Crypto-SVD based robust and protected digital image watermarking in discrete wavelet transform domain

Mayank Mishra [#1], Dr. Nirmal Kumar Rout[#2], Nageswara Rao Budipi[#3]

[#1] M. Tech Scholar, School of Electronics Engineering, KIIT University, Bhubaneswar, Odisha, India.
[1] mmishra1208@gmail.com

[#2] Professor, School of Electronics Engineering, KIIT University, Bhubaneswar, Odisha, India.
[2] routnirmal@rediffmail.com

[#3] Assistant Professor, School of Electronics Engineering, KIIT University, Bhubaneswar, Odisha, India.
[3] nageswar3521@gmail.com

Abstract— **With increase in image based applications, the necessity of providing security for the image data increases. Watermarking provides one of the best solution to overcome this issue. This paper presents the Crypto-SVD based robust image watermarking in Discrete wavelet transform (DWT) domain, in which the combination of cryptography and singular value decomposition (SVD) is applied in the DWT domain. The DWT is applied to the grayscale host image, which divides the image into low frequency (LL subband) and high frequency (HH, HL and LH subbands). The SVD is applied to HH subband and then encrypted watermark is embedded in the singular matrix of the SVD. In the proposed scheme the encrypted watermark is embedded in the host image. After encryption it is very difficult to predict the encrypted watermark, which saves the watermark from getting modified or destroyed. With various attacks i.e. image processing attacks, geometrical attacks, etc. the watermark is compared with the original watermark after extraction. The experimental results validate the robustness feature of the proposed scheme.**

Keyword - Digital image watermarking, Cryptography, SVD, DWT, Encryption, Robust.

I. INTRODUCTION

The expeditious growth in internet with evolution in the technology caused the popularity of digital media (audio, image, video etc.) in recent years. The main challenge is to solve the problem of protecting the media from the access of unauthorized person. Cryptography appear as a solution to this problem. But after the decryption of such media, it is very difficult to control its unauthorised circulation. Digital watermarking is proposed as the best solution, where the data (i.e. watermark) is permanently embedded into the host media. Generally the watermark is of two types: visible watermark and invisible watermark. Invisible watermark is the most commonly used watermark due to its application in various fields like data hiding, military purpose, medical purpose, etc. [1-2,4,12-14, 20]. To achieve the extreme protection, the watermark after embedding must have the following features:

1) The unauthorized person cannot remove it from the host data.
2) It should be invisible.
3) It should not be detectable statistically.
4) It should be resistant to lossy data compression.
5) It should be resistant to various common operations of image processing [3] .

An image watermarking scheme can be classified into two domains: spatial domain and transform domain. Image watermarking in transform domain are superior due to its excellent performance in comparison to an image watermarking in spatial domain [5-11,15-19]. In recent years several techniques are introduced in transform domain, among which wavelet transform appear as best technique due to its property of frequency localization [22].

LI Hui-fang et al. [5] puts forward a brief study on digital image watermarking in the discrete wavelet transform domain. Mohammad-Reza et al. [8] proposed a robust watermarking scheme in DWT domain. The watermark is embedded into the significant coefficients of wavelets in the dynamic blocks. The scheme is suitable for maps and natural image having better edges. Sukalyan Som et al. [9] proposed a scheme in which DWT based watermark is embedded in multiple region to perform well against critical tampering situations. Ho Seok Moon et al. [3] proposed a scheme in which DWT coefficient of two sub image is compared by four DWT sub image. Inducement of this scheme is to develop a watermarking scheme where the original image is not required during extraction of watermark. Ali Al-Haj [6] and R H Laskar et al. [7] proposed a scheme in which DWT and Discrete Cosine Transform (DCT) are combined for an image watermarking. The combination of

both the transform improves the performance in comparison to only the DWT watermarking. Thai-Son Nguyen [10] proposed a scheme which is reversible, invisible and correctly verify the tampered region. In this scheme, the authentication code is randomly generated and is embedded at low frequency subband of 2nd level of DWT. Nasrin M Makbol et al. [21] proposed a scheme which is based on Redundant Discrete Wavelet Transform (RDWT) and Singular Value Decomposition (SVD). The scheme appears to be robust against various image processing and geometrical attacks. Razieh Keshavarzian et al. [22] proposed a scheme based on region of interest using the Arnold map in the discrete wavelet transform domain. It fulfils various features like imperceptibility, robustness and security.

All the existing schemes show robustness but there is always a chance of improvement. Our proposed scheme combined cryptography and the SVD in the DWT domain. It provides robustness against various attacks by combining the SVD in the DWT domain.

II. DISCRETE WAVELET TRANSFORM (DWT)

Wavelet are used as basal function in representation of signal. It is comparable to sine and cosine in the Fourier study. The DWT is similar as dealing with the image by 2-D filter in every extent when applied to 2-D images. A filter splits the image into four non-imbricate ambiguous-resolution subbands LL, LH, HL and HH as shown in Fig. 1. The LL subband shows the approximation part of the image and high frequency subbands (HH, HL and LH) shows the detailed part of the image. For further splitting of wavelet coefficients, the LL part is repeatedly divided till some final required scale M is obtained. After the completion of splitting, there will be (3M+1) subband which will consist of different resolution subbands such as, LL_M , LH_y, HL_y and HH_y, where y lies between 1 and M.

Edges and texture of image exist in high frequency subband, and the eye of human is very less sensitive to changes in these high frequency subbands. This gives the advantage for embedding the watermark in high frequency subband [6].

III. SINGULAR VALUE DECOMPOSITION (SVD)

The SVD is a method of diagonalisation of a symmetric matrix. It splits the given matrix D (i.e. image) into three matrices as,

$$D = (A) . (B) . (C)T \quad (1)$$

LL	HL
LH	HH

Fig.1. Image sub-bands after DWT

where B is the diagonal matrix and it contains the singular values in decreasing manner. The decomposed and detailed information of the image are carried by matrices A and C. If the matrix D is rectangular matrix of order m x m, the diagonal matrix B will have maximum '*m'* number of diagonal elements.

A and C matrices satisfy few important property, such as

$$A.A^T = I_M \quad (2)$$

$$C.C^T = I_M \quad (3)$$

where I_m is the identity matrix of order m x m and the diagonal elements of the matrix B satisfies the following property:

$$e_1 \geq e_{2.....}e_z > e_{z+1} > e_{z+2.....} > e_m = 0 \quad (4)$$

where z ($\leq$ m) is the rank of diagonal matrix B and e_1, e_2,.....e_m are the diagonal elements of the matrix B [11]. In watermarking, the SVD is extensively used as transform because of its compelling properties. It is not used alone because of its complexity [2].

IV. THE PROPOSED SCHEME

The proposed scheme is described in this section. It includes two major steps such as, watermark embedding and extraction of watermark. The watermark embedding involves two processes such as encryption of watermark and embedding of encrypted watermark. In the same manner the extraction of watermark involves two processes such as extraction of encrypted watermark and decryption of extracted encrypted watermark. For validation of robustness, various image processing attacks and geometrical attacks are applied on the watermarked image. The watermark is compared with the original watermark on the scale of normalised correlation (NC) value and bit error rate (BER) value.

A. Watermark Embedding

The watermark embedding involves two steps such as: encryption of watermark and embedding of encrypted watermark. The details of the watermark embedding is briefly described in a flow diagram as shown in Fig.2.

1) Encryption of watermark

It involves three steps:

Step 1: Let the image have pixels P_i having different intensity at respective positions, where *i* lies between 1 to 256.

$$P_i = p_1, p_2, p_3, p_4.....$$

Let K be the key required for encryption, where

$$K = k_1, p_1, p_2, p_3, p_4.....$$

Let C_i be the ciphered pixels, where

$$C_i = (P_i + K) \bmod 256 \quad (5)$$

$$C = c_1, c_2, c_3, c_4,.....$$

where C is the ciphered image matrix.

This step1 is known as the algorithm of *auto cipher key*. Here, only first key is given by the owner of the given image and rest keys are automatically get selected from the given image's pixel values. It saves the time of giving the number of keys manually. After step1 *Block swapping* operation is applied to the ciphered image.

Step 2: Block swapping is applied on the ciphered image matrix 'C'.

For the block swapping, first half row of the ciphered image matrix C is placed at the second half row of the ciphered image matrix and vice versa. Similarly, first half column of the ciphered image matrix C is placed at the second half column of the ciphered image matrix and vice versa, i.e.,

First half row $\longleftrightarrow$ Second half row

First half column $\longleftrightarrow$ Second half column

The symbol '$\longleftrightarrow$' indicates swapping. The final step of encryption is applied on the ciphered image after step2.

Step 3: An image 'R' of random pixel having same size as the watermark is created. Exclusive-or (XOR) operation is performed between R and the ciphered image after step2 i.e.

$$X = R \oplus \text{ciphered image after step2} \quad (6)$$

where X is the final encrypted image to be embedded in the host image and the symbol '$\oplus$' represents the exclusive-or operation.

2) Embedding of watermark

It involves two steps:

Step 1: The DWT is applied to the gray scale host image, which splits the host image into four subbands (LL, LH, HL and HH).

Step 2: The SVD is applied to the HH subband, which split the HH subband into three matrices as follows,

$$D = (A) . (B) . (C)^T \quad \text{(from eqn. 1)}$$

where B is the diagonal matrix having singular values and D represents the HH subband.

The encrypted watermark X obtained after step 2 of the encryption of watermark is embedded in the matrix B. The resultant matrix is denoted by matrix W is defined as follows,

$$W = B + kX \quad (7)$$

where k is scaling factor.

And the SVD is again applied on the matrix W as follows:

$$W = A_w . B_w . C_w^T \quad (8)$$

The watermarked image D_w is obtained using matrix W as follows:

$$D_w = IDWT (D_{S)} \quad (9)$$

where IDWT is inverse DWT operation, and

$$D_S = (A) . (W) . (C)^T \quad (10)$$

B. Extraction of Watermark

After the embedding of watermark in the host image, various image processing and geometrical attacks are applied on the watermarked image and we get attacked watermarked image $D_w^{\#}$. It involves two steps: extraction of encrypted watermark from attacked watermarked image and decryption of extracted encrypted watermark as shown in Fig.3.

1) Extraction of Encrypted watermark

It involves two steps:

Step 1: The DWT is applied to the watermarked image $D_w^{\#}$, which splits the watermarked image into four subbands (LL, LH, HL and HH).

Step 2: The SVD is applied to the HH subband as follows:

$$D^{\#} = A^{\#} . W^{\#} . C^{\#T} \quad (11)$$

then again the SVD is performed on W matrix

$$W^{\#} = A_w . B_w^{\#} . C_w^{T} \quad (12)$$

$$X^{\#} = \frac{W^{\#} - B}{K} \quad (13)$$

where $X^{\#}$ is the extracted encrypted image. Here '#' shows the distortion due to various applied attacks.

2)Decryption of Encrypted watermark

The steps involved during encryption of the watermark are applied in reverse manner during decryption.

Step 1: The XOR operation is applied between the extracted encrypted image and image R of random pixels.

$$X \oplus R = M \quad (14)$$

where M is the ciphered image after step2 during encryption.

Step 2: Block swapping is applied in a reverse manner as applied in encryption.

First half column of the M matrix is placed at the second half column of the M matrix and vice versa. Similarly, second half row of the M matrix is placed at the first half row of the M matrix and vice versa, i.e.,

Second half column ⟷ First half column

Second half row ⟷ First half row

After block swapping operation the resultant matrix is denoted by 'S'. The final step of decryption is applied on the S matrix.

Step3: Reverse operation of auto cipher key is applied during decryption.

$$Pi = (Si - K) \bmod 256 \quad (15)$$

where Pi is the pixels having different intensities of the host image, Si shows the set of pixel having intensities at respective position and *i* lies between 1 to 256 and K is the key.

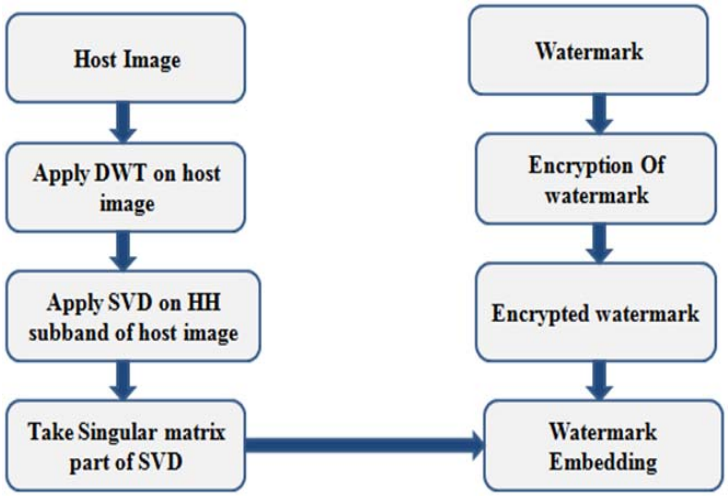

Fig.2. Flow diagram of watermark embedding

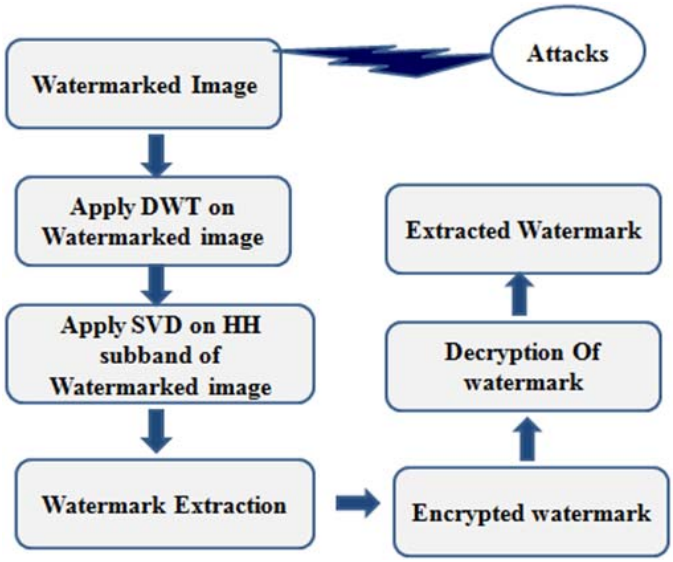

Fig. 3. Flow diagram of watermark extraction

V. EXPERIMENTAL RESULTS

The proposed scheme is tested on different standard gray scale images: Lena, Boat, Peppers and Baboon of size 512 x 512 . Gray scale watermark image of size 256 x 256 is considered during simulation. All the simulation is performed using MATLAB R2015a and Haar wavelet is used for the DWT operation. Scaling factor k is taken as 10 in the proposed scheme. From the experimental result the invisibility feature is achieved simply by visualising the watermarked image. The main focus of the proposed scheme is to increase the robustness. The extracted watermark from attacked watermarked image is compared with the original watermark on the scale of normalised correlation (NC) value and bit error rate (BER) value. The NC value closer to 1 and the BER value closer to 0 shows the maximum similarity.

The NC value is calculated as,

$$\mathrm{NC} = \frac{\sum_{a=1}^{D1}\sum_{b=1}^{D2} M(a,b)\,.\,Me(a,b)}{\sqrt{\sum_{a=1}^{D1}\sum_{b=1}^{D2} M(a,b)^2}\ \sqrt{\sum_{a=1}^{D1}\sum_{b=1}^{D2} Me(a,b)^2}} \tag{16}$$

where M is the original watermark and Me is the extracted watermark. D_1 and D_2 are the dimension of watermark and (a, b) are the pixels coordinate of the watermark.

The BER value is calculated as,

$$\mathrm{BER} = \frac{1}{S}\sum_{x=1}^{S} |Me(x) - M(x)| \tag{17}$$

where Me, M and S is the extracted watermark, real watermark and watermark size respectively.

Following attacks are applied on the watermarked image for testing robustness of the proposed scheme:

1) Salt and pepper noise attack (density = 0.1,0.2, 0.3 and 0.4)
2) Gamma correction attack (0.6, 0.7 and 0.8)
3) Speckle noise attack (variance = 0.01, 0.1, 0.3 and 0.4)
4) Gaussian noise attack (mean =0, variance = 0.1, 0.4, 0.5, 0.6 and 0.7)
5) Rotation attack (2˚, 30˚, 100˚ and -30˚)
6) JPEG attack (Q = 5, 10, 30 and 40)
7) Median filtering attack (3x3, 5x5 and 7x7)
8) Weiner filtering attack (2x2 and 3x3)
9) Gaussian filtering attack (3x3 and 5x5)
10) Scaling attack (Zoom out = 0.25 and 0.5, Zoom in = 4 and 2)
11) Shearing attack (x = 1 and 0.2, y = 0.2 and 1)
12) Cut attack (10, 20 and 30)
13) Translate attack [(10,10), (10,20) and (20,35)]
14) Sharpening attack

15) Histogram equalisation attack
16) Cropping attack (25% and 50 %)
17) Motion blur attack (70 pixels, 100˚)

By visualising the different watermarked images i.e. Lena, Baboon, Pepper and Boat as shown in Fig. 4, the invisibility propoerty of the proposed scheme is tested. The original watermark is shown in Fig. 5 and the encrypted watermark after applying the encryption algorithm is shown in Fig. 6. Attacked watermarked image by various attacks as shown in Fig. 7(a)-21(a) and the extraction of watermark from the respective attacked watermarked images as shown in 7(b)-21(b) validates the reversibility property. To test the robustness properly, extracted watermark is compared with the original watermark on the NC and BER value scale. The Table1 and the Table2 gives the NC value and BER values respectively at various attacks on the Lena, Baboon, Boat and Peppers images.

Fig. 4(a). Lena watermarked image

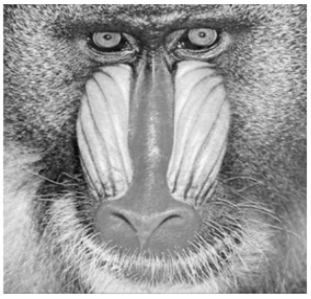

Fig. 4(b). Baboon watermarked image

Fig. 4(c). Pepper watermarked image

Fig. 4(d). Boat watermarked image

Fig. 5. Original watermark

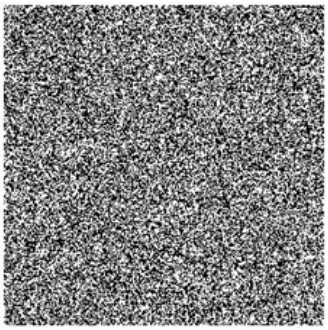

Fig. 6. Encrypted watermark

Fig. 7(a). Gaussian noise(variance=0.4)

Fig. 7(b). Extracted watermark

Fig. 8(a). Rotation attack(30˚)

Fig. 8(b). Extracted watermark

Fig. 9(a). JPEG attack(Q=5)

Fig. 9(b). Extracted watermark

Fig. 10(a). Median filtering (7x7)

Fig. 10(b). Extracted watermark

Fig. 11(a). Weiner filtering(3x3)

Fig. 11(b). Extracted watermark

Fig. 12(a). Gaussian filtering(5x5)

Fig. 12(b). Extracted watermark

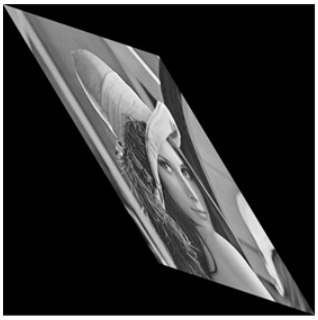

Fig. 13(a). Shearing attack(x=0.2, y=1)

Fig. 13(b). Extracted watermark

Fig. 14(a). Cut attack(30)

Fig. 14(b). Extracted watermark

Fig. 15(a). Translate attack(20, 35)

Fig. 15(b). Extracted watermark

Fig. 16(a). Sharpening attack

Fig. 16(b). Extracted watermark

Fig. 17(a). Histogram eq. attack

Fig. 17(b). Extracted watermark

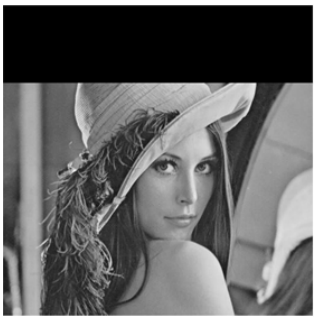

Fig. 18(a). Cropping attack(25%)

Fig. 18(b). Extracted watermark

Fig. 19(a). Motion blur attack

Fig. 19(b). Extracted watermark

Fig. 20(a). Speckle noise(variance=0.1)

Fig. 20(b). Extracted watermark

Fig. 21(a). Salt and pepper attack(d=0.4)

Fig. 21(b). Extracted watermark

TABLE I : NORMALISED CORRELATION VALUE AT DIFFERENT ATTACKS ON DIFFERENT IMAGES

Attacks	**Lena**	**Baboon**	**Pepper**	**Boat**
Gamma correction(0.8)	0.9966	0.9965	0.9966	0.9964
Gamma correction(0.7)	0.9967	0.9966	0.9966	0.9965
Gamma correction(0.6)	0.9967	0.9966	0.9966	0.9965
Salt and pepper noise (density =0.4)	0.9957	0.9958	0.9957	0.9957
Salt and pepper noise (density =0.3)	0.9958	0.9958	0.9957	0.9957
Salt and pepper noise (density =0.2)	0.9958	0.9959	0.9958	0.9958
Salt and pepper noise (density =0.1)	0.9959	0.9959	0.9958	0.9958
Speckle noise (variance = 0.5)	0.9957	0.9957	0.9956	0.9957
Speckle noise (variance = 0.4)	0.9957	0.9957	0.9957	0.9957
Speckle noise (variance = 0.3)	0.9958	0.9958	0.9958	0.9958
Speckle noise (variance = 0.1)	0.9959	0.9959	0.9958	0.9959
Speckle noise (variance = 0.01)	0.9959	0.9959	0.9958	0.9959
Gaussian noise (mean=0, variance =0.7)	0.9957	0.9957	0.9957	0.9957
Gaussian noise (mean=0, variance =0.6)	0.9957	0.9958	0.9957	0.9957
Gaussian noise (mean=0, variance =0.5)	0.9957	0.9959	0.9958	0.9958
Gaussian noise (mean=0, variance =0.4)	0.9958	0.9959	0.9958	0.9959
Rotation(2˚)	0.9957	0.9957	0.9957	0.9957
Rotation(30˚)	0.9958	0.9958	0.9957	0.9958
Rotation(100˚)	0.9958	0.9958	0.9958	0.9959
Rotation(-30˚)	0.9959	0.9959	0.9958	0.9959
Jpeg(q=5)	0.9906	0.9910	0.9908	0.9907
Jpeg(q=10)	0.9955	0.9955	0.9955	0.9955
Jpeg(q=30)	0.9955	0.9956	0.9956	0.9956
Jpeg(q=40)	0.9956	0.9956	0.9956	0.9958
Median filtering(3x3)	0.9957	0.9957	0.9956	0.9957
Median filtering(5x5)	0.9956	0.9957	0.9955	0.9955
Median filtering(7x7)	0.9955	0.9955	0.9955	0.9955
Mean filtering(3x3)	0.9958	0.9957	0.9956	0.9956
Weiner filtering(2x2)	0.9958	0.9960	0.9957	0.9958
Weiner filtering(3x3)	0.9957	0.9958	0.9956	0.9957
Gaussian filtering(3x3)	0.9958	0.9959	0.9957	0.9958
Gaussian filtering(5x5)	0.9957	0.9958	0.9957	0.9958
Scaling(zoom out=0.25, Zoom in= 4)	0.9945	0.9943	0.9945	0.9943
Scaling(zoom out=0.5, Zoom in= 2)	0.9949	0.9955	0.9957	0.9955
Shearing(x=1, y=0.2)	0.9958	0.9961	0.9957	0.9958
Shearing(x=0.2, y=1)	0.9958	0.9961	0.9957	0.9958
Cut(10)	0.9967	0.9967	0.9967	0.9967
Cut(20)	0.9967	0.9966	0.9967	0.9967
Cut(30)	0.9965	0.9965	0.9966	0.9966
Translate(10,10)	0.9967	0.9967	0.9967	0.9967
Translate(10,20)	0.9962	0.9966	0.9966	0.9965
Translate(20,35)	0.9957	0.9958	0.9958	0.9957
Sharpening	0.9957	0.9956	0.9957	0.9958
Histogram equalization	0.9957	0.9956	0.9957	0.9958
Cropping(25%)	0.9961	0.9959	0.9957	0.9960
Cropping(50%)	0.9843	0.9840	0.9809	0.9818
Motion blur (70 pixel, 100˚)	0.9958	0.9957	0.9957	0.9956

TABLE II : BER VALUES AT DIFFERENT ATTACKS ON DIFFERENT IMAGES

Attacks	**Lena**	**Baboon**	**Pepper**	**Boat**
Gamma Correction(0.8)	0.0059	0.0062	0.0061	0.0064
Gamma Correction(0.7)	0.0058	0.0059	0.0060	0.0066
Gamma Correction(0.6)	0.0058	0.0059	0.0059	0.0064
Salt and pepper noise(density =0.4)	0.0076	0.0073	0.0076	0.0075
Salt and pepper noise(density =0.3)	0.0074	0.0073	0.0075	0.0075
Salt and pepper noise(density =0.2)	0.0074	0.0071	0.0074	0.0074
Salt and pepper noise(density =0.1)	0.0073	0.0070	0.0074	0.0074
Speckle noise (variance = 0.5)	0.0075	0.0075	0.0078	0.0076
Speckle noise (variance = 0.4)	0.0075	0.0075	0.0075	0.0075
Speckle noise (variance = 0.3)	0.0074	0.0074	0.0074	0.0072
Speckle noise (variance = 0.1)	0.0073	0.0072	0.0074	0.0072
Speckle noise (variance = 0.01)	0.0073	0.0072	0.0074	0.0072
Gaussian noise (Mean=0, variance =0.7)	0.0076	0.0075	0.0076	0.0076
Gaussian noise (Mean=0, variance =0.6)	0.0076	0.0073	0.0076	0.0074
Gaussian noise (Mean=0, variance =0.5)	0.0075	0.0073	0.0074	0.0074
Gaussian noise (Mean=0, variance =0.4)	0.0073	0.0073	0.0074	0.0072
Rotation(2˚)	0.0076	0.0076	0.0075	0.0072
Rotation(30˚)	0.0075	0.0074	0.0075	0.0072
Rotation(100˚)	0.0075	0.0073	0.0074	0.0071
Rotation(-30˚)	0.0074	0.0071	0.0074	0.0071
JPEG(Q=5)	0.0164	0.0161	0.0162	0.00163
JPEG(Q=10)	0.0079	0.0078	0.0079	0.0079
JPEG(Q=30)	0.0079	0.0078	0.0078	0.0077
JPEG(Q=40)	0.0079	0.0078	0.0078	0.0074
Median Filtering(3x3)	0.0076	0.0075	0.0077	0.0075
Median Filtering(5x5)	0.0077	0.0076	0.0078	0.0079
Median Filtering(7x7)	0.0079	0.0079	0.0079	0.0079
Mean Filtering(3x3)	0.0076	0.0076	0.0077	0.0077
Weiner Filtering(2x2)	0.0073	0.0070	0.0076	0.0075
Weiner Filtering(3x3)	0.0076	0.0074	0.0077	0.0075
Gaussian Filtering(3x3)	0.0075	0.0072	0.0075	0.0074
Gaussian Filtering(5x5)	0.0076	0.0074	0.0076	0.0076
Scaling(Zoom out=0.25, Zoom in= 4)	0.0096	0.010	0.0080	0.0117
Scaling(Zoom out=0.5, Zoom in= 2)	0.0090	0.0080	0.0076	0.0079
Shearing(x=1, y=0.2)	0.0074	0.0069	0.0076	0.0074
Shearing(x=0.2, y=1)	0.0074	0.0069	0.0075	0.0073
Cut(10)	0.0058	0.0058	0.0058	0.0067
Cut(20)	0.0058	0.0061	0.0059	0.0067
Cut(30)	0.0059	0.0061	0.0059	0.0068
Translate(10,10)	0.0058	0.0058	0.0058	0.0058
Translate(10,20)	0.0067	0.0060	0.0058	0.0058
Translate(20,35)	0.0076	0.0235	0.0075	0.0118
Sharpening	0.0076	0.0077	0.0076	0.0074
Histogram Equalization	0.0076	0.0078	0.0073	0.0072
Cropping(25%)	0.0068	0.0073	0.0076	0.0070
Cropping(50%)	0.0274	0.0279	0.0330	0.0131
Motion Blur (70 pixel, 100˚)	0.0075	0.0075	0.0075	0.0077

Experimental results validate the robustness of the proposed scheme, as the NC value and BER value from the Table 1 and the Table 2 is closer to one and closer to zero respectively in every attack. It is concluded that our proposed scheme is robust not only for the single image but for all the images.

VI. CONCLUSION

This paper proposed the scheme which combines the cryptography and the SVD in the DWT domain. The encryption of watermark is carried out before embedding for image hiding purpose. It is difficult to predict the encrypted watermark so it can't be modified or corrupted. The DWT is applied to the gray scale host image. Then the SVD is performed on the HH subband which splits the HH subband into three matrices. The encrypted watermark is embedded in the singular matrix of the SVD. Similarly, the same process is performed for watermark extraction in the reverse manner. Experimental results validate the robustness property by comparing the extracted watermark with the original watermark on the basis of NC values and BER values. Robustness feature on the basis on NC value and BER value is also compared for various images. The experimental results validates the robustness of the proposed scheme. The reversibility property is achieved as the extraction of watermark is possible from the watermarked image and invisibility property is achieved as the watermarked image appears same as the original host image. Hence, the proposed scheme increases the robustness against various attacks and provide protection from unauthorised access of the data (i.e. image). The proposed scheme also has some limitation, it cannot be directly applied to the coloured images. Future work will be focused to overcome this limitation.

REFERENCES

[1] Padilla-Lopez Jose Ramon, Chaaraoui Alexandros Andre, Florez-Revuelta Francisco, Visual privacy protection method a survey, Elsevier-Experts systems with applications , vol. 42, pp.4177-4195, 2015.
[2] Nasrin Makbol, Be e Khoo, Taha Rassem, Block based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics, IET Image processing, vol.10, pp. 34-52, 2016.
[3] Ho Moon, Myung Sohn, Dong Jang, DWT- based image watermarking for copyright protection, Springer-Verlang Berlin Heidelberg-Lecture notes in computer science, pp. 490-497, 2005.
[4] Long Bao, Yicong Zhou, Image encryption generating visually meaningful encrypted images, Elsevier-Information science, vol.324, pp.197-207, 2015.
[5] LI Hui-fang, CHANG Ning, CHEN Xiao-ming, A study on image watermarking based on wavelet transform, Elsevier-The journal of China universities of posts and tellecommunication, vol.17, pp.122-126, 2010.
[6] Ali Al-Haj, Combined DWT-DCT digital image watermarking, Journal of computer science, vol.3, pp.740-746, 2007.
[7] R H Laskar, Madhuchanda Choudhury, Krishna Chakraborty, Shoubhik Chakraborty, A joint DWT-DCT based robust digital watermarking algorithm for ownership verification of digital images, Springer-CCIS, pp. 482-491, 2011.
[8] Mohammad-Reza Keyvanpour, Farnoosh Merrikh-Bayat, Xiao-ming Chen, Robust dynamic block based image watermarking in DWT domain, Elsevier-WCIT, vol.3, pp.238-242, 2010.
[9] Sukalyan Som, Sarbani Palit, Krishnath Dey, Dipabali Sarkar, Jayeeta Sarkar, Kheyali Sarkar, A DWT-based digital watermarking scheme for image temper detection localization and restoration, Springer-transaction, pp.17-36, 2015.
[10] Thai-son Nguyen, Chin-Chen Chang, Xiao-Qian Yang, A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain, Elsevier-International journal of electronics and communications, vol.70, pp.1055-1061, 2016.
[11] Irshad Ahmad Ansari, Millie Pant, Chang Wook Ahn, Robust and false positive free watermarking in IWT domain using SVD and ABC, Elsevier-Engineering applications of artificial intelligence, vol.49, pp.114-125, 2016.
[12] Ensherah A Naeem et al., Efficient implementation of chaotic image encryption in transform domains, Elsevier-The journal of system and software, vol.97, pp.118-127, 2014.
[13] Li Jiang, Zhengquan Xu, Yanyan Xu, A new comprehensive security protection for remote sensing image based on the integration of encryption and watermarking, IEEE-IGARSS, pp.2577-2580, 2013.
[14] Dong Zong, Chun Chen, The study of digital watermarking for protection of multimedia, IEEE 2nd International conference on computing control and industrial engineering, pp.304-307, 2011.
[15] Vinita Gupta, Atul Barve, Robust and secured image watermarking using DWT and encryption with QR codes, International Journal of computer applications, vol.100, pp.33-37, 2014.
[16] Osama S Faragallah, Efficient video watermarking based on singular value decomposition in discrete wavelet transform domain, Elsevier- Elsevier-International journal of electronics and communications, vol.67, pp.189-196, 2013.
[17] Asna Furqan, Munish Kumar, Study and analysis of robust DWT-SVD domain based digital image watermarking using MATLAB, IEEE-CICT , pp.638-644, 2015.
[18] Gursharanjeet Singh Kalra, Rajnish Talwar et al, Robust blind digital image watermarking using DWT and dual encryption technique, IEEE-CICSyN, pp.225-229, 2011.
[19] Roop Singh, Rekha Gupta et al, Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on psnr, IEEE-CSNT, pp.593-595, 2011.
[20] Sena Reddy M Indra, Siva Kumar A P, Secured data transmission using wavelet based stegnography and cryptography by using AES algorithm, Elsevier-CMS , vol.85, pp.62-69, 2016.
[21] Nasrin Makbol, Be e Khoo, Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, Elsevier-International journal of electronics and communications, vol.67, pp.102-112, 2013.
[22] Razieh Keshavarzian, Ali Aghagolzadeh, ROI based robust and secure image watermarking using DWT and arnald map, Elsevier-International journal of electronics and communications, vol.70, pp.278-288, 2016.

AUTHOR PROFILE

Mayank Mishra was born in Gorakhpur, Uttar Pradesh, India, in 1994. He has completed Dual M.Tech in Communication System Engineering at KIIT University, Bhubaneswar, Odisha, India. His current interests are Digital watermarking, Image processing, Digital signal processing and Cryptography.
Email**:** mmishra1208@gmail.com

Dr. Nirmal Kumar Rout received the B.E. degree in Electronics and Telecommunication Engineering from the University College of Engineering (presently known as Veer Surendra Sai University of Technology), Sambalpur University, Burla, India, in 1991and the M. Tech degree in computer science from the Utkal University, Bhubaneshwar, India, in 2001. He is awarded with PhD degree in Electronics and Telecommunication Engineering from the Kalinga Institute of Industrial Technology (KIIT) University, Bhubaneshwar, India, in 2014. From 1993 to 2002, he was a Lecturer with the Department of Electronics and Communication Engineering, Orissa Engineering College, Bhubaneswar. He also served as a Faculty Member of the Institute of Chartered Financial Analysts of India (ICFAI) Institute of Science Technology (ICFAITech), Hyderabad, India, from 2002 to 2007. He is currently working as Professor with the School of Electronics Engineering, KIIT University, Bhubaneshwar, India. He has published number of research papers in various refereed international journals and conferences. His current research interests include active noise control, adaptive signal processing, soft computing, evolutionary computing and image processing.
E-mail: routnirmal@rediffmail.com, nkrout@kiit.ac.in.

Nageswara Rao Budipi received the B.Tech. degree in Electronics and Communication Engineering from the VR Siddhartha Engineering college, Acharya Nagarjuna University, Andhra Pradesh, India, in 2010 and the M. Tech degree in Electronics and Communication Engineering (Signal Processing) from the National Institute of Technology Calicut, Kerala, India, in 2013. He is currently working as an Assistant Professor in the School of Electronics Engineering, KIIT University, Bhubaneswar, India. His current research interests include machine learning, computer vision and image processing.
E-mail: nageswarfet@kiit.ac.in, nageswar3521@gmail.com.