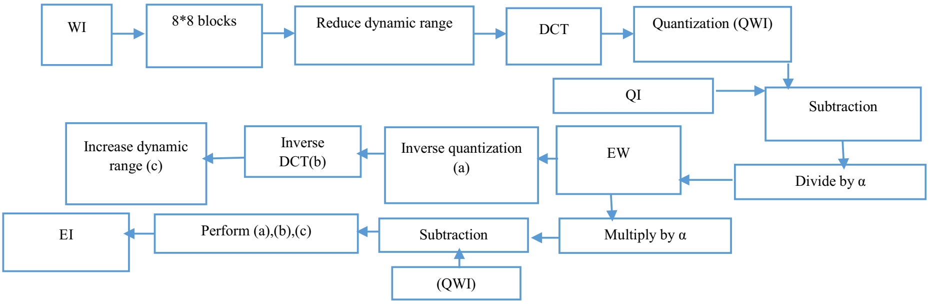


Fig. 5 Extraction process of DCT

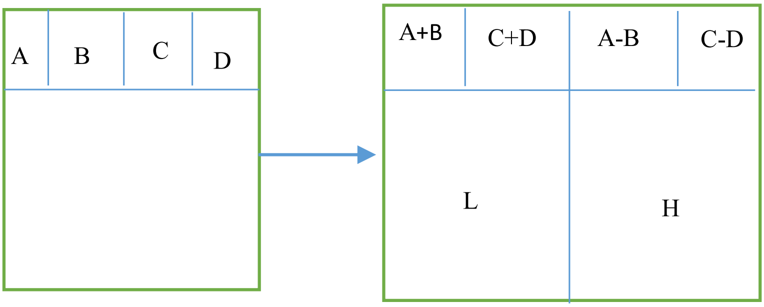


Fig. 6 Horizontal operation on first rows

Step 2: Pixels are scanned left to right in the vertical direction as shown in Fig. 7, performing addition with neighboring pixels and result store on the left, difference operation results at the right side. At last, the bands achieved are LL, LH, HL, and HH. The magnitude of the DWT coefficient is more significant in LL band also known as the approximation coefficient matrix. Most of the energy is concentrated in the LL band. Information of image like the smooth area is given by detailed coefficients matrix LH, HL, HH. Higher frequency part HH provides information about the sharp edges.

The advantage of DWT is that wavelets are localized in time and frequency around a certain point; it is designed to get good frequency resolution for low-frequency component and vice versa [39]

Application: Used to transfer more confidential matter like in military application, government application, broadcasting monitoring, advertisement and bank application, compression of signal and images. [4]

3.3 Embedding process in DWT

The embedding process is shown in Fig. 8. In 2D-Haar DWT operation the cover image (I) and watermark image (W) are converted from RGB to grayscale. On cover image, 2-D DWT operation (A) is applied which give approximation coefficient LL and detailed coefficients LH, HL, HH. The scaling factor is chosen (α) and multiplied with each pixel of the watermark (w). Also, one band out of four (LL, LH, HL, and HH) is selected to perform an addition operation. In this algorithm the chosen group is LL. Finally, apply inverse 2-D DWT to get the image *(WI).*

3.4 Extraction process in DWT

The extraction process is shown in Fig. 9. The 2-D DWT function is applied on the watermarked image (WI) and subtraction is performed between the same band of DWT (B) which is selected in embedding process and original image after 2D haar operation (A). After dividing by the scaling factor, inverse 2-D DWT is performed to receive extracted watermark image (EW). For the extraction of cover image (EI), the received watermark (EW) is multiplied by the (α) and subtracted from the watermarked (WI) after 2D haar operation (B). Inverse DWT is performed to retrieve the (EI). LL and LL3 are approximation coefficients of the original and watermarked image respectively.

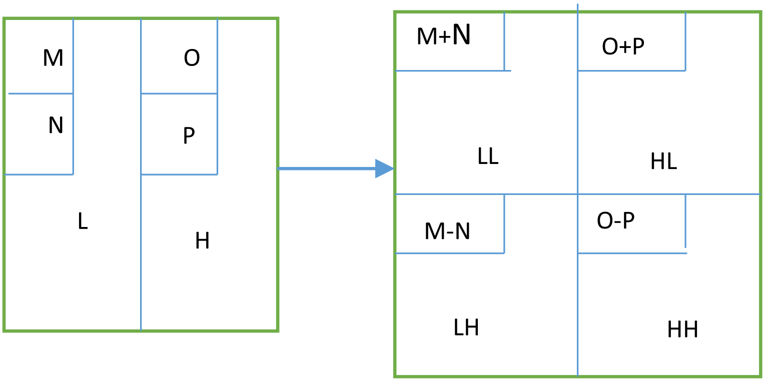


Fig. 7 Vertical operation

3) **DFT (Discrete Fourier Transform):**

It transforms the continuous function into a frequency domain which gives complex values consisting of both- magnitude and phase. [50] It is robust against various attacks like scaling, rotation, geometry. The dominant component of DFT is the main component with low frequency. Rotating the image through the angle in the spatial domain causes rotation in the same amount in Fourier representation. DFT magnitude of the signal can be altered without affecting the quality of the image because the human visual system is less sensitive to magnitude distortion as compared to phase alteration.

FFT (Fast Fourier transform) is an efficient algorithm to implement DFT which converts spatial to the frequency domain. It is an image processing tool used to decompose the image into cosine and sine component. Time to evaluate DFT on the computer depends on the number of multiplication N^2 whereas FFT only needs NLog2 (N). [13]

Application: Image construction, analysis, reconstruction and image compression.

3.5 Embedding process in DFT

This process is shown in Fig. 10. In DFT the(I) and (W) are inputs and converted into the grayscale image then 2-D FFT function is applied at both models which give (A) and (B) respectively. Watermark image (W) is multiplied by the scaling factor (α). The addition is performed up to the size of row and column of (W) image, between cover image pixel obtained by the FFT operation (A) and scaled watermark pixel (W, α). The resultant value of the pixel is used to find the inverse of FFT2 which gives the watermarked image (WI).

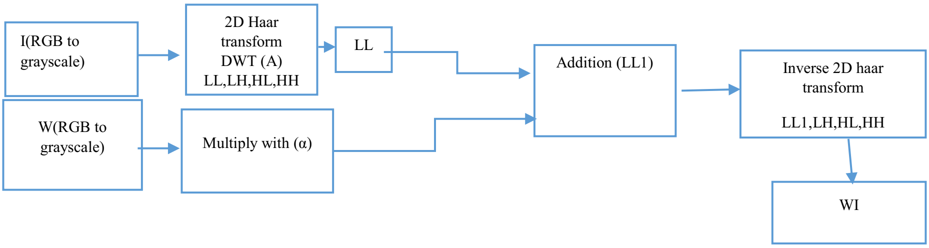

I(RGB to grayscale)
2D Haar transform DWT (A) LL,LH,HL,HH
LL
Addition (LL1)
Inverse 2D haar transform LL1,LH,HL,HH
W(RGB to grayscale)
Multiply with (α)
WI

Fig. 8 Embedding process of DWT

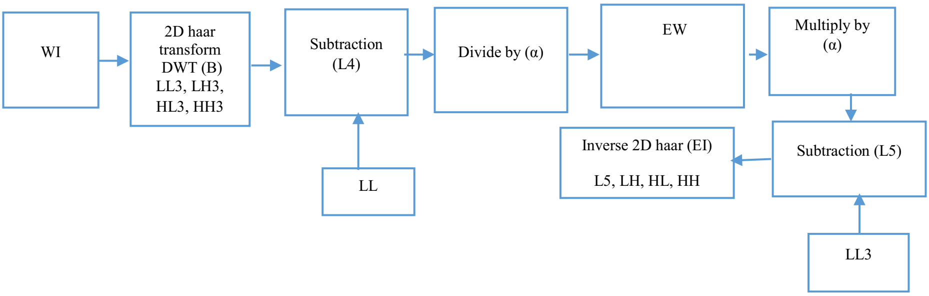


Fig. 9 Extraction process of DWT

3.6 Extraction process of DFT

This process is shown in Fig. 11. On *WI* image FFT operation is performed*(C)* and then the subtraction is done between the watermarked of FFT *(C)* and cover image*(A)* the result is divided by scaling factor *(α) and EW* is obtained by performing inverse FFT. In order to extract the cover image the *EW* is multiplied by the *(α)* and subtracted by the FFT of WI i.e. (*C)* the values of pixel obtained is inversed by the FFT process and retrieval of *EI* is attained. A and C are FFT inverse of original and watermarked image respectively.

4) **FRFT (FRactional Fourier Transform):**

It is a generalization of classical Fourier transform introduced in mathematics literature to solve differential equation in quantum mechanics. Other application of FRFT is in field of image manipulation, signal processing. Its output is combination of time and frequency component. [24]

FRFT of signal f (t) with p fractional order of transform is given by:

$$f_p = \int_{-\infty}^{+\infty} k_p(u,t) f(t) dt \qquad (1)$$

Where $k(u, t)$ is kernel function and is given by:

$$k_p(u,t) = \begin{cases} \delta(u{-}t), & \sqrt{1{-}j\cot\alpha}\exp[j\pi(u^2\cot\alpha{-}2ut\csc\alpha + t^2\cot\alpha)], \quad where\ \alpha{\neq}2\pi \\ & \alpha = 2n\pi \\ \delta(u+t), & \alpha = (2n+1)\pi \end{cases} \qquad (2)$$

Where $0 < |p| > 2$, u represent *pth* Fractional domain.

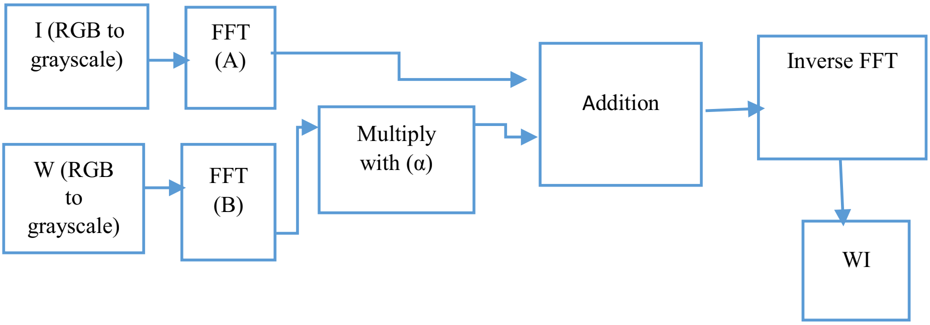


Fig. 10 Embedding process of DFT

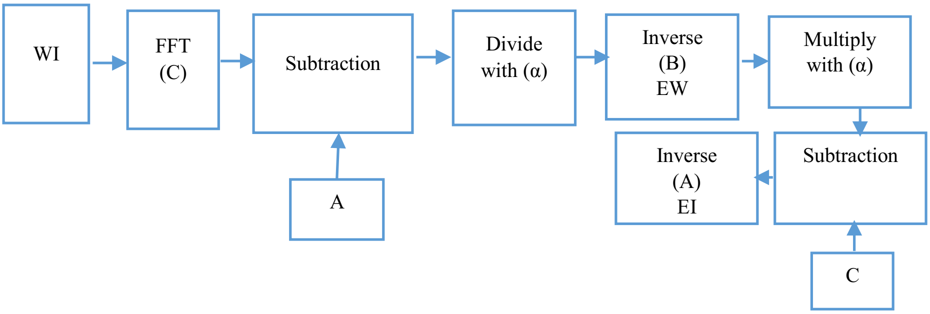


Fig. 11 Extraction process of DFT

2D DFRFT:

$$I(x,y) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(F_{\alpha_{1,\alpha_2}}\right)k_{-\alpha_{1,-\alpha_2(x,y,m,n)}} \tag{3}$$

where x, y are row and column of image with size of x varies from 0 to M-1 and y from 0 to N-1 and α_{1,α_2} is order of 2D-Frft.

When $p = 0$, FRFT coincide with identity operator and for $p = 1$ it coincides with Fourier operator. It corresponds to rotation in time frequency plane over an angle of$\frac{\pi}{2}$. Angle obtained will be purely time domain if $\alpha = 0$ and for frequency domain α=$p\frac{\pi}{2}$. [42]

3.7 Embedding process of FRFT

This process is shown in Fig. 12. Cover image *(I)* and watermark image *(W)* are inputs and get converted into gray scale. FRFT operation is performed on both the images *(I Frft)/ (W Frft).* Function used in FRFT take input image and fractional power value, if value = 0 then it is purely time domain. If value =2 then it is in frequency domain. For value laying between 1 and 2 it is in between frequency and time domain. Scaling factor is chosen *(α)* and multiplied with every pixel of watermark image *(W Frft).* Addition operation is performed with the cover image *(I Frft*). Inverse FRFT is performed on the pixel values obtained, which is referred as *WI.*

3.8 Extraction process of FRFT

This process is shown in Fig. 13. In FRFT to extract watermark and cover image *WI* is passed through FRFT process *(WI Frft)* with same fractional power value taken above for rotation. For extraction process the watermarked FRFT *(WI Frft)* is subtracted from the

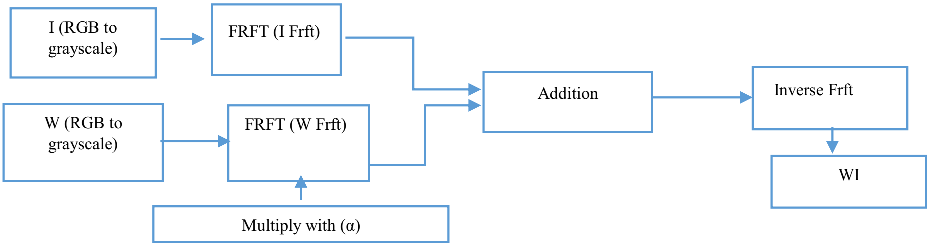


Fig. 12 Embedding process of FRFT

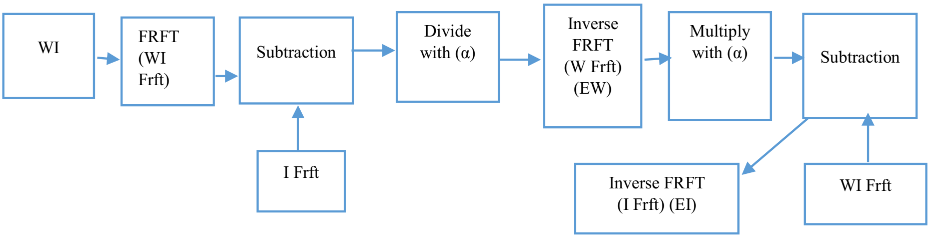


Fig. 13 Extraction process of FRFT

cover image *(I Frft*) and result is divided by (α). Inverse FRFT is performed to extract watermark *(EW)*. For the extraction of cover image the EW obtained is multiplied by the *(α)* and values obtained are subtracted by the *(WI Frft)*. Then resultant pixels undergone inverse FRFT and retrieval of (*EI) is* done.

5) **SVD (Singular value decomposition):**

SVD is a numerical technique used to diagonalize matrices in numerical analysis. It decomposes image of size M*N as: [48].

$$A = USV^T \tag{4}$$

Where U is M*M unitary matrix.

S is singular matrix of M*N with nonnegative number on diagonal and zero on off the diagonal side.

V^T is conjugated transpose of V which is N*N unitary matrix.

Properties of SVD:

1) Non negative number in S matrix represents the luminance value of image.
2) S matrix specifies the intrinsic geometry properties of image.
3) Singular values have slightly good stability means variations in value does not affect the visual perception of image.
4) Less effects of attacks on SVD technique. .
5) Output is more secure and robust.
6) It helps in achieving accuracy, imperceptibility.

This technique is applied to image compression, image hiding, image watermarking.

3.9 Embedding process of SVD

Cover *(I)* and watermark image *(W)* is first converted from RGB to gray scale image. SVD is applied on the original image *(a*), and singular matrix (*s1*) is used for watermark insertion. In embedding process, the watermark*(W)* is multiplied with scaling factor*(α)* then coefficient of cover image singular value pixel*(s1)* is added with watermark scaling pixel*(w*(α)).*

Take SVD again of embedded pixel *(a1)* followed by inverse of SVD *(a2*) with original image unitary matrix *(u1,v1)* and embedded image singular matrix values to make the size of watermarked image same as of original image WI is obtained after insertion. Whole process is shown in Fig. 14.

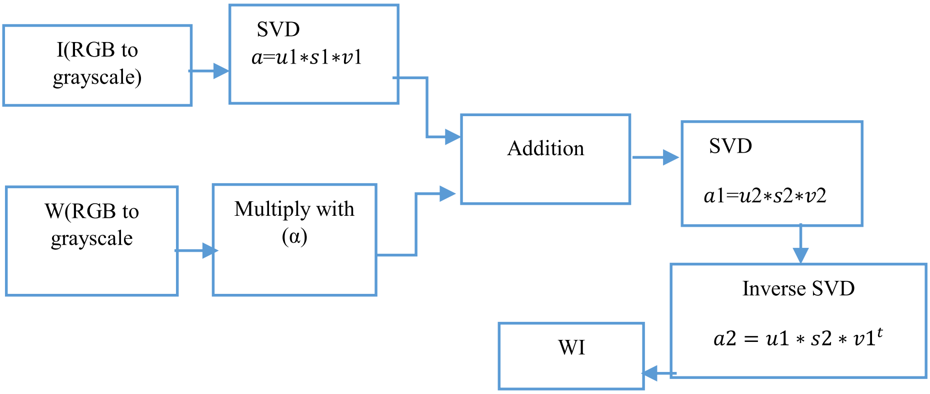


Fig. 14 Embedding process of SVD

3.10 Extraction process of SVD

On watermarked image *(WI)* SVD *(a3)* operation is applied and inverse *(a4)* is taken of watermarked singular coefficient with embedded matrix unitary matrix such as *U2* and *V2*. Extraction process is performed by subtracting the coefficient of inverse SVD singular matrix of watermarked image*(s3)* with original image singular matrix *(s1)* value then dividing with scaling factor value in order to obtained extracted watermark image *(EW)* from watermarked image (*WI*).

To receive the cover, image the singular value matrix of *WI* image *(s3)* is subtracted from the *EW* singular matrix (s5) after the multiplication of scaling factor thus inverse SVD (*EI*) is performed to get the *EI*. Complete extraction process is shown in Fig. 15.

6) **Contourlet transform**:

It is multidirectional and multi resolution transforms technique which analyses the image in contour, texture, fine details of image. It uses LP (laplacian pyramid) to decompose an image into LF (low frequency sub band) and HF (high frequency sub band). LF is obtained by filtering the cover image by 2D LPF and HF by subtracting the synthesized LF with the cover image but not by 2D HPF because, if HF coefficient changes it may affect the LF coefficient. LP spread the watermark in all the sub bands such as HF and LF which provide benefit at the time of attack that if HF sub band get destroyed then watermark can be easily restore from LF sub band. Contourlet is double filter band (FB) where LP is used to capture the point discontinuities, followed by directional filter bank (DFB) to link the point discontinuities with linear structure. It captures high frequency content like smooth contours and directional edges.

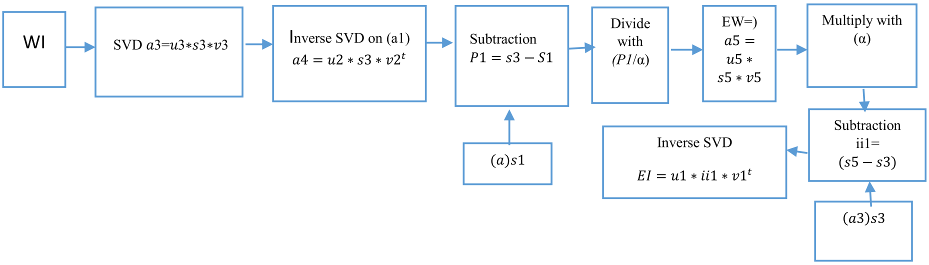

WI
SVD $a3$=$u3*s3*v3$
Inverse SVD on (a1) $a4 = u2 * s3 * v2^t$
Subtraction $P1 = s3 - S1$
$(a)s1$
Divide with $(P1/α)$
EW=) $a5 = u5 * s5 * v5$
Multiply with (α)
Subtraction ii1= $(s5 - s3)$
$(a3)s3$
Inverse SVD $EI = u1 * ii1 * v1^t$

Fig. 15 Extraction process of SVD

[16] Contourlet transform technique is more robust against attacks such as LF, gamma correction, histogram equalization, cropping etc. [33]

In Fig. 16 the cover image is decompose by LP into LF and HF sub band. LF sub band contain image size half of original image and HF image size same as cover image. HF is passed into DFB whereas LF into LP. Small value coefficients are presented by black and while the large coefficient by white. For n level DFB 2^n sub bands will be formed. [2]

Laplacian pyramid scheme is composed of analysis filter (H), synthesis filter (G), cover image (I), coarse approximation (c) (LF sub band), difference (r) (HF sub band), sampling matrix (M) as shown in Fig. 17.

Result image will be expansion than original by using basic elements like contour segment.

3.11 Embedding process of Contourlet

In Contourlet transform the cover image *(I)*,watermark image(*W*) converted from RGB2gray scale and then only *I* is decompose into contours using PDF (pyramidal directional filter bank) (y2) on the other side watermark image (*W*) pixel is multiplied with the (α) for embedding the watermark into main image the size of watermark is used to run the loop and pixel obtained by *y2* is added with the pixel obtained by the ($W^* \alpha$) than to combined the watermark into original image PDF reconstruction is performed to get *WI* image. This process is shown in Fig. 18.

3.12 Extraction process of Contourlet

WI image is firstly decompose using the *PDFdec (y6)* into the contours and for the extraction of watermark the pixel value obtained from the *y6* is subtracted from *y2 (PDFdec of I)* and then divide by the scaling factor this lead to extracted watermark (*EW*) from watermarked image. In order to extract the cover, image the *EW* extracted is multiplied with the (α) the pixel value obtained will be subtracted by the *PDFdec* of *WI (y6)* than *PDFrec* is performed to retrieve the extracted image (*EI*) as shown in Fig. 19.

7) **Hadamard transform:**

It is used extensively in image processing and compression of image. It is symmetric in nature and non-sinusoidal function. Normalized N*N matrix H must satisfy:

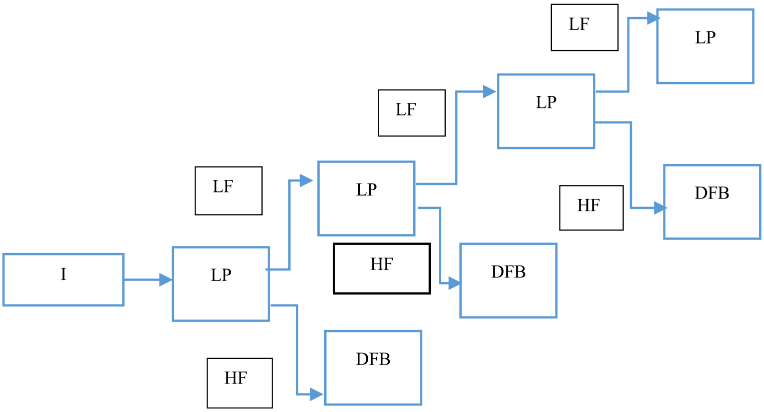


Fig. 16 LP analysis

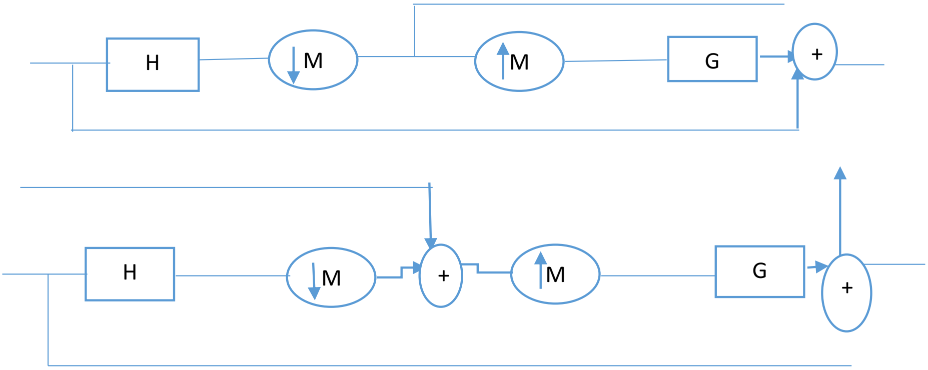


Fig. 17 LP reconstruction

$$HH^T = I$$

H is matrix of size N*N and H^T is transpose of H and there product must be equal to unitary matrix.

1D image F=Hf where H is Hadamard matrix and f is input image, in case of 2D F=HfH' as it is symmetric in nature so it can be rewrite as F=Hf. [58]

2*2 Hadamard matrix is given by: $= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, 4*4 matrixes is made by 2*2 matrix $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1. \end{pmatrix}$

Where I is unitary matrix.2 N*2 N matrix of Hadamard is given by:

$$H_{2N} = \frac{1}{\sqrt{2}} \begin{bmatrix} H_N H_N \\ H_N H_N \end{bmatrix} \tag{5}$$

3.13 Advantage

The transform matrix H_N are simple they are binary; row and column are orthogonal, real in nature. It is possible to embed the watermark coefficient in the low AC coefficient value increase the reliability, stronger in case of attacks, complexity is less as it require only addition or subtraction process. [41]

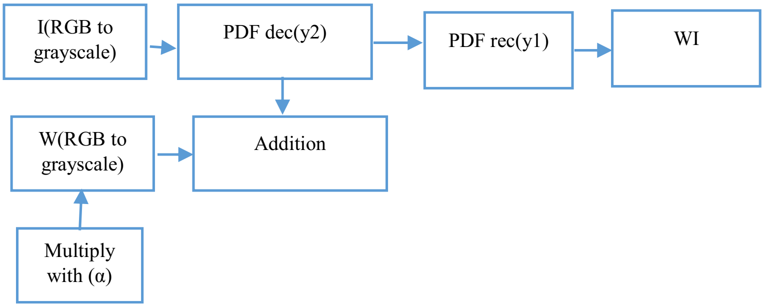


Fig. 18 Embedding process of Contourlet

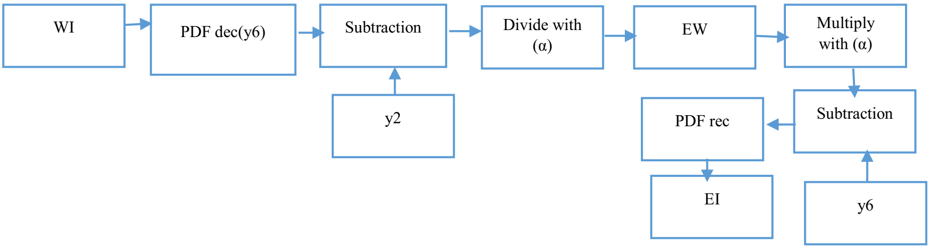


Fig. 19 Extraction process of Contourlet

3.14 Embedding process of Hadamard

In Hadamard transform the image *I* is first converted from RGB2gray and divide into 8*8 blocks. A random number is generated which is used in selection of blocks for embedding the watermark. The selected block is transformed by the fast Hadamard (*d*). On the other hand, *W* image is also converted from RGB2gray scale and is transformed by *Fwht (c)*. The size of *W* image is calculated and the loop will run for number of rows and column of *W* image addition operation is performed between the (*C*) and (*d*). After embedding, the inverse Hadamard transform is performed and modified block is again put into its location of the original image which gives *WI*. Complete embedding process is shown in Fig. 20. [62]

3.15 Extraction process of Hadamard

Extraction process is shown in Fig. 21.

WI is dividing into 8*8 block and again a same random number is generated and corresponding to that number block is selected for the extraction of both cover and watermark image. The selected block is transformed by *Fwht(d1)* and pixels obtained are subtracted by the pixel of *Fwht* of *I* image(*d*). The value obtained is divided by the (α), thus image obtained will be extracted watermark (EW). For the extraction of the cover image the *EW* pixels are multiplied by the (α) and the result is subtracted by the *WI fwht(c)*. The values obtained is inverse *Fwht* and the block is again put into the same location of *I* image in this way *EI* is obtained from *WI*

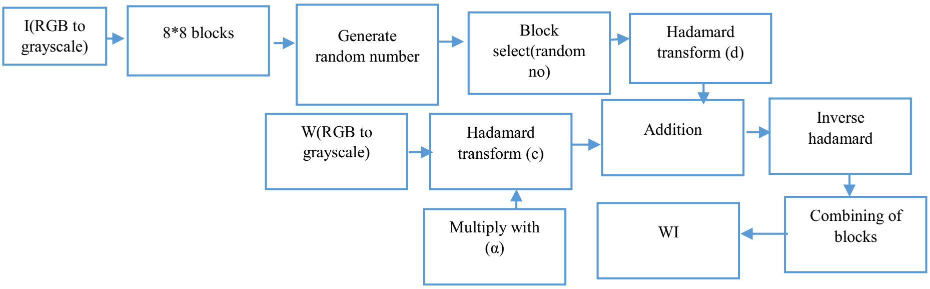


Fig. 20 Embedding process of Hadamard

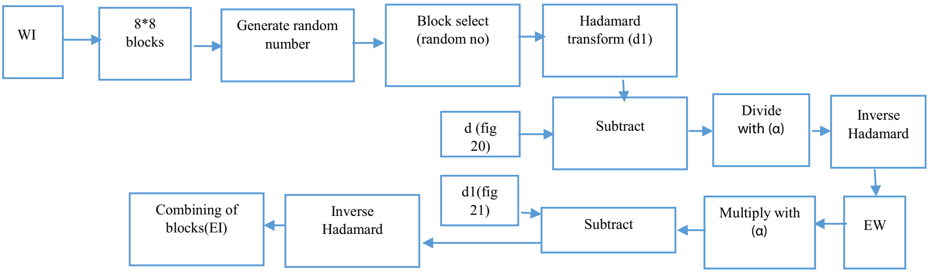


Fig. 21 Extraction process of Hadamard

8) Stationary wavelet transform

Stationary Wavelet Transform has been used to insert the robust watermark. The 1-level stationary wavelet transform decomposes an image into four sub bands as LL1, HL1, and LH1and HH1.

Matrix point of view SWT is given by:

$$Y = wy \tag{6}$$

Where Y is 1*N input vector, N is no of column in a matrix, W = (L + 1) N*N matrix, L no of decomposition level, y = (L + 1)1*N output matrix

$$W = [W_1, W_2, W_3, \ldots\ldots W_{L+1}]^T \tag{7}$$

W_i is N*N matrix and column of W_i is circularly shifted version of single vector which is ordinary DWT at ith scale and W_{L+1} is scaling function with largest scale value.

Inverse of transform is given by:

$$M = \left[\frac{1}{2}W_{1,}\frac{1}{2^2}W_{2,\ldots\ldots}\frac{1}{2^L}W_L\right] \tag{8}$$

Factor $\left[\frac{1}{2},\frac{1}{2^2}\ldots\ldots\ldots,\frac{1}{2^L}\right]$ are needed to offset the rising redundancy when scale becomes larger.

SWT follow important property that translation invariance means translation of original image, does not make the translation in corresponding wavelet coefficient. Translation invariance developed by removing the up and down sampler, which is part of DWT up sampler by padding zeros. SWT is linear, invariant, undecimated technique. [10]

There are several drawbacks such as computational complexity, lack of orthogonality, large output size.

3.16 Embedding process of SWT

In 2D-Haar SWT operation the cover image *(I)* and watermark image*(W)* is converted from rgb to gray scale. On cover image SWT2 operation *(A)* is applied which give approximation coefficient (*xar)* and detailed coefficient *(xhr, xvr, xdr)*. Scaling factor is chosen*(α)* and multiply with each pixel of watermark (*w)* also select one of the band from dwt2 function in which xar = LL band, xhr = HL band, xvr = LH band, xdr = HH band, in this algo the band selected is LL than perform addition operation. Apply inverse SWT2 the image received will be *(WI)*. This process is shown in Fig. 22. [56]

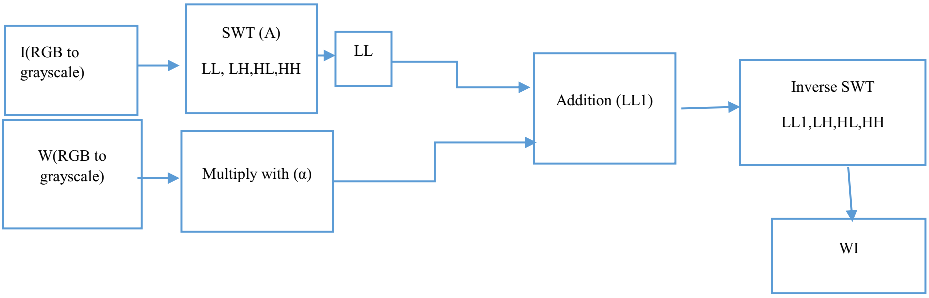


Fig. 22 Embedding process of SWT

3.17 Extraction process of SWT

The *(WI)* is passed through SWT2 and subtraction operation is performed between band of SWT*(B)* which is selected in embedding process and original image after 2D haar operation*(A)* then after dividing by scaling factor. Inverse SWT is performed to receive extracted watermark image *(EW)*. For the extraction of *EI* the received *EW* is multiplied by the *(α)* and subtracted by the WI 2D haar operation *(B)*. Inverse SWT is performed to retrieve the *(EI)*. This process is shown in Fig. 23.

9) **Lifting wavelet transform:**

Lifting wavelet transform is widely used in signal processing because of efficient implementation with low memory and computational complexity. This wavelet consists of three operations as shown in Fig. 24: split, predict and update operation. Let x (m, n) is original cover matrix: [29]

1) Split operation: Split of samples in odd $x_o(m, n)$ and even $x_e(m, n)$ samples sets

$$x_e(m,n) = x(m,2n) \tag{9}$$

$$x_o(m,n) = x(m,2n+1) \tag{10}$$

2) $2n$ is even multiple of number and $2n + 1$ odd multiple of number n .
3) Prediction operation also known as dual lifting it is used to predict odd sample set $x_o(m, n)$ from neighboring even coefficient .High pass coefficient $h(m, n)$ is calculated as a error in prediction of odd sample sets using prediction operator P.

$$h(m,n) = x_o(m,n) - P[x_e(m,n)] \tag{11}$$

$$x_o(m,n) = h(m,n) + p[x_e(m,n)] \tag{12}$$

This gives odd samples $x_o(m, n)$in terms of error and even sample set.

4) Update operator: known as primal lifting this operator help in producing low pass coefficient l $l(m, n)$and even sample is updated $u_h(m, n)$

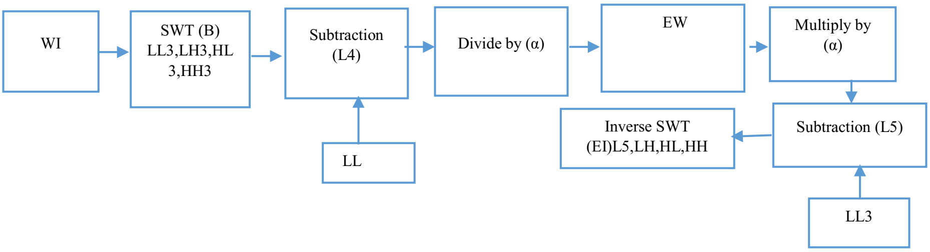


Fig. 23 Extraction process of SWT

$$I(m,n) = x_e(m,n) + u_h(m,n) \tag{13}$$

3.18 Advantage

1) Less computational complexity than convolution based algorithm.
2) No managing of image borders is needed.
3) All operation in one lifting stage can be performed in parallel. [24]

3.19 Embedding process of LWT

In 2D-Haar LWT operation, the cover image *(I)* and watermark image *(W)* is converted from rgb to gray scale. On cover image LWT2 operation *(A)* is applied which give approximation coefficient (*xar)* and detailed coefficient *(xhr, xvr, xdr)*. Scaling factor is chosen*(α)* and multiply with each pixel of watermark (*w)* also select one of the band from dwt2 function in which xar = LL band, xhr = HL band, xvr = LH band, xdr = HH band, in this algorithm the band selected is LL than perform addition operation. Apply inverse LWT2 the image received will be *(WI)*. This process is shown in Fig. 25.

3.20 Extraction process of LWT

The *(WI)* is passed through LWT2 and subtraction operation is performed between band of LWT*(B)* which is selected in embedding process and original image after 2D haar operation(*A)* then divide by scaling factor inverse LWT is performed to receive extracted watermark image *(EW)*. For the extraction of *EI* the received *EW* is multiplied by the *(α)* and subtracted by the WI 2D haar operation *(B)* inverse LWT is performed to retrieve the *(EI)*. This process is shown in Fig. 26.

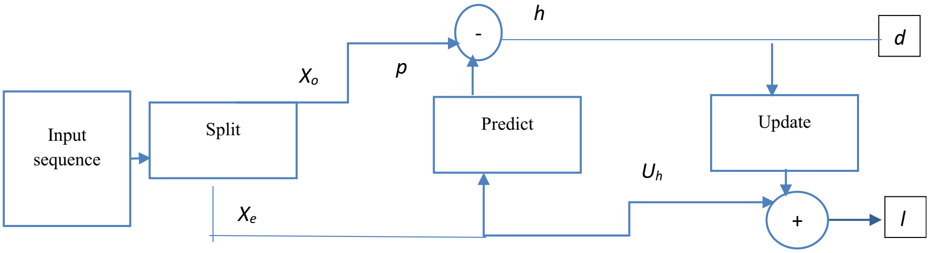


Fig. 24 LWT process

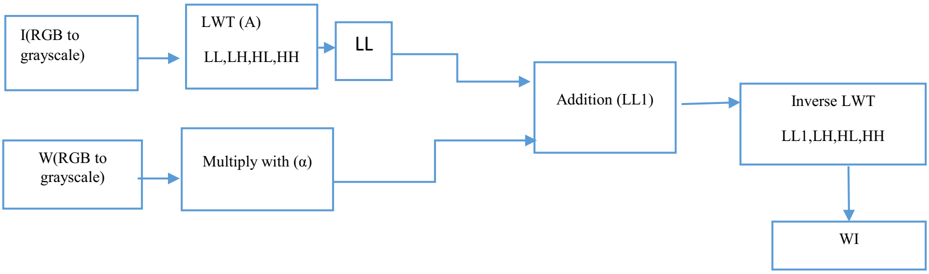


Fig. 25 Embedding process of LWT

10) **DCT-DWT technique**

It is a hybrid watermarking technique in which two techniques are used to provide better robustness, transparency to original and watermark image against different types of attacks such as cropping, scaling etc. This method is finer to LSB and DCT method. [30]

DCT is discrete cosine transform it is used to transform the image from spatial to frequency domain. It consists of real number values and it is symmetric in nature. Image at the output is divided into three frequency bands such as low, middle and high bands. Low frequency band and high frequency are suitable for embedding the watermark as most visible parts of image can be provided by these bands. High frequency band is not suitable for embedding so it is being removed by the process of quantization. Where the DWT is discrete wavelet transform and it decomposes the image into two coefficients, these are coarse and detailed coefficients. These consists of four bands LL, LH, HL, HH. LL band is generally preferred for embedding of watermark.

3.21 Embedding process of DCT-DWT

In the embedding process of DCT-DWT technique, cover *I* and watermark images *W* are first converted from rgb to gray scale followed by DCT($d1$) and DWT operations *I*. LL band is selected for watermark insertion, as it contains the largest magnitude of cover image. Add the pixel values of LL band with the watermark pixels of gray scale image after multiplying with the scaling factor (α). Perform inverse DWT and then DCT operation on sender side. Embedding process is shown in Fig. 27.

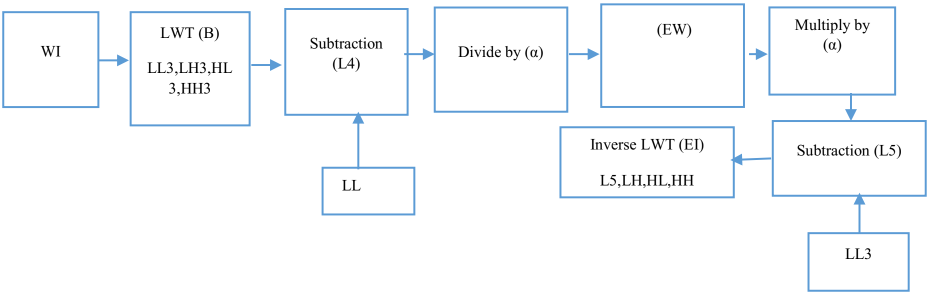


Fig. 26 Extraction process of LWT

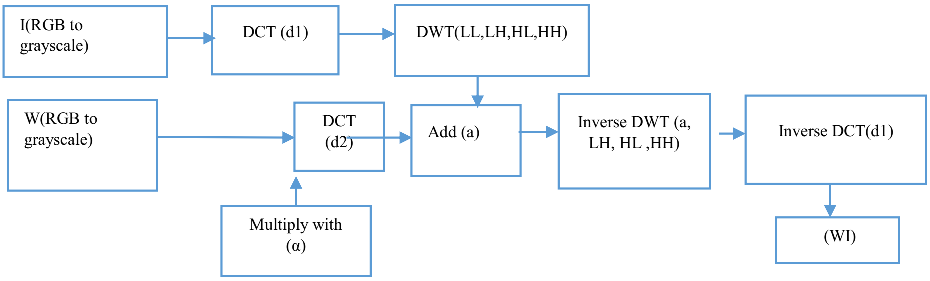


Fig. 27 Embedding process of DCT-DWT

3.22 Extraction process of DCT-DWT

At receiver side for watermark (*EW)* and cover image (*EI)* extraction from watermarked image (*WI),*firstly both undergoes DCT(*d3*) transformation and then DWT. LL band is selected (*LL1*) from *WI* image which is subtracted from the LL band (*LL*) of *I*. This difference is then divided by the scaling factor in order to obtained extracted watermark (*EW*). To obtain the cover image (*EI*) subtract the LL band of *WI* (*LL1*) with the *EW* pixels, obtained by multiplying with the value of scaling factor. Then apply inverse DWT and inverse DCT techniques to extract cover image (EI). Extraction process is shown in Fig. 28.

11) **DWT-SVD technique**

In this hybrid technique cover image is decomposed into 4 bands by applying DWT, such as lower resolution image (*LL*), vertical (*LH*), diagonal (*HH*), and horizontal (*HL*) bands are formed. *LL* band is selected for the singular value decomposition process, as magnitudes of DWT coefficients are largest in this band. SVD decompose the band into left singular vector, diagonal, and right singular vector. It provides good stability of image. [28]

It decomposes LL band of size M*N as: $A = USV^T$

Where U is M*M unitary matrix number of rows equal to number of columns, S is singular matrix of M*N with nonnegative number on diagonal and zero on the diagonal side, V^T is conjugate transpose of V which is N*N unitary matrix.

In this technique, embedding the watermark into LL band increases the robustness against various attacks such as rotation, cropping, filtering, scaling, and Gaussian without degrading the image quality. [34]

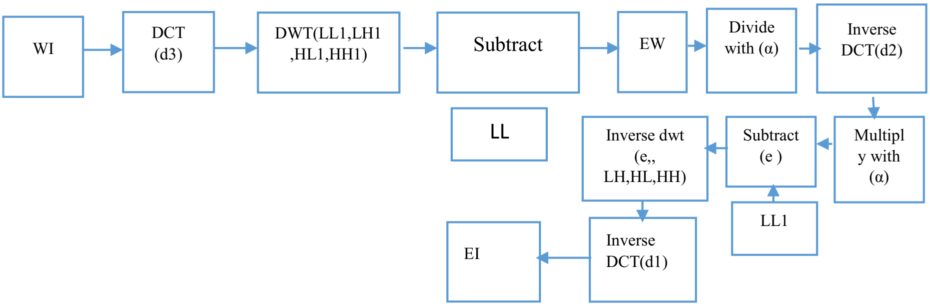


Fig. 28 Extraction process of DCT-DWT

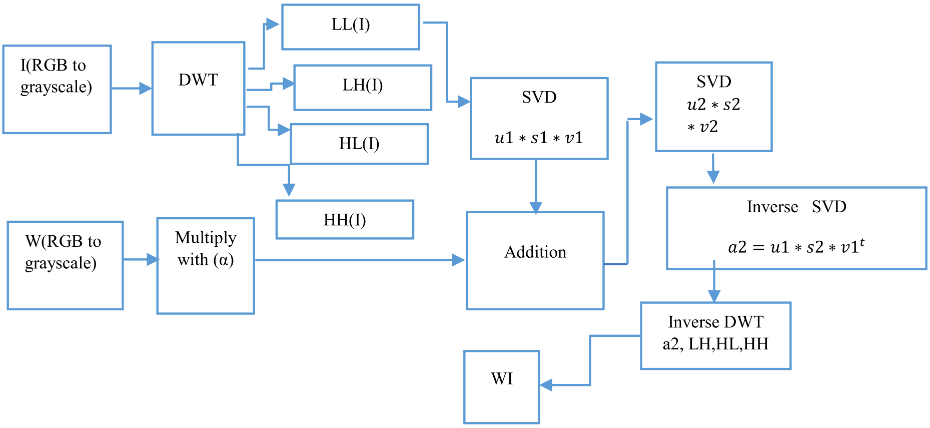


Fig. 29 Embedding process of DWT-SVD

3.23 Embedding process of DWT-SVD

Cover image *I* is read and converted to gray scale. Then DWT is applied which decomposes *I* into 4 bands. LL (I) band is selected for the embedding process, before embedding SVD (U1*S1*V1) is applied on LL (I) band. Diagonal matrix (S1) is used for further process. [31]

Watermark image *W* is read and converted to gray scale. Before performing addition method for embedding, watermark coefficient (*W*) is multiplied with scaling factor (α) and result is added with the diagonal matrix(S1) value of cover image. Again SVD (U2*S2*V2) is applied after watermark insertion followed by inverse SVD ($u1 * s2 * v1^t$). Then LL band is used in Inverse DWT to obtained *WI*. The U2*S2*V2 are used in further process of extraction. Complete process is shown in Fig. 29.

3.24 Extraction process of DWT-SVD

DWT is applied on the watermarked image *WI*, SVD (UW, SW, VW) is applied on the LL2 band of *WI* then inverse SVD $sw2 = u2 * sw * v2^t$is performed and values of left and right singular matrices are taken from embedding side. Retrieval of watermark image *W* is done by subtracting the *WI* (sw2) by the (s1) *I* image and dividing coefficient by scaling factor. This gives *EW*. For retrieval of cover image the *WI* (sw2) is subtracted by *EW* obtained by multiplying with the scaling factor in order to obtain *I* cover image. Inverse SVD $ii1 = u1 * ii * v1^t$ is performed on the coefficients obtained and then inverse DWT to extract cover image (*EI*). Extraction process is shown in Fig. 30. [26]

12) **LWT-SVD technique**

It is a hybrid robust technique which does not require human visual character (HVS) characteristics. In this technique two level lifting wavelet operations is performed on cover image followed by SVD operation. This method is robust against several attacks such as: cropping, rotation, JPEG compression, column removal. [65]

Lifting wavelet transform is widely used in signal processing because of efficient implementation with low memory and computational complexity. This wavelet consists of three operations: split, predict and update operation.

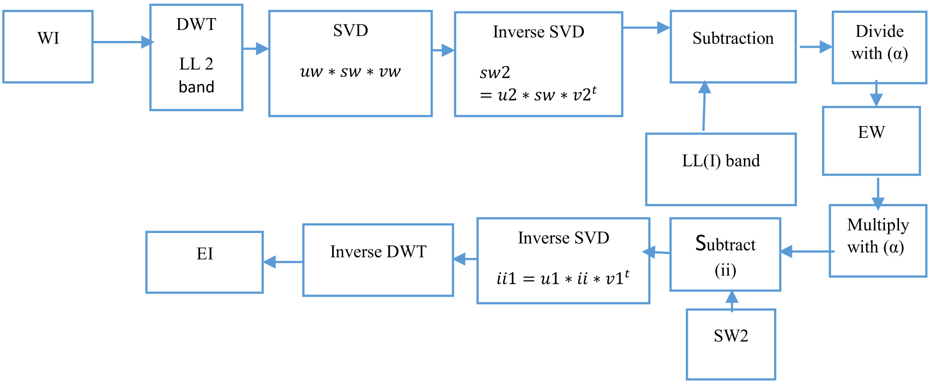


Fig. 30 Extraction process of DWT-SVD

Singular value decomposition has various applications in image processing such as image compression, image hiding, noise reduction because of these reasons that SVD image pixel does not change even if small interference is added to the image.

3.25 Embedding process of LWT-SVD

Cover Image *I* and watermark image *W* are converted to gray scale from RGB and then LWT1, LWT(1 W) is applied on the images, which decomposes the image into LL, LH, HL, HH bands and LL3, LH3, HL3, HH3 bands respectively. HH, HH3 bands are selected for next level LWT 2, LWT (2 W) operations in both the cases. HIH band is selected for the SVD (HH, HH3) operation. Diagonal matrix (sa) of watermark is multiplied with beta and addition is performed with the diagonal matrix (s) of cover image. SVD (S1) is performed on embedded *I* image followed by inverse SVD (s2) on S1 singular matrix *sa1*, to receive *WI* image. Then two level inverse LWT is performed. Embedding process is shown in Fig. 31.

3.26 Extraction process of LWT-SVD

LWT transform is done on watermarked image *WI* and 2nd level transform is applied on HH4 band. It is used for the SVD operation. Diagonal matrix(y) is used for retrieval of watermark from the original cover image diagonal matrix (s) using subtraction method and the result is

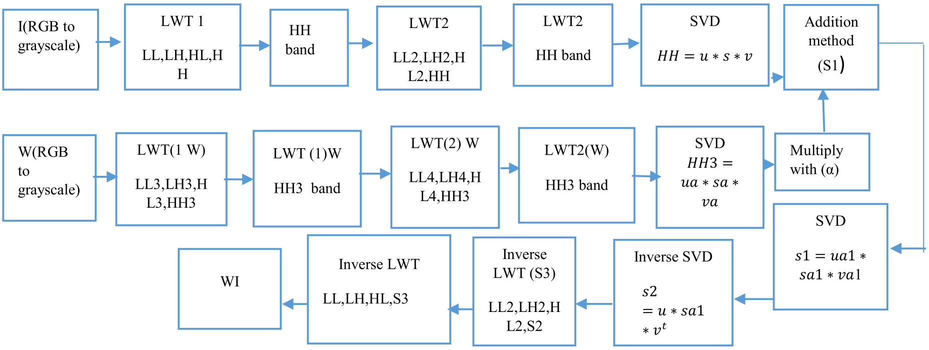


Fig. 31 Embedding process of LWT-SVD

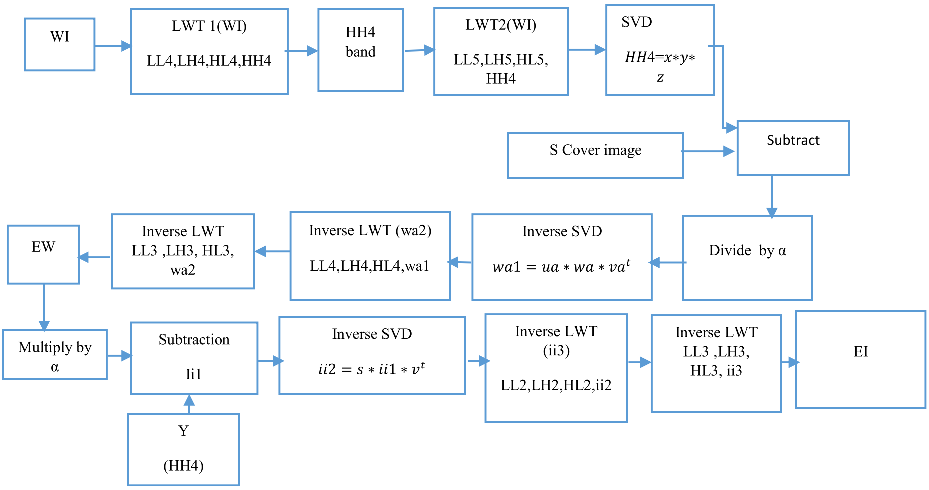


Fig. 32 Extraction process of LWT-SVD

divided by the scaling factor. Inverse SVD is applied to get the size of watermark followed by two levels LWT on HH band to get *EW*. Watermarked image (*Y*) is subtracted from the extracted watermark coefficient (*EW*) multiplied with scaling factor in order to obtain cover image coefficient. Finally, inverse SVD, inverse LWT is performed and using the value of inverse LWT again inverse operation of LWT is performed to extract cover image (*EI*). Extraction process is shown in Fig. 32.

13) **DWT-DFT technique**:

This technique is combination of DWT and FFT which provides robustness against attacks and in common image processing operation. [61] DWT is discrete wavelet transform in which after transformation the image is decomposing into 4 bands LL, LH, HL, HH and wavelet technique used is ‘haar’. The embedding is not done in HH band, as it is less robust against attacks. So embedding of watermark is done in low or middle frequency coefficients. In this technique the watermark is inserted in mid frequency such as LH or can be inserted in HL band also. Where L represents low pass filter and H represents high pass filter. It is widely used in signal, processing application. [27] Discrete fourier transform is a technique which transforms the image from spatial to frequency domain. It can provide FFT coefficient in terms of real part, imaginary part, magnitude, phase angle. This transform is faster than DFT as multiplication required to calculate N point DFT is less i.e. (N/2) [log_2N], where as in DFT it isN^2. [22]

3.27 Embedding process of DWT-DFT

Cover image *I* and watermark image *W* are converted from rgb to gray scale. Both images are transformed by using DWT method and its LH band is used for embedding process but before that on LH band FFT i.e. (FFT (I), FFT (W)) is performed. The coefficients obtained after FFT of both images are used for addition method in which watermark is inserted. The FFT coefficient FFT (W) of watermark is multiplied by the scaling factor and value is added with the FFT coefficient of cover image FFT (I). Inverse FFT is performed on the embedding coefficient and this value is used as LH coefficient value in case of inverse DWT to obtained watermarked image *WI* as shown in Fig. 33.

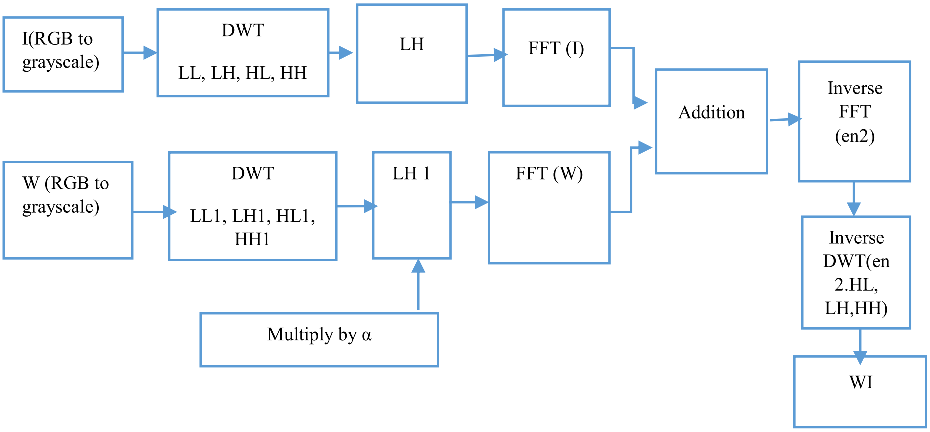


Fig. 33 Embedding process of DWT-DFT

3.28 Extraction process of DWT-DFT

Watermarked image *WI* is decomposed into four bands by using DWT method. LH2 band is selected for FFT operation. To extract the watermark from *WI* coefficient of FFT (WI) the coefficient of FFT(I) image is subtracted and divide by the scaling factor. In order to obtain the watermark coefficient than inverse FFT and inverse DWT are performed which gives extracted watermark (EW).

To extract the cover image (*EI*) from the *WI* image the *EW* image coefficients are multiplied by the scaling factor. This value is used to subtract from the FFT (WI) image and *EI* image coefficient are obtained. Than inverse FFT and DWT is performed to retrieve *EI*. This process is shown in Fig.34.

14) **DWT-FFT-SVD:**

This is three level hybrid watermarking technique which is a combination of DWT-FFT-SVD. DWT utilize the horizontal and detail coefficient values of 2D image in DWT. The translation problem is overcome by using FFT thought it exploit Frequency characteristics and SVD is used to embed the watermark [37].

DWT splits the image into four bands LL, LH, HL, HH bands where L represents low pass filter and H represents high pass filters. First filter denotes the horizontal direction while the

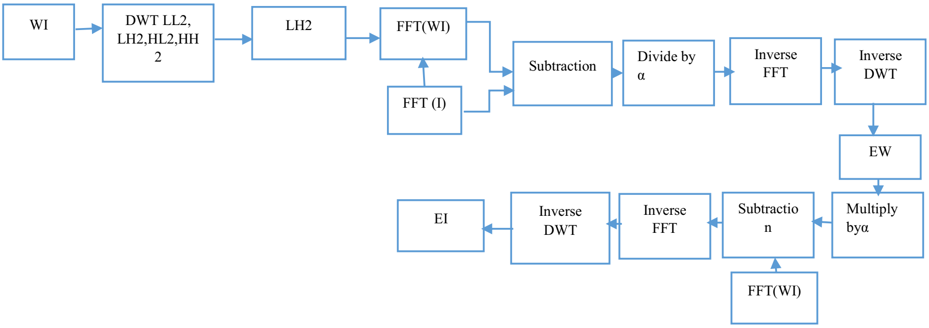


Fig. 34 Extraction process of DWT-DFT

2nd filter vertical direction. It helps in image compression and wavelet presents are of various types such as 'Haar', 'Daubechies', 'Coifelts'. DWT can be decomposed into various levels. [30] DFT transforms the image from spatial to frequency domain it provides effective distribution of energy. It provides immunity against rotation, scaling, translation.

SVD decomposes the image into left singular matrix, diagonal, right singular matrix.

3.29 Embedding process of DWT-FFT-SVD

Cover image *I* and watermark image *W* are transformed using DWT and its LL band is used for FFT transform, as the largest magnitude value can be found in LL band. FFT is performed on LL band to transform image in frequency domain than SVD is applied on the FFT coefficient. Singular values of diagonal matrix in both the images are used for embedding the watermark using addition method. Diagonal matrix of *W* image is multiplied by scaling factor and added with the Diagonal matrix of *I* image. Finally, inverse operation is performed, first inverse SVD than inverse FFT followed by inverse DWT to obtained watermarked image (*WI*). Embedding process is shown in Fig. 35.

3.30 Extraction process of DWT-FFT-SVD

Watermarked image *WI* is split into four bands and its LL band is used for FFT operation. The coefficients are transformed by SVD method. Inverse SVD is performed to get *WI* image. To extract the *W* image *WI* coefficient are subtracted by the diagonal matrix of *I* image and value obtained is divide by the scaling factor. Inverse SVD is performed on the coefficients followed by inverse FFT and then DWT to obtained *W* image.

In order to obtain *I* image the *W* image coefficient are multiplied by the scaling factor. The values obtained are subtracted by the *WI* coefficient and in this way *I* image coefficient are obtained and finally inverse SVD, inverse FFT and inverse DWT is applied to obtain *I* image. Extraction process is shown in Fig. 36.

15) **SWT-SVD:**

SWT is stationary wavelet technique; it is used because of its non-decimation and shift invariance property. SWT like DWT also split the image into four bands LL, LH, HL, and HH. It is also known as undecimated transform as there is no down sampling performed. LL

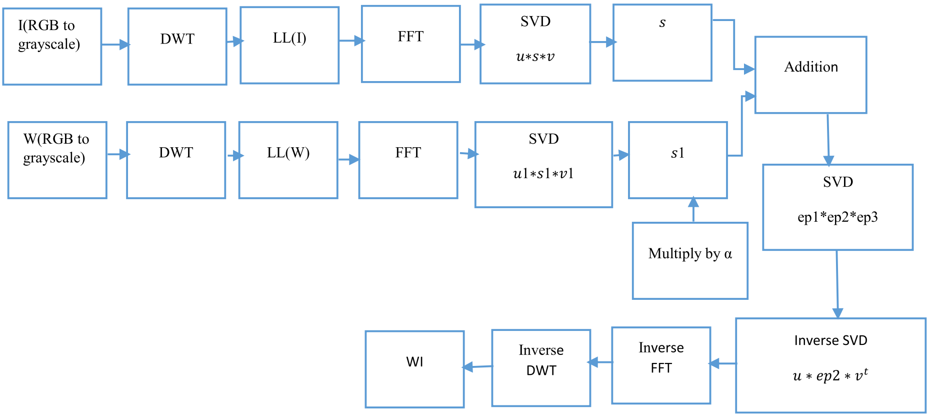


Fig. 35 Embedding process of DWT-FFT-SVD

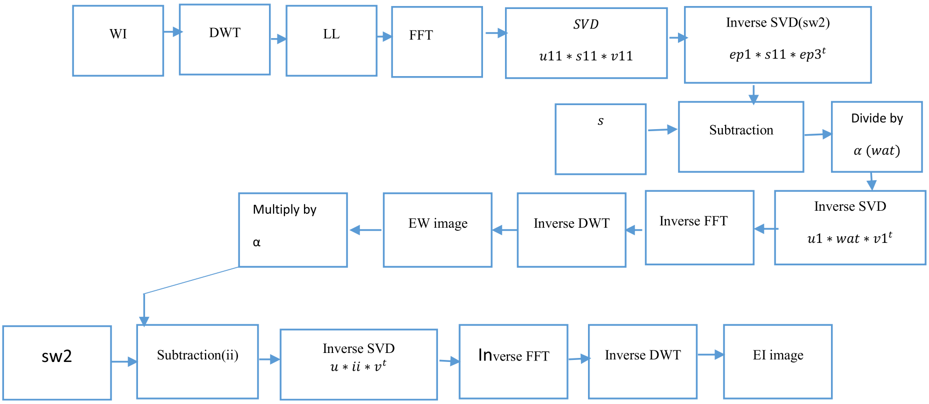


Fig. 36 Extraction process of DWT-FFT-SVD

gives low frequency sub band and LH, HL, HH gives horizontal, vertical, diagonal feature of image [36]. SVD decompose the image into left singular matrix U_x, diagonalS_x, right singular matrix. It provides good stability means lesser number of values altered when watermark is embedded. [66] It is also used to find the Eigen value and vector of image. [59]

3.31 Embedding process of SWT-SVD

Cover image *I* and watermark image *W* are first converted from RGB to gray scale. On both images SWT is applied, which splits the image into four bands, out of which HH band is used for further process. HH band of both images is transformed by applying SVD. Their singular value matrix is used in this hybrid technique to insert the watermark.

For embedding process, the singular value of *W* image coefficient is multiplied with the scaling factor and with singular value of *I* image coefficient addition is performed. To get the *WI* image inverse SVD is applied. The value obtained after embedding followed by inverse SWT uses HH band value of SVD. Finally, *WI* image is obtained.

This process is shown in Fig. 37.

3.32 Extraction process of SWT-SVD

Watermarked image *WI* image is transformed by applying SWT and its HH band is used for SVD operation. Again their singular values are used for extraction process. Singular value in case of *WI* and *I* image singular value coefficient are subtracted than divide by scaling factor. Inverse SVD is performed with inverse SWT in order to obtain the *EW* image.

For *I* image the coefficient of *EW* image is multiplied by scaling factor and subtracted from *WI* singular value. Inverse SVD and Inverse SWT are performed to retrieve full image of *EI*. Extraction process is shown in Fig. 38.

16) **DWT-DCT-SVD:**

DWT is used to transform the image from spatial to frequency domain by splitting the image into 4 bands which give approximate (LL band) and detailed coefficient (LH, HL, HH). [51] DCT is discrete cosine transform and used to provide the high robustness in the image. It is used in image and video compression. SVD is singular value decomposition and it

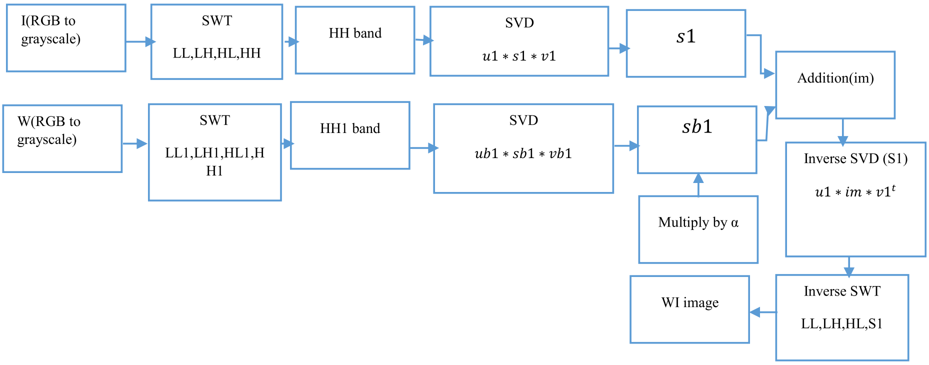


Fig. 37 Embedding process of SWT-SVD

decomposes the matrix into left singular value, right singular value and diagonal matrix. SVD have various advantages such as it provides good stability in the values of image. When distortion is added the value change in singular matrix is less. Singular value specifies the luminance of the image. The combination of three level hybrid techniques is more robust and provides better security against the standalone techniques. [25]

3.33 Embedding process of DWT-DCT-SVD

The cover image *I* and watermark image *W* are converted from RGB to gray scale. The image is transformed by using two levels DWT, 1stlevel DWT use LH band and 2nd level use HL band which split the both images into 4 bands. The band used for further process is HLr1 band as most of the visibility of the image is found in HH band. DCT transformation is performed on HLr1 band than the pixel obtained are passed through the SVD transform in which singular matrix (S1) is used for the embedding of watermark.

In embedding process, the singular value matrix of *W* (s2) image is multiplied with the scaling factor and then addition is performed with the singular value of *I* (s1) image. The pixels obtained are transformed using SVD inverse. SVD is performed followed by inverse DCT and then inverse 2 level DWT is performed to obtained *WI* image. This process is shown in Fig. 39.

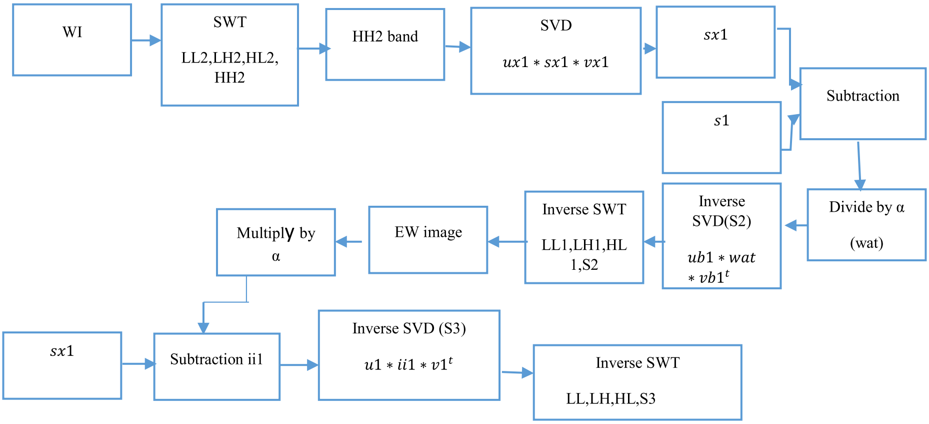


Fig. 38 Extraction process of SWT-SVD

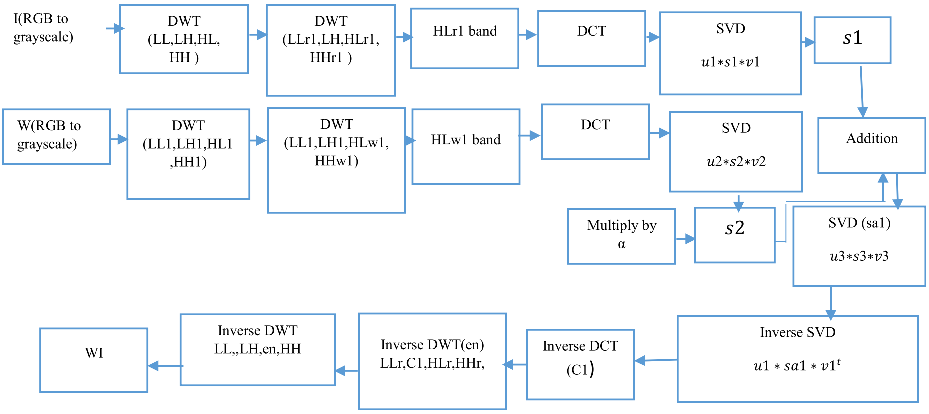


Fig. 39 Embedding process of DWT-DCT-SVD

3.34 Extraction process of DWT-DCT-SVD

Watermarked image *WI* is decompose using 2 level DWT and its HLr2 band is selected for the DCT transformation and the pixel obtained are than passed by the SVD technique. Inverse SVD is performed to obtain the *WI* image on receiver side. To extract the *EW* image the WI (s4) pixels value are subtracted from the singular matrix obtained by the SVD operation on I (s1) image. Then the value is divided by the scaling factor in order to obtain the *EW* image. Finally inverse SVD, inverse DCT and inverse 2 level DWT is performed.

For extraction of *EI* image the *EW* image obtained at receiver side is multiplied by the scaling factor and the value obtained is subtracted by the singular value of I (s1) image obtained by the SVD operation. Inverse SVD is performed than inverse DCT and inverse DWT to obtained *I* image at receiver side, after the extraction of watermark from watermarked image which gives *EI*. Extraction process is shown in Fig. 40.

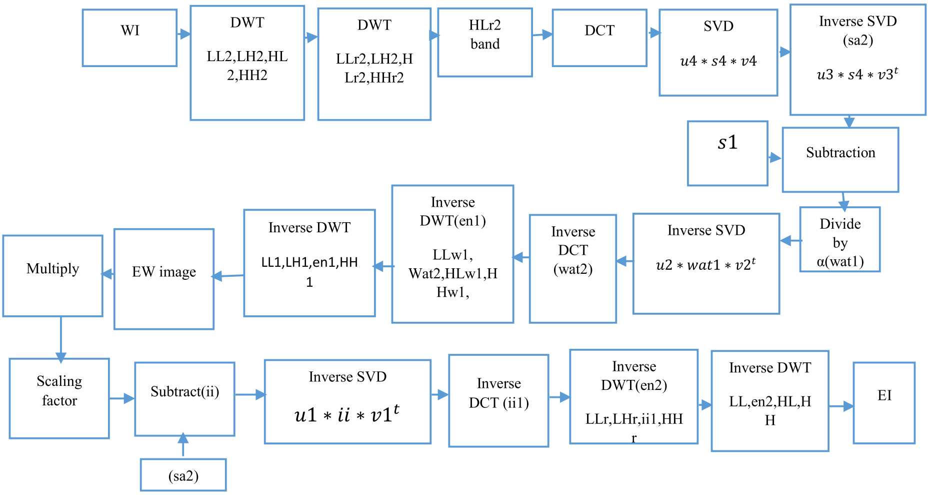


Fig. 40 Extraction process of DWT-DCT-SVD

17) **DWT-HADAMARD-SVD:**

DWT have an advantage of inserting the watermark in high resolution area which is less noticeable to human visual system this improves the quality and robustness of an image. Hadamard offer the simplicity and fastest calculation in the coefficient of transform where as SVD is used for stability and it also store maximum energy of an image. [21] DWT is used to transform the image from spatial to frequency domain by splitting the image into 4 bands which give approximate (LL band) and detailed coefficient (LH, HL, HH). Detailed coefficients are corresponding to the edges and texture of image.

Hadamard transforms the image signal in value of −1 or 1. SVD decompose the image into left singular matrix, diagonal, right singular matrix. It provides good stability means lesser number of values altered when watermark is embedded.

3.35 Embedding process of DWT-HADAMARD-SVD

Cover image *I* and watermark image *W* are first converted from RGB to gray scale. For DWT-Hadamard-SVD hybrid technique the DWT is performed on both (I, W) the images and which split the image into four bands. In this technique the HH band is selected for DCT transformation and value obtained by DCT is passed by the SVD transform from which the singular value matrix of both images are used for embedding process but before that the singular matrix obtained by SVD operation, *W* image is multiplied by the scaling factor and then the coefficient value (s2) is added by the singular matrix obtained by the I (s1) image SVD operation. SVD is applied to the values obtained by addition, Inverse SVD is performed on the pixels to put the watermark into cover image, than inverse Hadamard transform and its value is used as HH band in inverse DWT operation. In this way the watermark is inserted in the cover image. *WI* image is obtained. This process is shown in Fig. 41.

3.36 Extraction process of DWT-HADAMARD-SVD

Watermarked image *WI* is transformed by the DWT operation in which the HH band is selected for the DCT operation and pixel obtained by such operation are used in SVD transform. Inverse SVD is performed to receive the watermarked image pixel at the receiver side. Singular matrix obtained after inverse SVD (SA) is used for extraction of watermark and cover image.

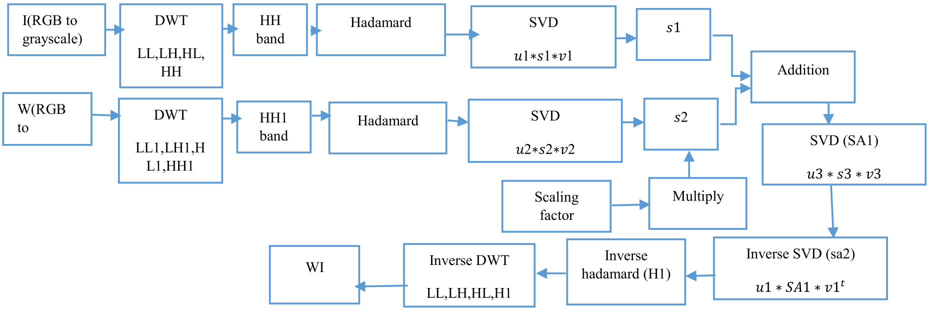


Fig. 41 Embedding process of DWT-HADAMARD-SVD

Singular matrix obtained from WI (SA) is subtracted from the singular matrix obtained by I (s1) image. The result is divided by scaling factor to obtain the *W* image. Inverse SVD is performed then inverse Hadamard which is used as HH band for inverse DWT technique. In this way watermark (EW) is extracted at receiver side from watermark image.

To extract cover image the *EW* image pixel are multiplied with the scaling factor, the value obtained after such operation is subtracted from the singular matrix of watermark (s2) image. Again inverse SVD transformation is performed followed by inverse Hadamard and inverse DWT, *EI* is retrieved. This process is shown in Fig. 42.

18) **DCT-SVD**

DCT is used in image compression and image processing. It is robust against attacks such as noising, compression, sharpening and filtering. The primary application is the pan card, I-card, fingerprint, etc. [8]. SVD decomposes the image into left singular matrix, diagonal, right singular matrix. It provides excellent stability means a lesser number of values altered when the watermark is embedded. It is also used to find the Eigen value and vector of the image. [40]

3.37 Embedding process of DCT-SVD

Cover and watermark images I and W respectively are converted from RGB to grey scale. I, W images are scrambled by performing zigzag operation now (a1, b1) image is divided into the 8*8 block, and DCT transform is applied on each block, and dc coefficient value is calculated. SVD is used on each DC coefficient and on (b1). For embedding the watermark singular matrix of both DC coefficient (s1) and watermark, SVD (s2) is used, and addition is performed. Than SVD of the embedded coefficient is applied, the value obtained is divided into 8*8 blocks, and DC coefficient is taken on which inverse DCT is implemented and put the DC coefficient again back at their same location after the modification. WI is obtained. This process is shown in Fig. 43. [45]

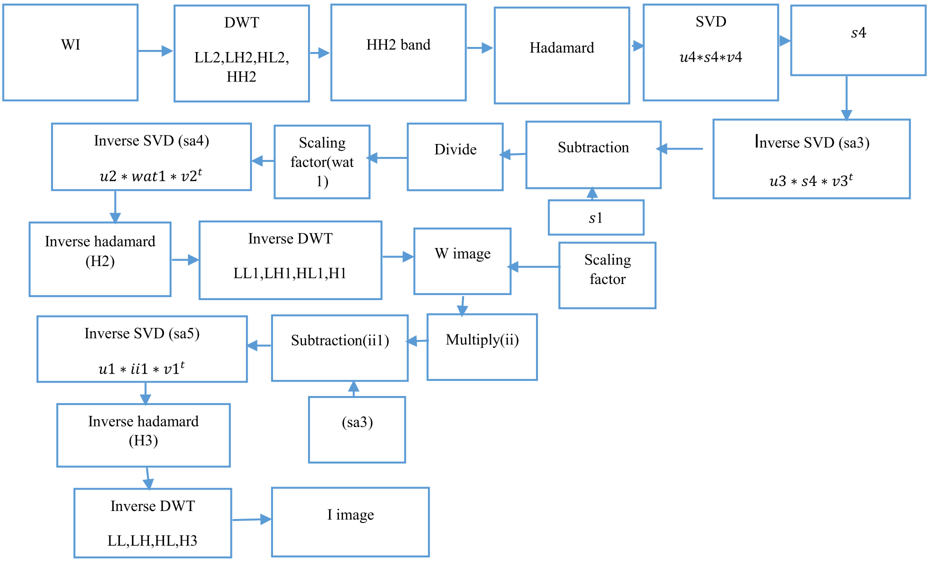


Fig. 42 Extraction process of DWT-HADAMARD-SVD

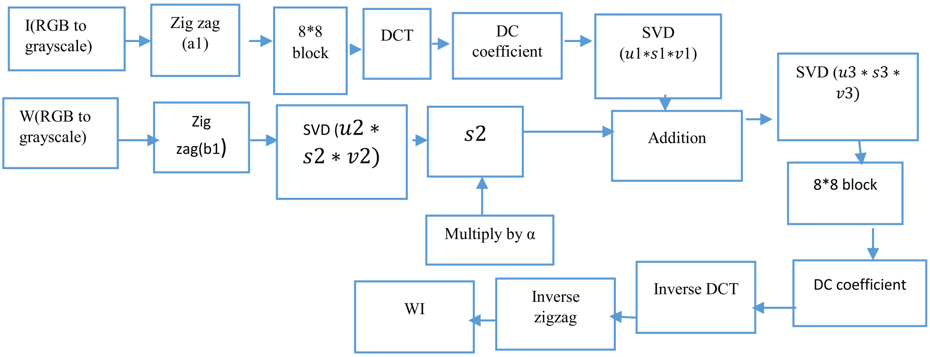


Fig. 43 Embedding process of DCT-SVD

3.38 Extraction process of DCT-SVD

Watermarked image *WI* image is scrambled by zigzag operation (c1) and divided into 8*8 blocks which is further transformed by DCT and from each block its DC coefficient value is taken and SVD is applied on it. To extract the watermark, the singular value of WI (s4) is subtracted by the singular matrix of I image (s1). The value obtained is divided by the scaling factor and inverse SVD is performed to get extracted watermark *EW*.

In order to extract the *I* image the *EW* coefficients are multiplied by the scaling factor and subtracted by singular matrix of W image (s2) the value obtained is inverse SVD and divided into 8*8 blocks, DC coefficient are extracted and placed at their location from which it is extracted than inverse DCT is performed which give *EI* from *WI*. This process is shown in Fig. 44. [52]

4 Setup parameters

This section gives detail description of set up parameters and performance metrics used for evaluating the performance of the given schemes Table 3.

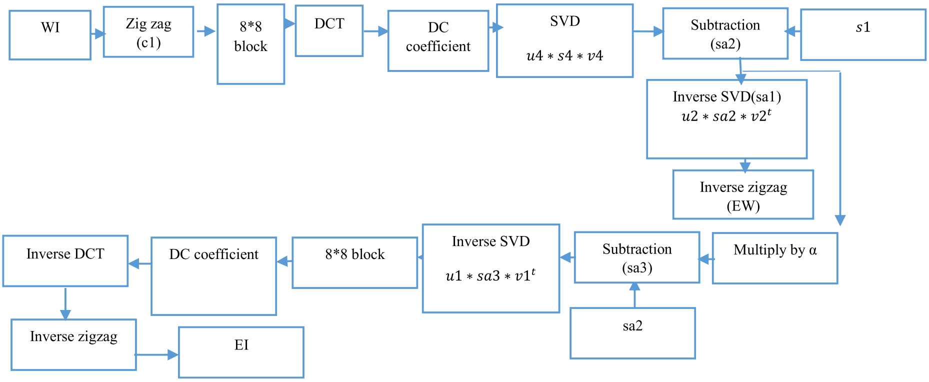
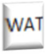


Fig. 44 Embedding process of DCT-SVD

Table 3 Simulation set up parameters

Cover Image size	256*256
Watermark image size	32*32
Image type (cover image and watermark image)	.jpg
Simulation tool	MATLAB R2013a 32 bit (win 32)
Processor Core-	INTEL® core TM i5-7200 CPU@2.50GHZ
Watermark image	
Cover image	
Constant	Beta =0.4, b=8,q (quantization matrix)
Scaling Factor (α)	0.1

4.1 Performance metrics

The performance metrics used are given below [6]:

4.1.1 Imperceptibility analysis

This type of analysis evaluates the quality of the watermarked image with respect to the original cover image after the incorporation of watermark. Visual inspection or qualitative analysis of snapshots of images before and after embedding is the measure of this property.

4.1.2 Robustness analysis

Robustness analysis is used for image quality measurements. The extensively used parameters for robustness analysis are given below:

- **Mean square error (MSE)**

This parameter is a quantitative representation of the error that occurs in the final watermarked-image with respect to the original image. For a color image the MSE is given as:

$$MSE=\frac{1}{M*N*3}\sum_{C=1}^{3}\sum_{Y=1}^{N}\sum_{X=1}^{M}\left[F^{c}(x,y)-F^{c\sim}(x,y)\right]^{2} \qquad (14)$$

where $M \times N$ is the size of image (height and width respectively), $C = 1$ to 3 denotes the red, green and blue colour plane respectively, $Fc(x, y)$ = value of pixel at position (x, y) in c colour plane of cover image, $Fc\sim(x, y)$ = value of pixel at position (x, y) in c color plane of watermarked-image.

- **Mean absolute error (MAE)**

MAE is the average of absolute errors between the cover image and the watermarked-image. For a colour image the MAE is given as:

$$MSE = \frac{1}{M{*}N{*}3} \sum_{c=1}^{3} \sum_{y=1}^{N} \sum_{x=1}^{M} \left[F^{c}(x,y) - F^{c\sim}(x,y)\right]^2 \tag{15}$$

where $M \times N$ is the size of image (height and width respectively),$C = 1$ to 3 denotes the red, green and blue colour plane respectively, $Fc(x, y)$ = value of pixel at position (x, y) in c colour plane of cover image, $Fc\sim(x, y)$ = value of pixel at position (x, y) in c color plane of watermarked-image.

- **Peak signal to noise ratio (PSNR)**

PSNR is the most commonly used parameter to measure the quality of image after embedding. Higher the PSNR value, higher the robustness of the watermarked-image. PSNR value is most commonly defined in terms of MSE. The PSNR is given as:

$$PSNR = 10 log_{10} \frac{MAX^2}{MSE} \tag{16}$$

where MAX is the maximum value of a pixel in the image. It is 255 for colour image of 8 bits.

- **Probable Attacks**

When documents are available online one of the main threats is exposure to noises and probable attacks. Bit Error Rate (BER) is a measure to calculate the number of bits change before and after attack in the host image.

BER can be calculated as: [number, ratio] = biterr (x,y)

number is a scalar or vector that indicates the number of dissimilar bits before and after attack. *Ratio* is number divided by the total number of bits. x and y are watermarked image without and with attack respectively. .

– **Simple Attacks [61]**
– **Salt & pepper:**

It is referred to as on off pixels. [62] Syntax:

u = imnoise (I, ‘salt& pepper’,d)

where *imnoise* means addition of noise (salt and pepper), *I* is the watermarked image on which the attack will transpire, *d* is noise density which is the measure of noise to be added in the image. Its default value is 0.05.

- **Gaussian Attack:**

This attack will transpire as noise into the watermarked image, which act upon as white Gaussian noise with mean and variance. Syntax:

u = imnoise (I,'Gaussian', m, v)

where *m* is mean and its default value is 0 and *v* is the variance with default value 0.01.

angle can be 90,180,270 or 360.

- **Poisson Attack:**

This attack generates the Poisson noise in data by using the syntax:

u = imnoise (I, 'poisson').

- **Geometric Attack**
- **Rotation Attack:**

This attack rotates the image with any angle. Syntax:

u = imrotate (I, 'angle')

1.1.1 Security analysis

The security analysis of a technique is done by comparing the histograms of cover image and watermarked -image. A histogram is a graphical representation of the distribution of the data. Various parameters are used to compare the histograms. For a technique to be secured these parameters should have ideal values or values close to the ideal values which implies very less change in histograms. The parameters used for security analysis are:

- **Jaccard index:**

The Jaccard index, also known as the Jaccard similarity coefficient is used for comparing similarity between the cover image and the watermarked -image. The Jaccard index is mathematically given as:

$$J(A,B) = \frac{A \cup B}{A \cap B} \tag{17}$$

where *A* is the original image and *B* is the watermarked -image

J(*A*, *B*) is the Jaccard index between image matrices *A* and *B, A* ∩ *B* is the intersection of matrices *A* and *B, A* ∪*B* is the union of matrices *A* and *B*. The value of Jaccard index lies between 0 and 1. 1 signifies perfect matching and 0 signifies total mismatch.

- **Correlation coefficient**

The correlation coefficient is a measure of the linear correlation (dependence) between two images *A* and *B*, giving a value between +1 and − 1 inclusive, where 1 signifies perfect match and − 1 signifies total mismatch. The correlation coefficient is given as:

$$\rho(A,B) = \frac{cov(A,B)}{\sigma_A \sigma_B} \tag{18}$$

where A is the original image and B is the watermarked –image (A, B) is the correlation coefficient between image matrices A and B,cov (A, B) is the covariance between matrices A and B,σA is the standard deviation of A,σB is the standard deviation of B.

- **Intersection coefficient**

Intersection coefficient counts the common number of pixels of same value between two histograms (histograms of cover image and watermarked -image). The intersection coefficient is given as:

$$I(A,B) = \sum_{I=1}^{M} \min(p(i),q(i)) \tag{19}$$

where A is the original image and B is the watermarked –image, I (A, B) is the intersection coefficient between image matrices A and B, p and q are the probability distributions of images A and B respectively.

If value of intersection coefficient is 1 it signifies perfect match and if the value is 0 it signifies total mismatch.

- **Bhattacharyya coefficient**

The Bhattacharyya coefficient measures the similarity between two images by using their probability distributions. The formula for Bhattacharyya coefficient is given as:

$$BC(A,B) = \sum_{I=1}^{N} \sqrt{p(i)q(i)} \tag{20}$$

where A is the original image and B is the watermarked –image, (A, B) is the Bhattacharyya coefficient between image matrices A and B, p and q are the probability distributions of images A and B respectively.

If value of Bhattacharyya coefficient is 1 it signifies perfect match and if the value is 0 it signifies total mismatch.

- **UIQI**

It stands for universal image quality index it splits the comparison between cover and watermarked image in terms of luminance, contrast, structural comparison. It is given as:

$$l(x,y) = \frac{2u_x u_y}{{u_x}^2 + {u_y}^2} \tag{21}$$

$$c(x,y) = \frac{2\sigma_x \sigma_y}{{\sigma_x}^2 + {\sigma_y}^2} \tag{22}$$

$$s(x,y) = \frac{2\sigma_{xy}}{\sigma_x + \sigma_y} \tag{23}$$

where u_x, u_y are mean of cover and watermarked image respectively. σ_x, σ_y, are standard deviation of cover and watermarked image respectively.σ_{xy} is covariance of both images.

4.1.3 Data extraction

Extraction of hidden information (sign, logo or symbol) from the watermarked image is a significant parameter. It can be calculated by weighing the correspondence between the extracted and original watermark. Bit Error Rate (BER) is its gauge. It tells the number of bits changed between original and extracted watermark.

BER can be calculated as: [number, ratio] = biterr (x,y)

The number is a scalar or vector that indicates the number of dissimilar bits before and after the attack. The ratio is number divided by the total number of bits. x and y are original and extracted watermark respectively. [32]

5 Comparative analysis

5.1 Imperceptibility

Visual inspection of the resultant images after implementation is the best way to judge imperceptibility competence of diverse techniques.

As per Table 4, for most of the techniques imperceptibility of watermark in cover image is high (DWT, SVD, LWT and many amalgamations) but extracted watermark is distorted in many techniques (DCT, DWT, SWT and in many combinations).

5.2 Robustness analysis

To measure the performance of various frequency domain watermarking techniques diverse parameters like (PSNR, MAE, MSE, bit error) are calculated to measure the robustness of schemes. [43] Even after applying the attacks (salt& pepper, Gaussian, rotation, Poisson), number of bits change are measured between received watermark with respect to original watermark image and received cover image with respect to original cover image to ensure the recovery of watermark after attacks and make certain image perceptibility. [5]

▨ DCT	▨ DWT	▨ DFT	▨ FRFT
▨ CT	▨ HADAMARD	▨ SVD	▨ SWT
▨ LWT	▨ DCT-DWT	▨ DCT-SVD	▨ DWT-SVD
▨ LWT-SVD	▨ DWT-FFT	▨ DWT-FFT-SVD	▨ SWT-SVD
▨ DWT-DCT-SVD	▨ DWT-HADAMARD-SVD		

where in graph the different colors allotted to different techniques are given above:

Table 5 shows graphs for different robustness parameters. Analysis of these graphs is done as follows:

- **MSE:**

  MSE is used to calculate the error between the cover and watermarked image. Results are calculated on the basis of three cover images of different sizes i.e.

256*256,512*512, 1024*1024. MSE and PSNR are inversely proportional to each other. In Table 5 the lowest value of MSE is obtained by DWT-FFT technique i.e. 0.0045, as LH band is selected for the watermark insertion which provide low deformation to image, as well as magnitude of LH band is high where as in DCT technique. The value of MSE is high as number of bit changes is more due to the quantization step which involves for suppression of high frequency component.

- **MAE:**

  MAE calculates the absolute error between cover and watermarked image. This error should be minimum to get the better result because the techniques which will reflect less change have more chances to achieve robustness. In this case MAE value of technique DWT-FFT is very less because of appropriate band selection for watermark insertion which results in less distortion and highest value of MAE is for DCT technique.

- **PSNR:**

  PSNR stands for Peak signal to noise ratio. It is one of the key parameter to compute the robustness of any technique. Higher value of PSNR means the low error

Table 4 Snapshots of different frequency domain watermarking techniques

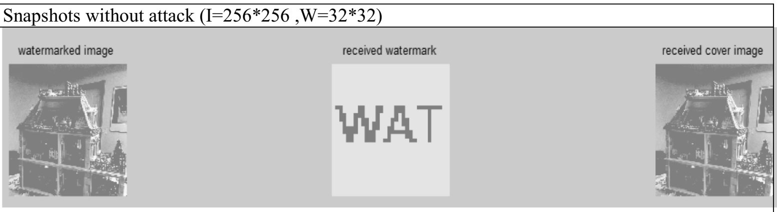
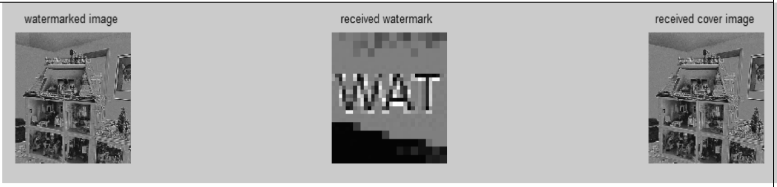
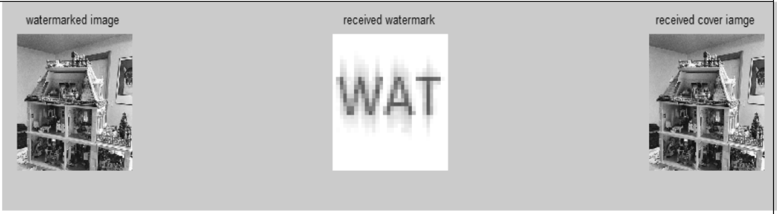
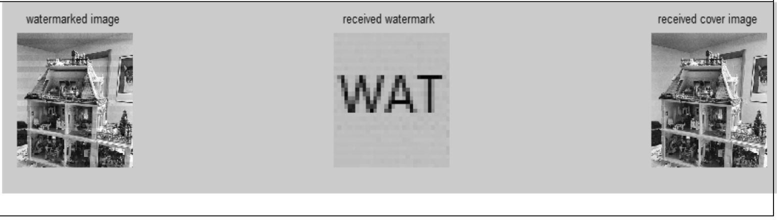
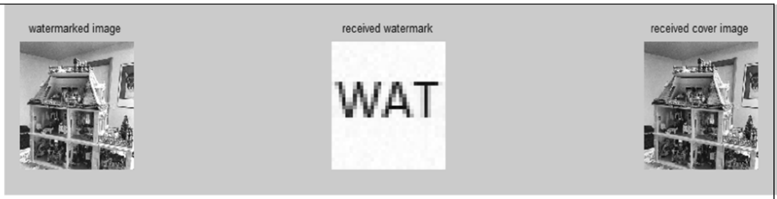
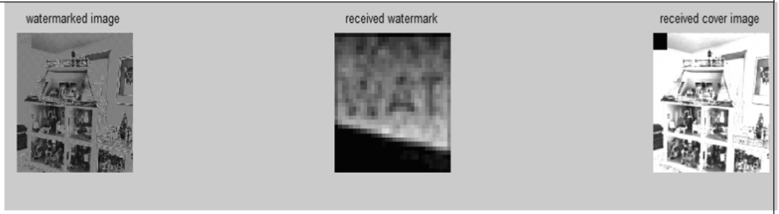
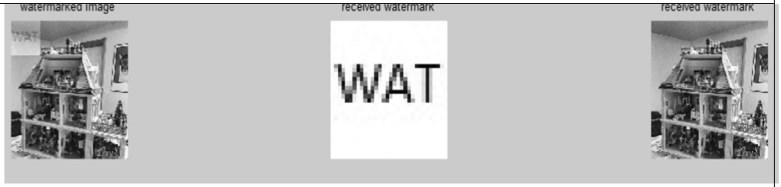
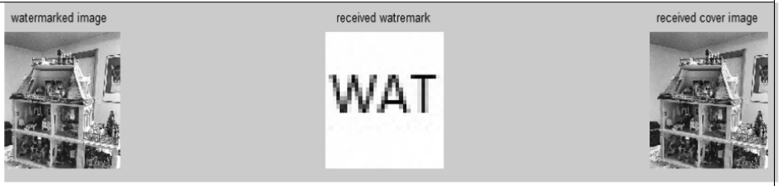
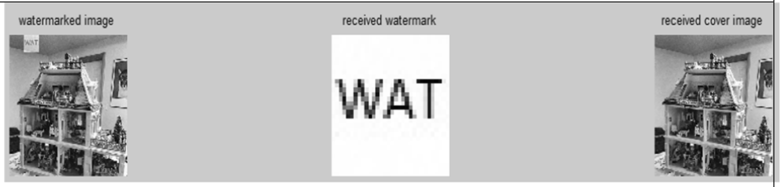
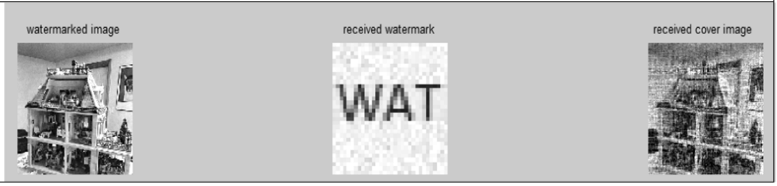
Techniques	Snapshots without attack (I=256*256 ,W=32*32)
DCT	 watermarked image received watermark WAT received cover image
DWT	 watermarked image received watermark WAT received cover image
DFT	 watermarked image received watermark WAT received cover iamge
FRFT	 watermarked image received watermark WAT received cover image

Table 4 (continued)

SVD	 watermarked image received watermark received cover image
SWT	 watermarked image received watermark received cover image
LWT	 watermarked image received watermark received watermark
DCT-DWT	 watermarked image received watremark received cover image
HADAMARD	 watermarked image received watermark received cover image
DCT-SVD	 watermarked image received watermark received cover image

between the cover and watermarked image. Highest PSNR value is 71.5534 of DWT-FFT technique because while applying DWT on cover image its appropriate band is selected such as LH which provide information of smooth area, then Fast Fourier is carry out which result in less distortion, 2nd highest PSNR value obtained is 60.1975 which is for LWT-SVD technique. This is because of the fact that modification in the

Table 4 (continued)

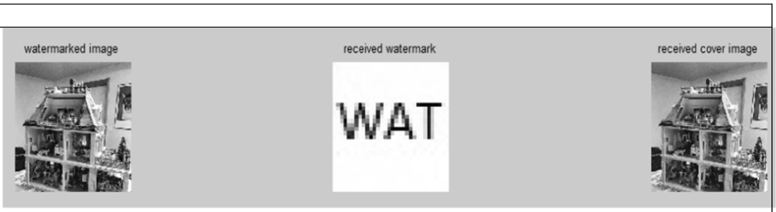
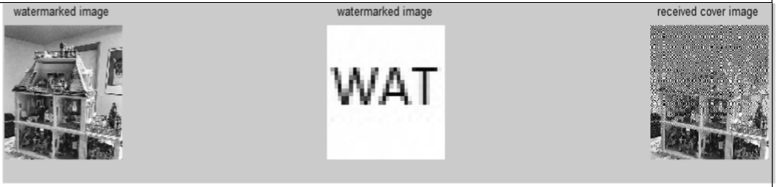
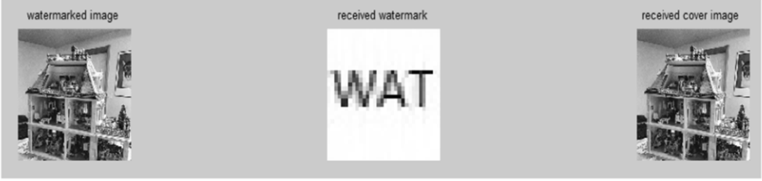
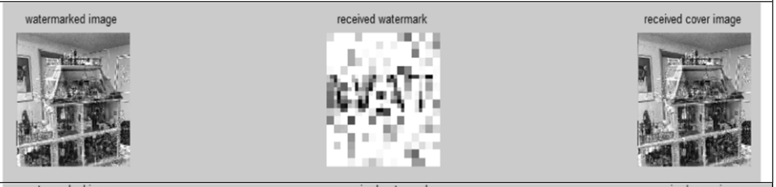
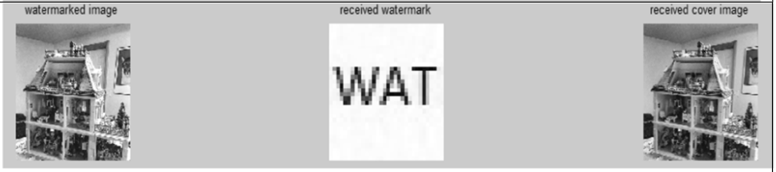
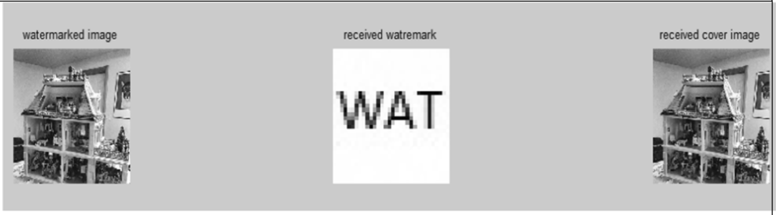
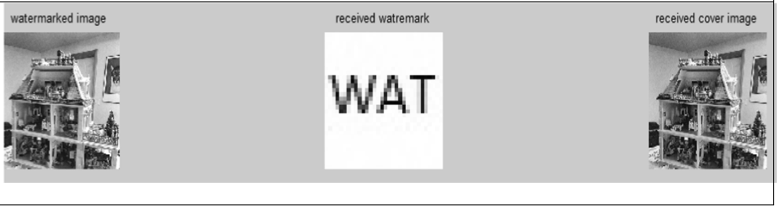
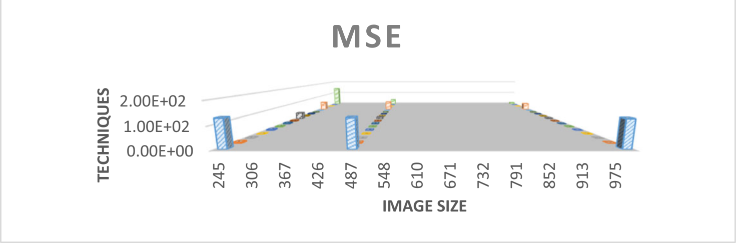
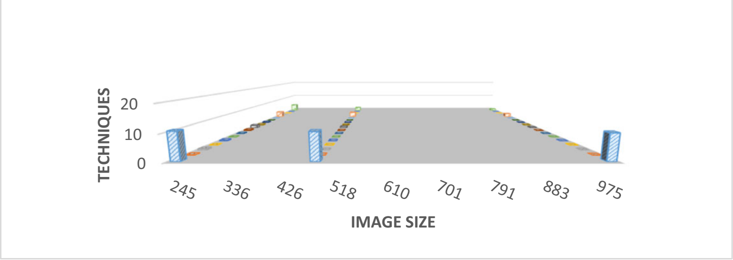
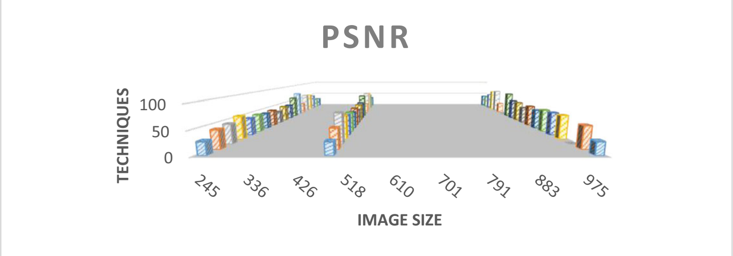
DWT-SVD	 watermarked image received watermark WAT received cover image
LWT-SVD	 watermarked image watermarked image WAT received cover image
DWT-DFT	 watermarked image received watermark WAT received cover image
DWT-FFT-SVD	 watermarked image received watermark received cover image
SWT-SVD	 watermarked image received watermark WAT received cover image
DWT-DCT-SVD	 watermarked image received watremark WAT received cover image
DWT-HADAMARD-SVD	 watermarked image received watremark WAT received cover image

Table 5 Robustness parameters results

Robustness parameters	Graphs
MSE	
MAE	
PSNR	

value of SVD leads to less alteration of data. Lowest PSNR value is for DCT which is 27.071, as the transformation from spatial to frequency domain using DCT leads to more number of bit changes.

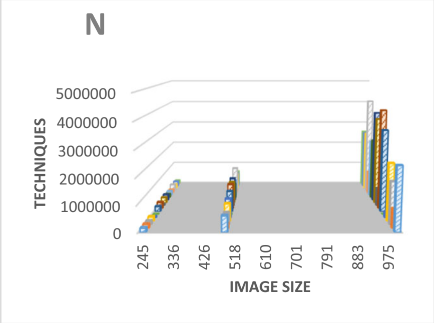
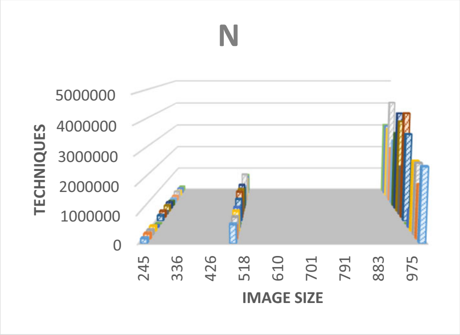
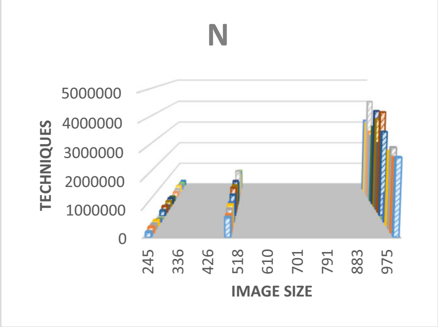
- **Bit Error (with Attacks)**
- **Salt and pepper noise:**

The attack is applied on the watermarked image and after that cover and watermark images are extracted from it, this attack is also known as on off attack. The noise density is a parameter of variation for this attack; on the basis of this variation results are calculated:

Tables 6 and 7 shows graphs for bit error in terms of number of bit changes (N) and ratio of bit changes (R)

For watermark and cover image before and after retrieval of watermark with varying noise density of salt and pepper noise. After observing graphs of both tables it is wrap up that with increase in the noise density the value of bit error will goes on increasing. Bit error measures the number of bit change in between the received cover image and watermark image. With increase in the image size and noise density the number of bit change goes on increasing. The major change after attack is

Table 6 Salt & pepper attack between cover image (I) & extracted cover image (EI)

<table>
<tr><td colspan="2">Salt &amp; Pepper attack , N=No of bits change between cover image(I) & extracted cover image(EI) ,n=Noise density</td></tr>
<tr><td>n=0.05</td><td>n=0.15</td></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>n=0.25</td><td></td></tr>
<tr><td>
</td><td></td></tr>
</table>

found on DWT-FFT-SVD technique as in this technique three frequency domain transformations are applied which result in drastic change in values, hence results in high bit error in extracted cover and watermark image. Very less changes obtained are for Hadamard technique, as it is symmetric in nature and less prone to attacks, DWT-FFT also has less effect of this attack as effective distribution of energy is made which make it less effective in terms of noise.

- **Gaussian noise**

The attack is applied on the watermarked image and after that cover and watermark images are extracted from it, mean and variance are the parameters of variation for this attack; mean taken here is 0 and variance is (0.01, 0.10, 0.20). On the basis of this variation results are calculated:

Tables 8 and 9 shows graphs for bit error in terms of number of bit changes (N) and ratio of bit changes (R) for watermark and cover image before and after retrieval of watermark with different values of variance of Gaussian noise. After observing graphs of both tables it is wrap up that as the variance increases the number of bits change also increases for different image size i.e. 256, 512, and 1024 for all techniques. Amongst all the mechanisms the Hadamard method gives least number of bit changes, as it is symmetric in nature but DCT in case of cover image and SVD and DWT in case of watermark show significant changes in bits after this attack.

Table 7 Salt & pepper attack between watermark image (W) & extracted watermark image (EW)

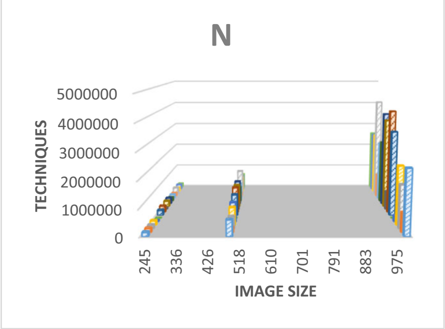
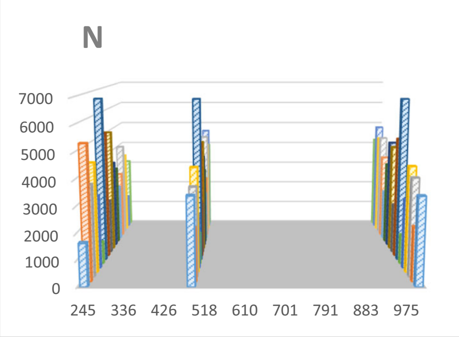
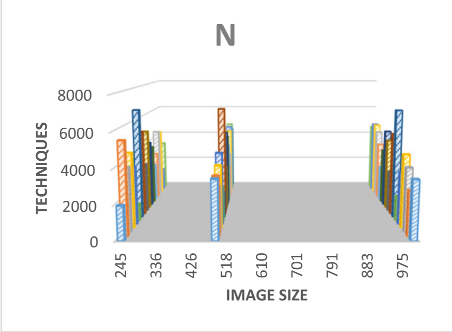
<table>
<tr><td colspan="2">Salt & Pepper attack , N=No of bits change between watermark image(W) & extracted watermark image(EW) ,n=Noise density</td></tr>
<tr><td>n=0.05</td><td>n=0.15</td></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>n=0.25</td><td></td></tr>
<tr><td>
</td><td></td></tr>
</table>

Table 8 Gaussian attack between cover image (I) & extracted cover image (EI)

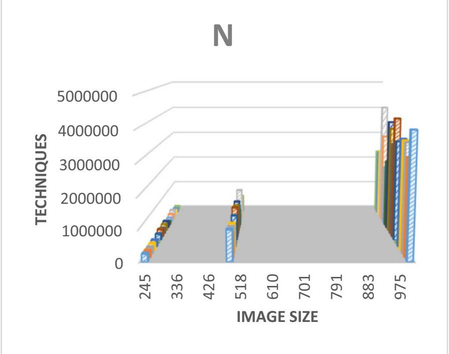
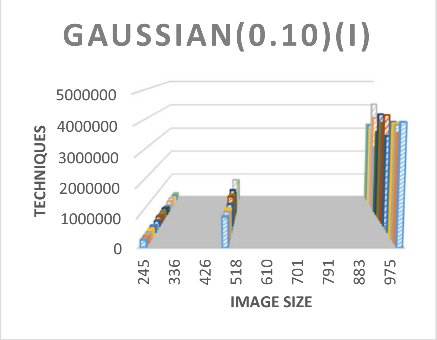
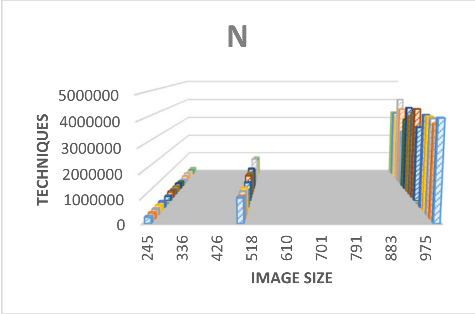
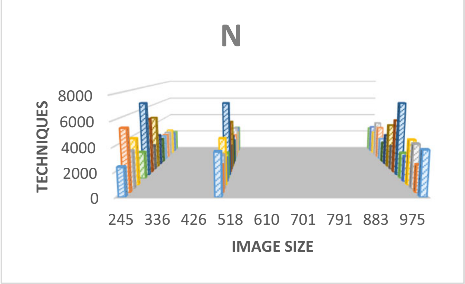
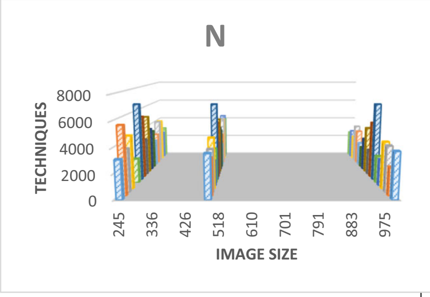
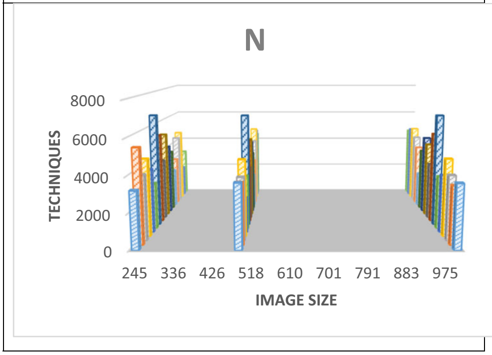
<table>
<tr><td colspan="2">Gaussian attack , N=No of bits change between cover image(I) & extracted cover image(EI) ,v=variance</td></tr>
<tr><td>v=0.01</td><td>v=0.10</td></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>v=0.20</td><td></td></tr>
</table>

Table 9 Gaussian attack between watermark image(W) & extracted watermark image (EW)

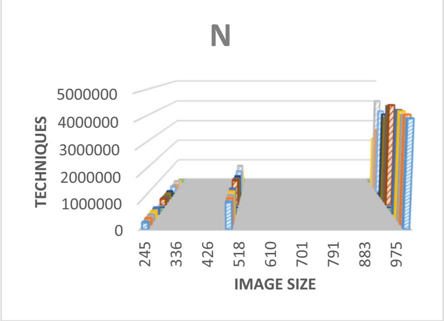
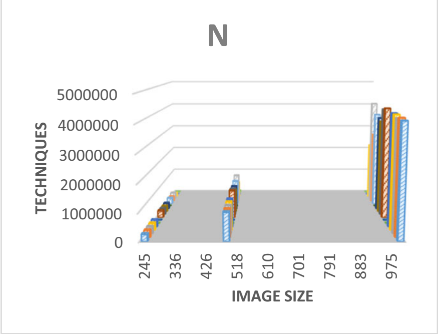
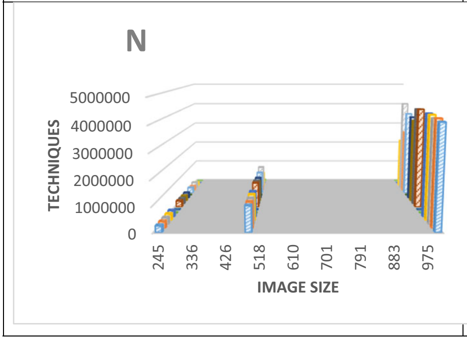
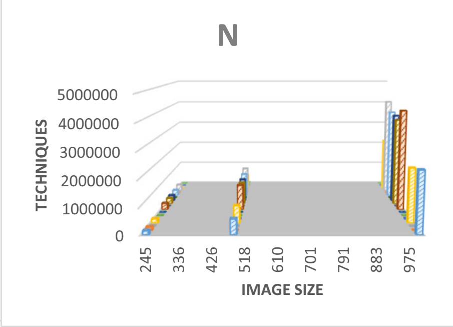
<table>
<tr><td colspan="2">
</td></tr>
<tr><td colspan="2">Gaussian attack , N=No of bits change between watermark image(W) & extracted watermark image(EW) ,v=variance</td></tr>
<tr><td>v=0.01</td><td>v=0.10</td></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>v=0.20</td><td></td></tr>
<tr><td>
</td><td></td></tr>
</table>

- **Rotation Attack**:

This attack make the watermarked image rotated at different angle (90, 180, 270, and 360) and then watermark and cover image are extracted from watermarked image.

Tables 10 and 11 shows graphs for bit error in terms of number of bit changes (N) and ratio of bit changes (R) for watermark and cover image before and after retrieval of watermark with different values of rotation angle. After observing graphs of both tables it is wrap up that the SVD, DWT-SVD are immune to rotation attack as their luminosity

Table 10 Rotation attack between cover image (I) & extracted cover image (EI)

Rotation attack , N=No of bits change between cover image(I) & extracted cover image(EI) , a=angle	
a=90	a=180
	
a=270	a=360
	

is less effected due to which effect of noise get reduced. Also numbers of changes are less at 90 and 360 degrees angle, as it comes back to its original position. Moreover there are some techniques in which the value obtained at 90 degree rotation of watermarked image is same for rest of the angles such a LWT-SVD, DWT-FFT-SVD, SWT-SVD, DWT-DCT-SVD, DWT-HADAMARD-SVD.

- **Poisson Attack:**

The attack is applied on the watermarked image and after that cover and watermark images are extracted from it.

Table 12 shows graphs for bit error in terms of number of bit changes (N) and ratio of bit changes (R) for watermark and cover image before and after retrieval of watermark with poisson noise. After observing graphs it is wrap up that the maximum bit change occurs in DWT-FFT-SVD technique as it is hybrid and consist of three methods. DWT is used from compression and FFT for fast transformation and conversion from spatial to frequency domain and SVD for embedding the watermark. Least effect is found in DWT-SVD technique.

Table 11 Rotation attack between watermark image (W) & extracted watermark image (EW)

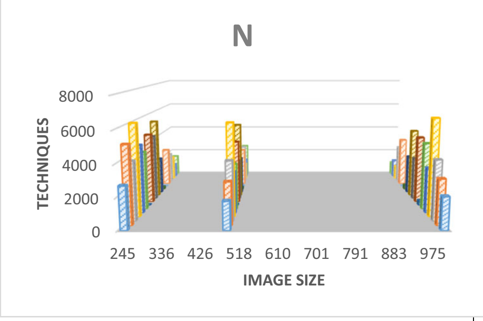
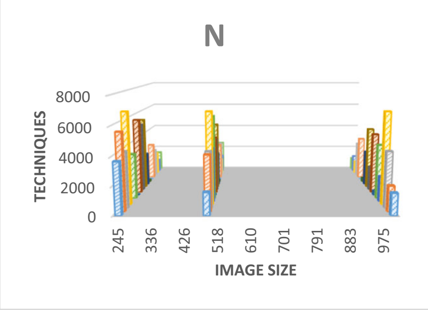
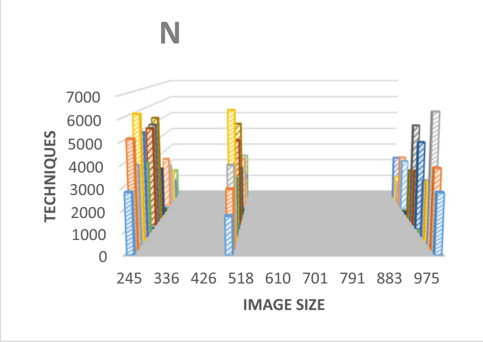
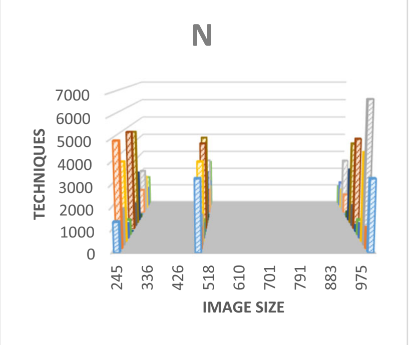
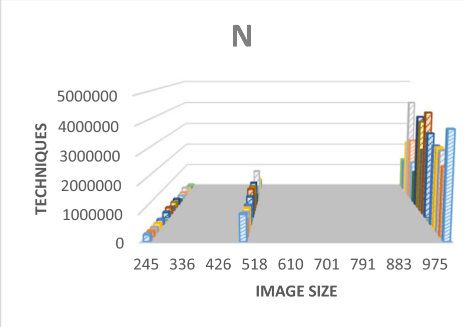
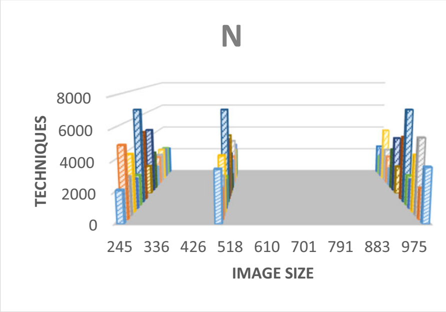
Rotation attack , N=No of bits change between watermark image(W) & extracted watermark image(EW) , a=angle	
a=90	a=180
	
a=270	a=360
	

Table 12 Poisson attack bit error

Bit error	
N=between cover image (I) & extracted cover image (EI)	N= between watermark image (W) & extracted watermark image (EW)
	

5.3 Security analysis

In order to secure the documents inserted watermark needs to be hidden in such a way that its existence can't be detected by anyone. To ensure this fact many performance matrices are calculated and compared, such parameters are Jaccard index, Bhattacharya coefficient, UIQI, Intersection and correlation coefficient [14].

Table 13 shows graphs for different security parameters. Analysis of these graphs is done as follows:

- **UIQI**

  Universal image quality index measures the similarity between the cover and watermarked image. Maximum value obtained 0.999999392157608 is of DWT-FFT technique which provides high PSNR value and less image distortion.
- **Jaccard Index:**

  This measures the match between two images i.e. cover image and image obtained after watermark insertion for perfectly match pixel values, the index must be equal to 1.Various frequency domain watermarking techniques are implemented and the best result for perfect match is found for DWT-FFT technique as DFT is excellent tool for transformation from spatial to frequency domain and provides wide range of applications in image reconstruction.
- **Bhattacharya coefficient:**

  It measures the similarity between the cover image and image obtained after the modification (inserting the watermark). On the basis of probability distribution function, the highest value obtained is of DWT-FFT technique as in this hybrid technique the cover image is distributed into four bands and LH band is selected which gives information of smooth area. They are also referring to coarse coefficient and extraction of the watermark is also possible with minimum distortion.
- **Intersection coefficient:**

  It is used to measure the common pixel value between the cover and watermarked image. If most of the values will be same this leads to swell perceptibility and robustness of the technique. The best result is drawn by DWT-FFT watermarking technique for 256*256, which is 0.997116088867188. As the image size increases and fixed watermark size, the value of Intersection coefficient also get increases and reaches towards 1.
- **Correlation**

  It is used to measure the similarity between cover and watermarked image. Its value must be nearly 1 for a perfect correlation. As observed from results the value for DWT-FFT watermarking scheme is 0.999998784346817 which direct to perfectly match data due to less distortion, as the band selection is appropriate due to which change in image is less.

5.4 Data extraction

Extraction of watermark from watermarked image is very essential process for assessment purpose. As for copyright protection defined signature or logo is required to be extracted and verified. For comparison among different techniques bit change error (BER) is calculated between original and extracted watermark.

Table 13 Security parameters results

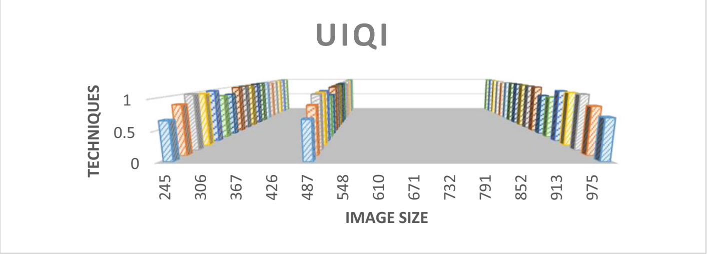
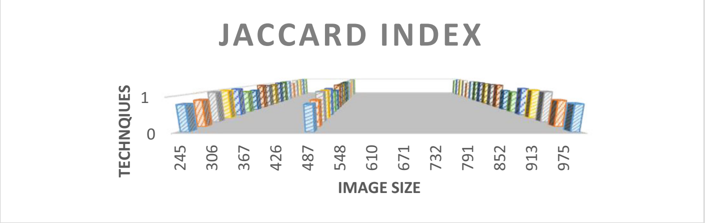
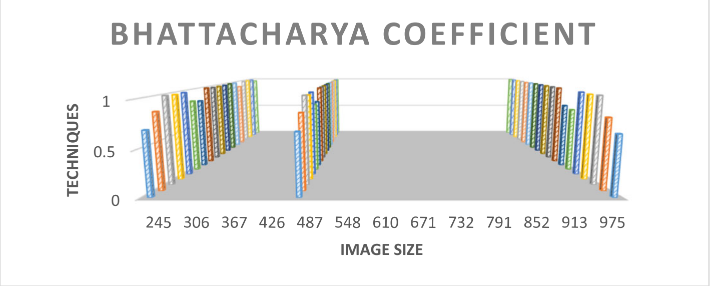
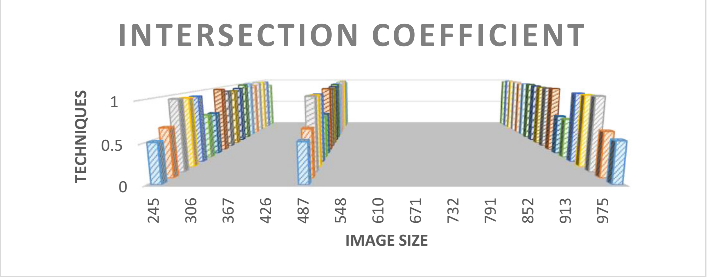
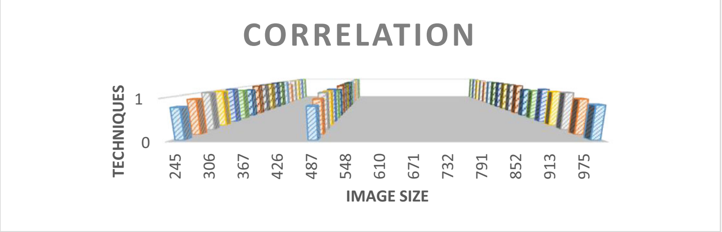
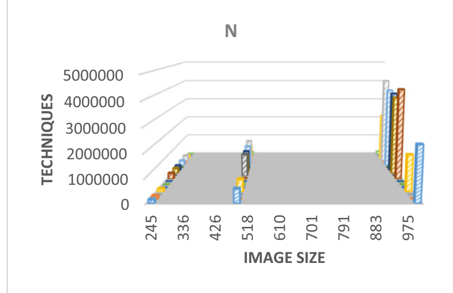
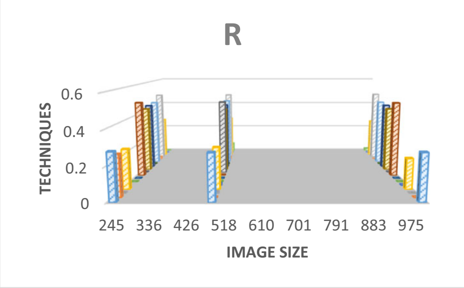
UIQI	
JACCARD INDEX	
BHATTACHARYA COEFFICIENT	
INTERSECTION COEFFICIENT	
CORRELATION	

Table 14 Bit error without attack between cover image (I) & extracted cover image (EI)

Bit error between cover image(I) & extracted cover image (EI)	
N=No of bits change	R=Ratio of bits change
	

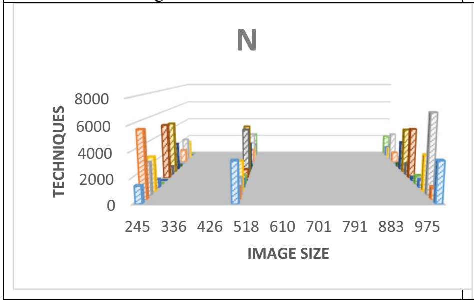
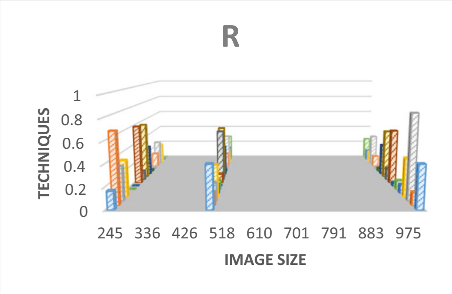
- **Without attacks (Bit error)**

This parameter of bit error is calculated in terms of the number of bits change (N) and ratio (R), for different techniques as shown in Table.

1. Amid cover image (I) with extracted cover image (EI).
2. Amid watermark (W) with extracted watermark (EW).

Tables 14 and 15 shows graphs for bit error in terms of number of bit changes (N) and ratio of bit changes (R) for watermark and cover image before and after retrieval of watermark. After observing graphs of both tables it is wrap up that the values for DWT, SVD, LWT-SVD, DWT-SVD technique is 0 which notify, no change take place in cover image before and after extracting watermark image. As in DWT, LWT techniques its LL band is used which provide more visibility to image and less distortion, also in SVD the change in pixel value reflects small alteration in the overall image. Its luminance does not get effected easily and provide stability. The changes in these values occur mainly due to transformation of Image from spatial to frequency domain and the method used to embed the watermark into cover image. As per graphs minimum change in N and R for watermark can be seen in DWT-SVD, DWT-FFT techniques.

Table 15 Bit error without attack between watermark image (W) & extracted watermark image (EW)

Bit error between watermark image(W) & extracted watermark image (EW)	
N=No of bits change	R=Ratio of bits change
	

6 Conclusion

Transform domain is a mechanism for digital watermarking in which various frequency domain techniques are implemented, and each procedure has its characteristics and application, the combination of two or more performances gives better effect than standalone. After assessment of techniques for different types and sizes of cover images (256, 512 and 1024) and embedding the watermark of fixed image size (32*32) analysis is done by security and robustness parameters. Finally, results are calculated which wrap up that preeminent outcomes are found from the amalgamation of different standalone techniques:

- The combination DWT and DFT technique, i.e., DWT-FFT gives the minimum error and high PSNR value. DWT technique is used to decompose the image into bands which helps in achieving imperceptibility of the image due to the appropriate band selection provides high magnitude value whereas in DFT effective distribution of energy take place which immune the image against various attacks such as rotation, invariance, scaling. Standalone DCT mechanism gives the high error and low PSNR.
- After observing the effects of the different attacks and noises on extracted watermark and cover image, it is concluded that least number of bits are changed in DWT-FFT and Hadamard technique for salt & pepper and Gaussian noise. As Hadamard technique is symmetric and less prone to attacks and DWT-FFT as effective distribution of energy is made which make it less effective in terms of noise and significant change is observed in standalone DCT, SVD and DWT and the combination of DWT-FFT-SVD.
- For rotation attack and Poisson noise least change is found in DWT-SVD and LWT-SVD as these are immune to rotation attack, so their luminosity is less affected due to which effect of noise get reduced. But significant change occurs in DWT-FFT-SVD. As in this technique, three frequency domain transformations are applied which result in the drastic change in values, hence results in high bit error.

References

1. Abraham J, Paul V (2016) A DCT based imperceptible color image watermarking scheme. Int J Signal Process Image Process Pattern Recogn 9(7):137–146
2. Akhaee MA, Mohammad Ebrahim Sahraeian S, Marvasti F (2010) Contourlet-based image watermarking using optimum detector in a Noisy environment. IEEE Trans Image Process 19(4):967–980
3. Al-Afandy KA, El-Shafai W, El-Rabaie E-SM, Abd El-Samie FE, Faragallah OS, El-Mhalaway A, Shehata AM, El-Banby GM, El-Halawany MM (2018) Robust hybrid watermarking techniques for different color imaging systems. Multimed Tools Appl, Springer Science+Business Media, LLC, part of Springer Nature 77(19):25709–25759
4. Al-Ataby A, Al-Naima F (2010) A modified high capacity image steganography technique based on wavelet transform. Int Arab J Inform Technol 7(4):358–364
5. Anita Pradhan KRS, Swain G (2016) Digital image steganography based on seven way pixel value differencing. Indian J Sci Technol 9(37):1–11
6. Arya H, Singh S, Kushwah BV, Jain P (2016) A Survey on Digital Watermarking Techniques. Int J Eng Technol Sci Res IJETSR ISSN 2394–3386 3(5):240–245
7. Md Asikuzzaman And Mark R. Pickering, “An Overview Of Digital Video Watermarking”, IEEE Trans Circ Syst Video Technol, Volume 28, Issue 9 , pp.2061–2077, 2018
8. Assini I, Badri A, Safi K, Sahel A, Baghdad A (2017) Hybrid multiple watermarking technique for securing medical image using DWT-FWHT-SVD. 3rd international conference on advanced Technologies for Signal and Image Processing – ATSIP '2017, Fez, Morocco

9. Bhaskar T, Vasumathi D (2015) DCT based watermark embedding into mid frequency of DCT coefficients using luminance component. Int Res J Eng Technol (IRJET) 02(3):738–741
10. Chaudhari MM, Pawar KN (2015) Stationary wavelet transform based steganography for transmitting images. International Journal of Innovative Research in Science, Engineering and Technology 4(12):12064–12069
11. Dar SB, Dar AB (2014) Watermarking in frequency domain a review. Int J Eng Comput Sci ISSN: 2319–7242 3(11):9215–9218
12. Dar SB, Dar AB (2014) Watermarking in frequency domain a review. Int J Eng Comput Sci ISSN:2319–7242 3(11):9215–9218
13. Dar SB, Dar AB (2014) Watermarking in frequency domain a review. Int J Eng Comput Sci 3(11):9215–9218
14. Dhall S, Bhushan B, Gupta S (2016) An improved hybrid mechanism for secure data communication. Int J Comput Netw Inform Sec 8(6):67–78
15. Dinesh Kumar G, Teja DP, Sykam SR, Devi NS (2017) An efficient watermarking technique for biometric images. 7th Int Conf Adv Comput Commun ICACC 2017 115(2):423–430
16. Do MN, Vetterli M, Fellow IEEE (2005) The Contourlet transform: an efficient directional multiresolution image representation. IEEE Trans Image Process 14(12):2091–2106
17. Favorskaya M, Oreshkina E (2015) Digital gray-scale watermarking based on biometrics. Intell Interact Multimed Syst Services 40:203–214
18. Fazlali HR, Samavi S, Karimi N, Shirani S (2017) Adaptive blind image watermarking using edge pixel concentration. Multimed Tools Appl 76(2):23459–23479
19. Goel S, Rana A, Kaur M (2013) A review of comparison techniques of image steganography. IOSR J Electr Electron Eng (IOSR-JEEE) 6(1):9–14
20. Guru J, Damecha H (2014) Digital watermarking classification: a survey. Int J Comput Sci Trends Technol (IJCST) 2(5):8–13
21. Hallur SR, Kuri S, Kulkarni GH (2015) Robust digital watermarking using DWT-DCT-SVD algorithms for color image. Int J Curr Eng Technol 5(4):2722–2727
22. Hemani, Singh S (2017) A survey of digital watermarking techniques and performance evaluation metrics. Int J Eng Trends Technol 46(2):128–132
23. Ingale SP, Dhote CA (2016) Digital watermarking algorithm using DWT technique. International Journal of Computer Science and Mobile Computing, IJCSMC 5(5):1–9
24. Irfan M, Zheng L, Shahzad H (2013) Review of computing algorithms for discrete fractional Fourier transform. Res J Appl Sci Eng Technol 6(11):1911–1919
25. Islam MS, Chong UP (2014) A digital image watermarking algorithm based on DWT DCT and SVD. Int J Comput Commun Eng 3(5):356–360
26. Jain P, Ghanekar U (2017) Robust watermarking technique for textured images. 6th Int Conf Smart Comput Commun ICSCC 2017 Procedia Comput Sci 125:179–186
27. Jain R, Jain M (2015) Digital image watermarking using 3-level DWT and FFT via image compression. Int J Comput Appl 124(16):35–38
28. Jane O, Elbaõ E, Lk HG (2014) Hybrid non-blind watermarking based on DWT and SVD. J Appl Res Technol 12(4):750–761
29. Jangde K, Raja R (2014) Image compression based on discrete wavelet and lifting wavelet transform technique. Int J Sci Eng Technol Res (IJSETR) 3(3):394–399
30. Katharotiya A k, Patel S, Goyani M (2011) Comparative analysis between DCT & DWT techniques of image compression. J Inform Eng Appl 1(2):9–17
31. Kullayamma and Sathyanarayana (2016) A novel method of digital image watermarking in spatial domain based on interpolation. International J Adv Res Comput Commun Eng 5(2):451–457
32. Kumar Sahu A, Swain G (2018) An improved data hiding technique using bit differencing and LSB matching. Int Netw Indonesia J 10(1):17–21
33. kumar M, Manikandan T, Sapthagirivasan V (2011) Non-blind image watermarking using countourlet transform. Indian J Comput Sci Eng (IJCSE) 2(1):31–38
34. Lai C-C, Tsai C-C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
35. Lokeswara Reddy V, Subramanyam DA, Chenna Reddy DP (2011) Implementation of LSB steganography and its evaluation for various file formats. Int J Ad Netw Appl 2(5):868–872
36. Loukhaoukha K, Refaey A, Zebbiche K, Nabti M (2015) On the security of robust image watermarking algorithm based on discrete wavelet transform, discrete cosine transform and singular value decomposition. Appl Math Inf Sci 9(3):1159–1166
37. Manikandaprabu S, Ayyasamy S (2014) An efficient watermarking algorithm based on DWT and FFT approach. Int J Comput Sci Eng (IJCSE) 6(6):211–216
38. Media K (2018) Online copyright infringement tracker latest wave of research" published by intellectual property office

39. Pambi M, Swapna E (2016) A review on digital watermarking for copyright protection of digital data. Int J Innovative Eng Manag Res 5(2):169–173
40. Pareek S, Vyas A (2014) Hybrid watermarking techniques. 1(9):189–192
41. Parvathavarthini S (2014) An adaptive watermarking process in Hadamard transform. Int J Adv Inform Technol (IJAIT) 4(2):1–7
42. Patel MB, Patel PKR (2015) Implementation of digital image watermarking using discrete fractional Fourier transform. IJSRD - Int J Sci Res Dev 3(3):1060–1064
43. Pradhan A, Sahu AK, Gandharba S, Raja Sekhar K (2016) Performance evaluation parameters of image steganography techniques. IEEE Int Conf Res Adv Integrat Nav Syst 14(12):1–11
44. Pramanik M, Sharma K (2014) Analysis of visual cryptography, steganography schemes and its hybrid approach for security of images. Int J Emerg Technol Adv Eng 4(2):174–179
45. Ruanaidh JJKO, Dowling WJ, Boland FM (1996) Phase watermarking of images. IEEE Int Conf Image Process 6(3):239–242
46. Sahu AK, Swain G (2017) Information hiding using group of bits substitution. Int J Commun Antenna Propagation 7(2):162–167
47. Sahu AK, Swain G (2018) An improved image steganography using bit flipping. Cybernet Inform Technol 18(1): 69–80
48. Saiyyad MAM, Dept NNP (2014) Watermarking of compressed images using SWT technique and fragile approach. IEEE Global Conference on Wireless Computing and Networking (GCWCN) 1(1):254–257
49. Sangeetha P, Chacko P (2014) Image authentication: a few approaches using digital watermarking. IJAICT 1(1): 149–152
50. Senthilkumaran N, Abinaya S (2016) Digital image watermarking using DFT algorithm. Advanced Computing: An International Journal (ACIJ) 7(1/2):9–17
51. Shokrollahi Z, Yazdi M (2017) A robust blind watermarking scheme based on stationary wavelet transform. J Inform Hiding Multimed Sign Process 8(3):676–687
52. Singh P, Agarwal S (2013) A hybrid DCT- SVD based robust watermarking scheme for copyright protection. International Conference on Emerging Trends Eng Technol (ICETET'2013) 13(3):1–5
53. Snehlata Maloo NL, Pareek NK (2017) Study of digital watermarking techniques for against security attacks. Information Commun Technol Intell Syst (ICTIS 2017) 1:509–515
54. Sreenivas K, Kamkshi Prasad V (2018) Fragile watermarking schemes for image authentication: a survey. Int J Mach Learn Cybern 9(7):1193–1218
55. Sun Q, Wang L, Shao Y, Zuo J (2016) Watermarking technique based on three-coefficient comparison in DCT domain. J Supercomput 72(7):189–192
56. Swain G (2016) Digital image steganography using variable length Group of Bits Substitution. Procedia Comput Sci 85(4):31–38
57. Tejal, Rao D (2017) A review paper on image steganography and its techniques. Int J Res Appl Sci Eng Technol (IJRASET) 5(4):1756–1761
58. Thota NR, Devireddy SK (2008) Image compression using discrete cosine transform Nageswara. Georgian Electronic Sci J: Comput Sci Telecommun 17(3):35–43
59. Tiwari N, Hemrajamani N, Goyal D (2017) Improved digital image watermarking algorithm based on hybrid DWT-FFT and SVD techniques. Indian J Sci Technol 10(3):1–7
60. Tyagi S, Singh HV, Agarwal R, Gangwar SK (2016) Digital watermarking techniques for security applications. International conference on emerging trends in electrical, electronics and sustainable energy systems (ICETEESES–16): 380–382
61. Varshney Y (2017) Attacks on digital watermarks: classification, implications, benchmarks. Int J Emerg Technol (Special Issue NCETST-2017) 8(1):229–235
62. Vijay B, Swathi J (2015) An efficient fast Hadamard transform oriented digital image-in-image watermarking. Int J Res Appl Sci Eng Technol (IJRASET) 3(5):570–585
63. Viraktamath SV, Attimarad GV (2011) Impact of quantization matrix on the performance of JPEG. Int J Future Gen Commun Netw 4(3):107–118
64. Walia E, Jain P, Navdeep (2010) An analysis of LSB & DCT based steganography. Global J Comput Sci Technol 10(1):4–8
65. Yadav K, Kaushik A (2013) A Review of hybrid digital watermarking. Int J Eng Trends Technol (IJETT) 4(Issue 7):3123–3126
66. Yadav M, Kumar A (2017) Digital image watermarking using SWT and SVD. International J Adv Res Comput Commun Eng 6(5):87–91

Ms. Anshul Chopra is B.Tech (Electronics and Communication Engineering) and M.Tech (Electronics and Communication Engineering). Her academic interests include network security and image processing.

Dr. Shailender Gupta is B.Tech (Electronics Engineering), M.Tech (Computer Engineering) and received his Ph. D in the area of ad-hoc mobile network security. His academic interests include network security, Signal Processing, automata theory and fuzzy logic. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.

Ms. Sangeeta Dhall is B.Tech (Instrumentation and Control Engineering), M.Tech (Electronics and Instrumentation) and pursuing her Ph. D in the area of network security. Her academic interests include network security, embedded systems and digital system design. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.