International Journal of Engineering & Technology, 7 (3.6) (2018) 243-248

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Robust Digital Image Watermarking in Hybrid Frequency Domain

P. Sridhar[1*]

[1]Junior Research Fellow, Dept. Of Computer Science And Engineering, Amrita School Of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India.
**Corresponding Author E-Mail:Cb.En.D.Cse17011@Cb.Students.Amrita.Edu*

Abstract

Image watermarking is a method to hide the secret information in a host image for copyright protection of watermark data during the transmission by means of insecure channel. The proposed scheme protects our data with adaptive level of visual quality and robustness against signal processing and geometric attacks. The proposed method divides the host image into four non-overlapping segments labelled as sub-images, DWT is applied on each sub images and then block based DCT is applied on mid frequency channels LH and HL of discrete wavelet transform. Embedded matrix is formed using hybrid transformed coefficients where matrix elements are chosen from the localized two mid frequency coefficients of each block in DCT. SV Decomposition is applied on embedded matrix to factorize it into singular values, left and right singular vectors and embed the scrambled watermark image along with scaling factor in singular value matrix. This repetition of watermark data in each sub-image reduces the PSNR values of the watermarked image. Despite this proposed scheme scales down PSNR value, changing the scaling factor favours to adjust the PSNR to the acceptable level and withstand the signal processing attacks such as JPEG compression and geometrical attack such as rotation, translation. Compared to the other method, the proposed scheme gives better correlation coefficient value for above mentioned kinds of attacks and also provide adaptive PSNR for imperceptibility on watermarked image.

Keywords: *Singular value decomposition (SVD), discrete wavelet transform, discrete cosine transform, arnold transform.*

1. Introduction

The prime advantages of the digital data are easily storing, processing and transmitting. Image is a digital data which is accessed through internet for various purposes. Foremost among them is the security for intellectual property rights and proprietorship of images. Watermarking is a secure technique to protect our image against information piracy in communication networks and authenticated owner can prove ownership rights whenever needed.
Another key issue is robustness of watermarking algorithm to with stand the various kinds of distortion which is generated on transmission channel. The effective algorithm needs to have the following characteristics for robustness:

1. Imperceptibility: No visual difference between original and watermarked image. Even though there is no visual difference, some level of degradation is added by watermark image which is measured by PSNR.
2. Pay load: How much pixels of watermark data is embedded into host image which is based on our algorithm.
3. Robustness: In channel, watermarked image signal is compressed by JPEG for bandwidth constraint of the channel. The channel might generate Additive White Gaussian Noise (AWGN) or salt & pepper noise. Intruders attacks such as affine transformation, cropping to the extracted watermarked image for degrading the watermark image. Authenticated owner may apply mean, median filter for pre processing and scaling .The above mentioned distortions and attacks even happened but the proposed scheme provides acceptable level of extracted watermark image.

Digital watermarking is classified into three types based on the requirements of data during extraction process.

1. Non-Blind: Host image is needed to get the extraction process.
2. Blind: Host image is not required for extraction process.
3. Semi-Blind: Side information is needed for extracting process.

The proposed scheme is a Semi-Blind watermarking. Generally, watermarking is achieved in spatial domain or frequency domain. In spatial domain, modifying the specified pixel's bit which needed less hardware demand, easy to implement and low cost. Despite spatial domain is not robust against JPEG, affine transformation and cropping attacks. While the frequency domain has high robustness against these kinds of attacks, the proposed scheme is working in hybrid-frequency domain such as Discrete Wavelet Transform (DWT) followed by block based Discrete Cosine Transform (DCT). (i)DWT has good spatial-frequency localization property(ii)DCT has a high energy compaction property which packs most of the information into few coefficients.SV Decomposition used to factorize the matrix and embed the watermark signals which maintains the imperceptibility of watermarked image.

2. Background

Navneet Yadav etal [1] suggested a new spread spectrum based adaptive watermarking technique. This scheme used high entropy blocks for embedding the watermark bits. A high entropy block causes low visual sensitivity which gives good imperceptibility of watermarked image. This scheme has a variable strength factor which is adjusted to control the visual quality of the watermarked image. Drawback of this method is the high entropy of each block is defined by those blocks that are greater than or equal to average entropy of all the blocks. The number of high entropy blocks is not equal to watermark size to adjust the average entropy value which compromises the visual sensitivity and not withstand all kinds of geometrical attacks.

Tamirat Tagesse Takore etal [2] addressed a watermarking based on the genetic algorithm in a hybrid domain. In DWT-DCT based watermarking, SVD is applied on chosen frequency coefficients to embed the data in S components. Using genetics algorithm, the performance of the watermarking scheme was optimized. This method gives the acceptable visual quality of watermarked image and with stand signal processing and geometric attacks. Drawback of this method was not robust against rotation. Manuel Cedillo-Hernández [3] two distinct ways for embedding a watermark are used in this scheme. In the first move, the luminance component (Y) information was used to embed the watermark bit sequence into mid- frequency coefficients of the Discrete Fourier Transform (DFT).In the second move, a selected region of 2D histogram chrominance components was modified according to the watermark bit sequence. This method gives robustness against various attacks. Drawback of this method was the extraction of watermark image without the knowledge of the type of attack. Athanasios Nikolaidis [4] proposed moment and radial symmetry transform based watermarking. Image normalization can be done using moments, then applied radial symmetry transform which gives feature points for embedding the watermark data. Drawback of this method was not robust against signal processing attacks and high computational complexity. Yongqing Xin [5] proposed the moments based watermarking. This method was invariant to flipping, rotating and other signal processing attacks. The drawback of this method had high numerical manipulations and rotating attacks result gives less NC values compared to proposed method.

3. Proposed Algorithm

The proposed method is using hybrid transform domain on localization of host image (H) to improve the robustness against signal processing and geometrical attacks. We divide the host image (H) with size mxn into four non-overlapping sub images SIx with size m/2xn/2 x varies from 1,2,3,4. as can be seen in Fig.1.

Sub Image I	Sub Image II
Sub Image III	Sub Image IV

Figure 1: Host image divides into four sub images

One Level Discrete wavelet transform (DWT) is applied on each sub image which converts sub images in spatial domain into frequency domain sub bands LL_{1x}, HL_{1x}, LH_{1x}, HH_{1x}.We choose mid-frequency subbands HL and LH with size m/4xn/4.Here we use Haar wavelet. Then block based Discrete Cosine transform (DCT) is applied on LH and HL sub bands. We divide the LH and HL sub bands into 8x8 non overlapping block with size m/32 x n/32, then DCT II is applied on each blocks to form a E matrix with size m/32xn/32x4 from the selected mid frequency coefficients as can be seen in Fig.2.The watermark (W) is embedded in SVD of E. So that information is dispersed over the host image (H) and withstand the geometrical attacks. Generally, discrete cosine transform coefficient is expressed as a finite set of points (N) in terms of a sum of finite cosine function sampling points oscillating at different frequencies. It is expressed as

$$F(k,l)=\alpha(k)\,\alpha(l)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}W(m,n)\cos\left(\frac{(2m+1)}{2N}\right)\cos\left(\frac{(2n+1)}{2N}\pi l\right)$$ k=0, 1, 2 ...N-1

l=0, 1, 2 ... N-1 (1)

$$\alpha(k)=\begin{cases}\sqrt{\frac{1}{N}}\,if\,k=0\\ \sqrt{\frac{2}{N}}\,if\,k\neq 0\end{cases}\qquad \alpha(l)=\begin{cases}\sqrt{\frac{1}{N}}\,if\;l=0\\ \sqrt{\frac{2}{N}}\,if\,l\neq 0\end{cases}$$

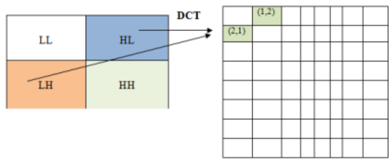

Figure 2: Mid-Frequency sub bands divided into 8x8 sub blocks

SVD Transform: In General, SVD transform is a factorization of a real or complex matrix.SVD transforms a matrix A with size mxn into $U\sum V^T$ where U is a real or complex unitary matrix with size mxm, $\sum$ is a singular values of matrix A with size mxn, V is an real or complex unitary matrix with size nxn. The columns vectors of U and V matrices are called left-singular vectors and right singular vectors. $\sum$ is a diagonal matrix of non negative singular entries is σ1> σ2> ....> σn. Consider eigen value and eigen vector relationship as

$$Ax=\lambda x \qquad (2)$$

Where A is a transformation matrix with size mxn, λ is a eigen value. If x is a eigen vector with size nx1, the equation won't make sense. In order to multiply A^T with A, this equivalent matrix is symmetric matrix and equation made sense.

$$A^TAv_i=\sigma_i^2v_i \quad \text{where } \sigma_i=\sqrt{\lambda_i} \qquad (3)$$

Where A^TA is the transformation matrix and σ_i^2 is the eigen value. Multiply both side on v_i^T we get $v_i^T A^TAv_i = \sigma_i^2 v_i^T v_i$ v is an orthogonal matrix so $v^T=v^{-1}$ and $v_i^T v_i=I$ where I is an identity matrix. $v_i^T A^TAv_i = \sigma_i^2$. Another matrix properties is $(v^TA^T)=(Av)^T$, So we get $(Av_i)^T(Av_i)=\sigma_i^2$.Finally,

$$\|Avi\|^2=\sigma_i^2 \qquad (4)$$

From equation (2) we multiply A on both sides we get $AA^TAv_i=\sigma_i^2 Av_i$, here Av_i is an eigen vector and σ_i^2 is an eigen value of AA^T

Now introduce a orthonormal vector matrix $u_i=\frac{Avi}{\sigma i}$ then we write

$$Av_i=u_i\,\sigma_i \qquad (5)$$

using orthogonal property have mentioned for $v^T=v^{-1}$

$$A=U\sum V^T \qquad (6)$$

Here instead of A, we are using E matrix with size m/32xn/32x4.The SV Decomposition is applied on matrix E, obtaining three sub-matrices

$$[U\;\; S\;\; V]=SVD\,(E) \qquad (7)$$

Watermark image is W with size m/16 x n/16 can be seen in Fig.3.Using Arnold transform with key (k) is applied on it to get the Scrambled image W_{scr}.

$$S_w=S+\sigma\, W_{scr} \qquad (8)$$

σ is the scaling factor which gives adjustable PSNR values of the watermarked image [6][7].

S_w is the modified singular value which carries the watermark bits. We have to form singular matrix where SV Decomposition is applied again on S_w. A small magnitude changes in the S matrix which reflects small degradation in the host image.

$$[U' \;\; S'_w \;\; V'] = SVD\,(S_w) \quad (9)$$

From the proof of equation (6) modified matrix (E') can be obtained by

$$E_w = U\, S'_w\, V^T \quad (10)$$

The coefficients of the E_w matrix are placed to the respective blocks and perform inverse discrete cosine transform (IDCT) on each block. The blocks are merged then applied inverse discrete wavelet transform (IDWT) for getting share image. The above mentioned processing steps are applied on each sub images and combined for getting the watermarked image (H_w).The proposed scheme is shown in Fig.3.

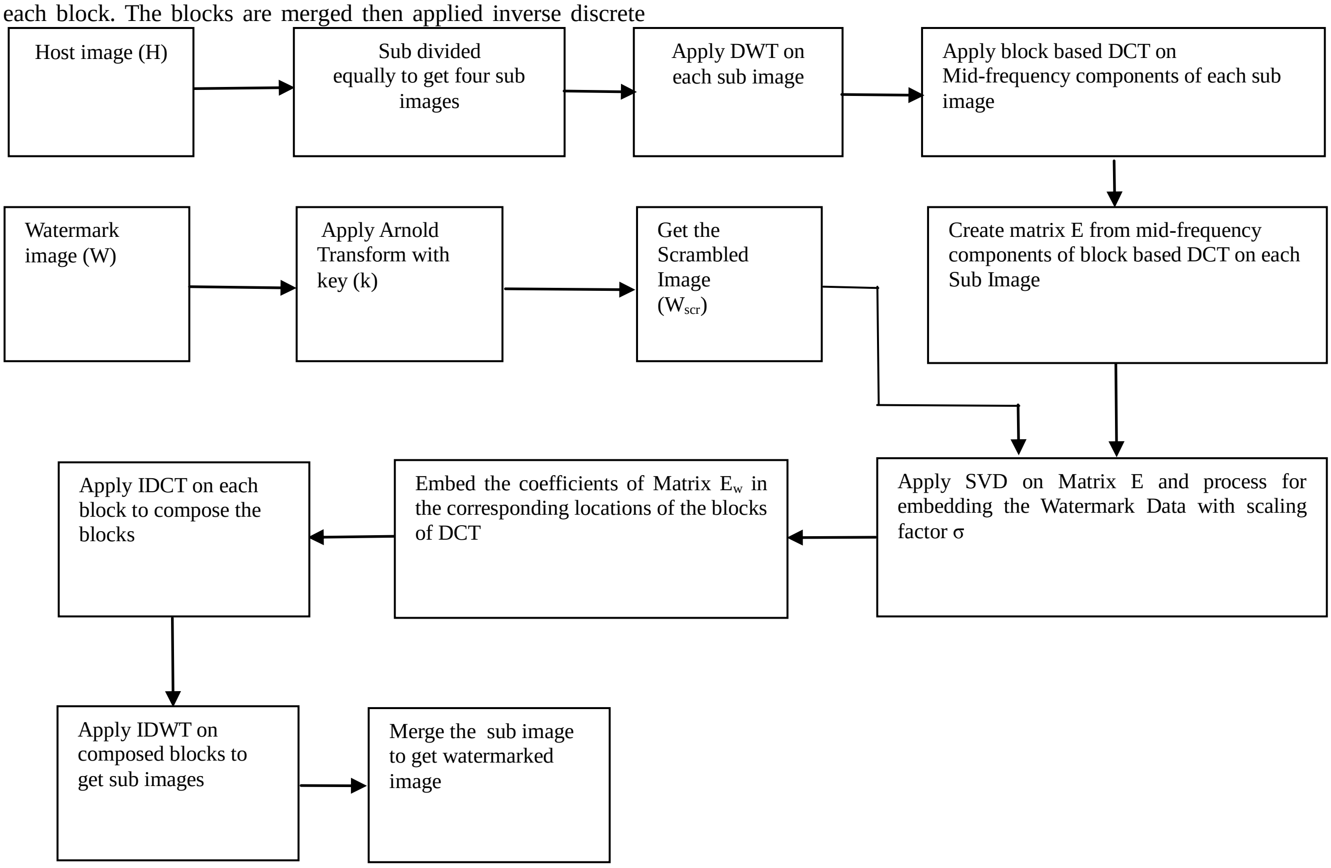

Figure 3: Watermark embedding procedure

Watermark Extracting Procedure

The watermarked image H_w may corrupt by signal processing and geometrical attacks when it is transmitted through insecure channel. The authenticated person restores the attacked watermarked image is H_{wa} which is subdivided into four sub images SI^*_x with size m/2xn/2 x varies from 1,2,3,4. Watermark Extracting Algorithm:

1. Apply one level Haar type DWT is applied on sub image $SI^*_{x.}$ to obtain four subbands LL_{1x}, HL_{1x}, LH_{1x}, HH_{1x} each one has size of m/4xn/4.
2. The mid-frequency subbands LH^* and HL^* of each sub image are partitioned into 8x8. Non-overlapping blocks with size of m/32xn/32.
3. Apply DCT II on each one block and select the embedded watermark coefficients which is located at (1, 2), (2,1) and form the matrix E^*.
4. Apply SV Decomposition on matrix E^*.

$$[U^* \;\; S^* \;\; V^*] = SVD\,(E^*) \quad (11)$$

5. Singular values S_w^* can be computed given below:

$$S_w^* = U' S^* V'^T \quad (12)$$

6. Generally attacked scrambled image of each sub image is

$$W^*_{scr} = (S^*_w - S)\,/\,\sigma \quad (13)$$

7. Inverse Arnold transform is applied on each scrambled matrix to get W^*_1,W^*_2,W^*_3,W^*_4 which has fractional value between 0 to 1.
8. Final extracted watermark image W_{ext} is determined by using thresholding technique is applied on W*.

4. Results and Analysis

This section we analyse the efficiency of the proposed algorithm. The proposed method uses the following metrics 1.PSNR (Peak

signal to Noise ration), 2.Normalized correlation 3.Bit Error Rate (BER) to evaluate the visual quality, imperceptibility, robustness against different kinds of attacks and error rate of extracted image. All our simulation results is performed using MATLAB R2014b 64-bit on a Sony SVE15133CNP system with 2 GB RAM, and i3 3120M at 2.50GHz processor with Ubuntu 14.04 LTS operating system. A standard host image is Lena with size 512x512. Watermark image size is m/16=32 n/16=32.The pay load depends on host image size. Here σ value is 0.5.Watermark and scramble image can be seen in Fig.4

Figure 4: (a) Watermark image (b) Scrambled image

PSNR

We evaluate the visual quality and imperceptibility of the watermarked image using PSNR. This is usually expressed in terms of dB. PSNR is defined as follows:

$$MSE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \| H(i, j) - - Hw(i, j) \|^2 \quad (14)$$

$$PSNR = 20 \log_{10}\left(\frac{\max(255)}{MSE}\right) \quad (15)$$

If PSNR value is high, then the watermark image is invisible and good visual quality. The PSNR value 30-50 dB is acceptable values for 8-bit image. The proposed scheme PSNR value is 87.63dB.In Fig.5 shows watermarked images their PSNR values is tabulated in Table I. The resultant values are good compared to the [3].

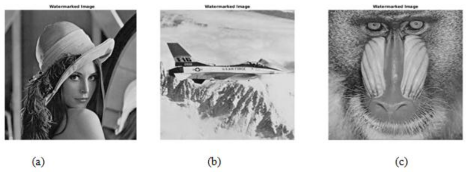

Figure 5: Watermarked image (a) lena (b) airplane-F16 (c) mandrill

Normalized Correlation

Normalized correlation is abbreviated as NC which measures robustness performance of the attacked image in a transmission channel. The difference between original watermark image (W) and extracted watermark image (W*). The value is between -1 to 1.High correlation gets 1 and no correlation is 0 and inverse correlation is -1.NC is defined by

$$\text{Normalized correlation (NC)} = \frac{\sum_{Bm}(W.Wext)}{\sqrt{\sum_{Bm}(Wext)^2}} \quad (16)$$

Table I: PSNR

Images	[3]dB	Proposed(dB)
Lena	49.4524	87.6396
Pepper	49.4440	87.7323
Cameraman	49.1441	86.7624
Barbara	47.5800	87.5341
Airplanef-16	48.4654	87.2790
Goldhill	49.1461	87.3252
Boat	48.0253	87.1417
Mandrill	47.7395	87.7144

Table II: Rotation Attack

Angle(Degree)	[5]	Proposed (NC)	Proposed (BER)
10	0.060	0.9128	0.0264
20	0.050	0.8990	0.0312
30	0.059	0.8594	0.0469
40	0.062	0.8569	0.0488
50	0.072	0.8582	0.0488
60	0.059	0.8621	0.0449
70	0.055	0.8921	0.0322
80	0.054	0.9249	0.0225
90	0.052	0.9449	0.0166

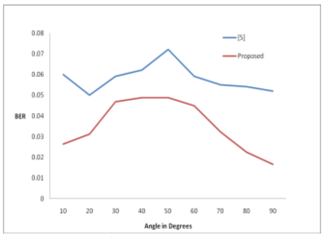

Figure 6: BER for Proposed and [5] Scheme

Table III: Filtering attacks

Median Filter						
Images	NC			BER		
	[3X3]	[5X5]	[7X7]	[3X3]	[5X5]	[7X7]
Lena	0.9232	0.9204	0.9066	0.0244	0.0254	0.0303
Pepper	0.9267	0.9212	0.9212	0.0234	0.0254	0.0254
Cameraman	0.9453	0.9282	0.9204	0.0166	0.0225	0.0254
Barbara	0.9468	0.9267	0.9239	0.0166	0.0234	0.0244
Airplanef-16	0.9458	0.9239	0.9239	0.0166	0.0244	0.0244
Goldhill	0.9542	0.9480	0.9234	0.0137	0.0156	0.0234
Boat	0.9317	0.9239	0.9212	0.0215	0.0244	0.0254
Mandrill	0.9354	0.9239	0.9049	0.0195	0.0244	0.0312
Mean Filter						
Images	NC			BER		
	[3X3]	[5X5]	[7X7]	[3X3]	[5X5]	[7X7]
Lena	0.9419	0.9212	0.9239	0.0176	0.0254	0.0244
Pepper	0.9193	0.9225	0.9154	0.0244	0.0244	0.0264

Cameraman	0.9360	0.8927	0.8954	0.0186	0.0322	0.0322
Barbara	0.9476	0.9253	0.9182	0.0156	0.0234	0.0254
Airplanef-16	0.9631	0.9384	0.9176	0.0107	0.0186	0.0254
Goldhill	0.9427	0.9445	0.9223	0.0166	0.0166	0.0234
Boat	0.9473	0.9232	0.9260	0.0156	0.0244	0.0234
Mandrill	0.8969	0.9140	0.8942	0.0312	0.0273	0.0322

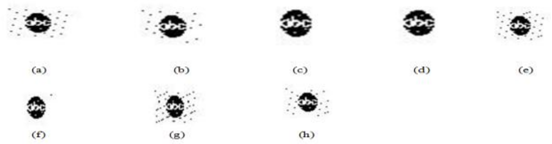

Figure 7: Extracted watermark after different kinds of attacks (a) Mean Filtering [3x3]. (b) Median Filtering [3x3]. (c) Gaussian Noise with variance 0.5(d)Salt &Pepper Noise with intensity 0.5 (e) JPEG compression with 10% quality (f) Histogram Equalization attack (g) Crop with 35% (h) Rotate the watermarked image with 50^{o}

Table IV: JPEG attack

JPEG Compression	Proposed (NC)	Proposed (BER)
10	0.9013	0.0322
20	0.9157	0.0273
30	0.9212	0.0254
40	0.9212	0.0254
50	0.9212	0.0254
60	0.9767	0.0068
70	0.9766	0.0068
80	0.9239	0.0244
90	0.9381	0.0195

Table V: Histogram Equalization attack

Images	NC	BER
Lena	0.9733	0.0078
Pepper	0.9766	0.0068
Cameraman	0.9699	0.0088
Barbara	0.9800	0.0059
Airplanef-16	0.9766	0.0068
Goldhill	0.9733	0.0078
Boat	0.9766	0.0068
Mandrill	0.9733	0.0078

Generally moment based watermarking is invariant to rotation. But numerical accuracy is needed. NC values of the proposed scheme provides not less than0.9.BER is also less than 0.05 can be seen in Fig.6 and tabulated with the values in Table II. Pre-processing steps for mean and median filtering with different window size provides good NC value which is not less than 0.89.The filtering result is shown in Table III. Due to Bandwidth constraint in a transmission medium, sending signal is compressed. Here JPEG standard can be used. The linear relationship between quality and NC values of compressed watermarked image is tabulated in Table IV. The visual quality is improved by Histogram equalization in receiver side. The proposed method gives good withstanding capability compared to the [2] has been tabulated in Table V&VI.

Table VI

[2]	
Histogram Equalization	
Images	NC
Lena	0.9378
Cameraman	0.9023
Salt &pepper noise	
Images	NC
Lena	0.9290
Cameraman	0.9188
Median filtering	
Images	NC
Lena	0.8284
Cameraman	0.8393
Gaussian noise	
Images	NC
Lena	0.9454

Cameraman	0.9159

Table VII: Gaussian Noise with variance 0.5

Images	Gaussian noise 0.5		Salt & pepper noise 0.5	
	NC	BER	NC	BER
Lena	0.9800	0.0059	0.9766	0.0068
Pepper	0.9800	0.0059	0.9766	0.0068
Cameraman	0.9733	0.0078	0.9733	0.0078
Barbara	0.9659	0.0088	0.9733	0.0078
Airplanef-16	0.8143	0.0684	0.9800	0.0059
Goldhill	0.9395	0.0176	0.9766	0.0688
Boat	0.9733	0.0078	0.9766	0.0068
Mandrill	0.9800	0.0059	0.9699	0.0088

Table VIII: Scaling Factor (Lena Image)

Scaling Factor	NC	BER
0.25	0.7006	0.1094
0.5	0.8546	0.0469
1.5	0.9433	0.0174
2.0	0.9578	0.0127
3	0.9716	0.0085
5	0.9820	0.0053
10	0.9904	0.0028

The proposed scheme gives more than 0.8 NC values and less than 0.08 BER against the signal processing attacks of Gaussian, Salt and pepper noise with respective variance 0.5 and intensity 0.5.Scaling level from 0.25 to 10 which gives linear relationship of NC and BER has been reduced linearly. This is tabulated in Table VIII. Table XI depicts the combination of signal processing and geometrical attacks and compare proposed scheme and [3] for NC and BER values. This provides better performance compared to [3].

Table IX: Combination of Attacks

Attack	Mandrill			Airplane-F16		
	DFT [3]	2D-H [3]	Prop	DFT [3]	2D-H [3]	Prop
JPEG (10%)+rotation(75^{o})	0.09	0.45	0.0078	0.15	0.43	0.0025
JPEG (20%)+translation(100,200)	0.01	0.45	0.1670	0.09	0.43	0.3672
JPEG (20%)+ centred cropping(35%)	0.03	0.43	0.0068	0.10	0.43	0.0088
JPEG (20%)+scaling(0.5)	0.09	0.45	0.0664	0.10	0.44	0.0703
JPEG (20%)+scaling(2)	0.01	0.45	0.0088	0.09	0.43	0.0093
JPEG (20%)+Gaussian noise(0.005)	0.06	0.53	0.0117	0.17	0.53	0.9289
JPEG (20%)+median filtering(3x3)	0.01	0.53	0.0244	0.10	0.53	0.0205
JPEG (20%)+Gaussian Filtering(3x3)	0.01	0.51	0.0195	0.09	0.53	0.0195
JPEG (20%)+histogram equalization	0.04	0.54	0.0078	0.10	0.57	0.0068

5. Conclusion

The proposed scheme withstands the signal and geometrical processing attacks and also provides high PSNR values. This semi-blind watermarking scheme is performed in hybrid frequency domain using DWT, DCT and SVD. We embed the watermark data in mid-frequency components this awards robustness against attacks. Imperceptibility is enlightened by varying the σ values for getting the good visual quality. Here we simulated the signal processing attacks JPEG, mean and median filtering, Salt and pepper noise, Histogram equalization and geometrical attacks such as rotation, translation, cropping, scaling on watermarked images. The metrics NC and BER gives better results compared to earlier schemes.

References

[1] Yadav N & Singh K, “Robust image-adaptive watermarking using an adjustable dynamic strength factor”, *Signal, Image and Video Processing Springer-Verlag London*, (2015), pp.1531–1542.

[2] Takore TT, Rajesh Kumar P & Lavanya Devi G, “A Modified Blind Image Watermarking Scheme Based on DWT, DCT and SVD domain Using GA to Optimize Robustness”, *International Conference on Electrical, Electronics, and Optimization Techniques*, (2016), pp.2725-2729.

[3] Cedillo-Hernández M, García-Ugalde F, Nakano-Miyatake M & Pérez-Meana HM, “Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification”, *Signal Image Video P.*, Vol.8, No.1, (2014), pp.49–63.

[4] Nikolaidis A, “Affine transformation invariant image watermarking using moment Normalization and radial symmetry transform”,*18th IEEE International Conference on Image Processing*, (2011), pp.2729-2732.

[5] Xin Y, Liao S & Pawlak M, “Circularly orthogonal moments for geo-metrically robust image watermarking”, *Pattern Recognit.*, Vol.40, No.12, (2007), pp.3740–3752.

[6] Hemalatha T, Joevivek V, Sukumar K & Soman K, “Robust water-marking of remote sensing images without the loss of spatial information”, *Proc. 10th ESRI India User Conf.*, Vol.1, No.2, (2009), pp.1–8.

[7] Praveen K & Sethumadhavan M, “A Probabilistic Essential Visual Cryptographic Scheme for Plural Secret Images”, *International Conference on Adv.Comp. Net. and Informatics*, Vol.2, (2014), pp.225-231.