# DWT-SVD Based Watermarking Scheme of JPEG Images Using Elliptic Curve Cryptography

**Ritu Gupta[1], Pulkit Mundra[2], Shikha Karwal[3], Abhilasha Singh[4]**

*[1,2,3,4]Department of Information Technology, Amity University, Uttar Pradesh, India*
*[1]ritu4006@gmail.com, [2]pulkitmundra28@gmail.com, [3]shikhakarwal07@gmail.com, [4]abhilashasingh28@gmail.com*

*Abstract:* **The image watermarking technology is a vital facet about multimedia authentication and copyright protection to improve its reliability and security. This paper proposes an embedment of encrypted watermark in a JPEG image to address the issues of proprietorship of digital images. Amongst the cryptographic solutions, the most satisfactory cryptography method is Elliptic Curve Cryptography because of its small usage of bandwidth, low computational time and small key size. DWT and SVD are used as a scientific means to implant watermark in the image. The quality of watermarked image is measured by Peak signal to noise ratio (PSNR) and to compare the recovered watermark and the original watermark Normalized correlation (NC) is used.**

*Keywords:* **Elliptic Curve Cryptography, Discrete Wavelet Transform, Singular Value Decomposition, Watermarking.**

## I. INTRODUCTION

Digital watermarking is the procedure by which the proprietorship of multimedia data is protected. It avoids fraudulence, illegitimate replication and improves copyright assurance in the developing time of web and computerized advancements. The succeeding are the necessities of watermarking: I) Imperceptibility – When the original image and the modified image cannot be distinguished, the watermark is called imperceptible whereas a watermark is termed perceptible if its occurrence in the modified image is detectable, (II) Robustness – If the watermark endures any practical processing imposed on the carrier, it is called robust. A watermark is termed delicate if it fails to be discovered after the least alteration, (III) Security - The watermarked image must not disclose evidences of the existence of the watermark at all, with respect to an illegal recognition [1].

Various techniques were projected for multimedia security. Amongst the projected methods, many gave their focus on digital pictures. As per the area in which the watermark is embedded, these techniques are categorized as: spatial-domain and frequency-domain. Although the implementation becomes easy and the complexity reduces when the watermark is embedded in the spatial-domain component of a cover picture [2] but it becomes more vulnerable to image processing methods. Whereas, the frequency-domain methods insert the watermark by balancing the size of coefficients in a transform domain, such as DCT, DFT, and DWT [3,4,5,6,7]. For encrypting the watermark, ECC is growing as a main cryptography, and shows an ability to be a substitute of RSA. Its size being small and security being high characterizes it. ECC is appropriate in the environments where processing power, storage, bandwidth or power ingestion is controlled [8].

Barni et al. [9] introduced watermarking plan in light of wavelet space. In this plan all picture sub-groups are changed taking into account the surface and luminance content. This method demonstrates great power to picture preparing operations yet not well for geometric assaults. Mohammad-Reza et al. [10] suggested a picture watermarking in wavelet space. In the proposed watermarking plan, rather than altering the particular values, the U segment to be specific the left solitary vector is investigated and changed under various edge values. The projected plan [11] exploits attributes of human visual framework prototype for choosing pieces of a picture for implanting watermark. To choose the watermark installing blocks, entropies are calculated that is used in [12] to fulfill the principle prerequisite of watermarking calculation. Subsequent to calculating the entropies of every piece, both of them are summed and the squares are organized in climbing request. Number of chosen squares is equivalent to extent of the watermark. The plan projected in this paper is intangible and vigorous against a few image preparing processes. Calculation of the performance is done by matching the proposed work in [11] and [13].

The paper is prepared in following sequence:

In Section II, Encryption technique (ECC) and DWT-SVD is described. Section III describes the projected encryption, embedding and extraction algorithm. In Section IV, the experimental outcomes, algorithm contrast and results are examined and finally in Section V, conclusion is determined.

## II. LITERATURE REVIEW

### *A. ENCRYPTION- Elliptic Curve Cryptography*

Elliptic Curve Cryptography (ECC) is likewise called as open key cryptography, where every client or the gadget taking an interest in the correspondence generally have a few keys, an open key and a private key, and an arrangement of operations related with the keys to do the cryptographic operations. Little key size is the fundamental point of interest of ECC. The operations of elliptic bend cryptography are characterized more than two limited fields: Prime field and Binary field [8]. The suitable field is chosen with limitedly immense number of focuses for cryptographic operations. Here, we have utilized

978-1-5090-1489-7/16/$31.00 ©2016 IEEE

prime field operations by picking a prime number N, and unendingly substantial quantities of base focuses are produced on the elliptic curve, such that the created focuses are between 0 to N. At that point, we haphazardly select one base point $P_i(x, y)$ for cryptographic operations and this point fulfils the mathematical statement of the elliptic bend on a prime field, which is characterized as

$$Y^2 = x^3+ax+b \bmod N \qquad (1)$$

In equation 1, (a, b) are the coefficients that define the curve, and x and y are the coordinate values of the generated point P.

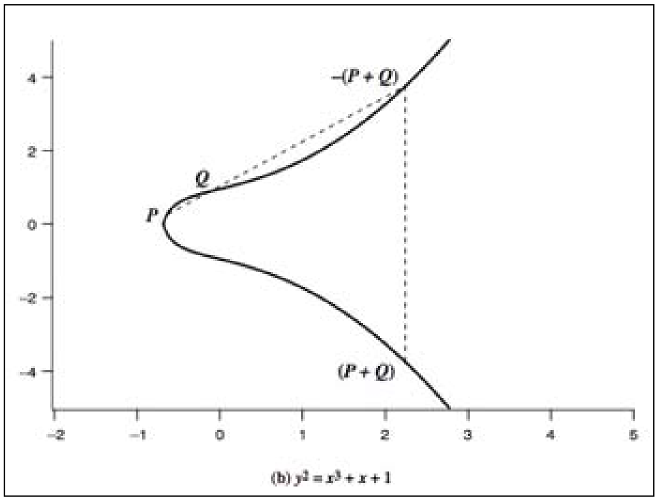
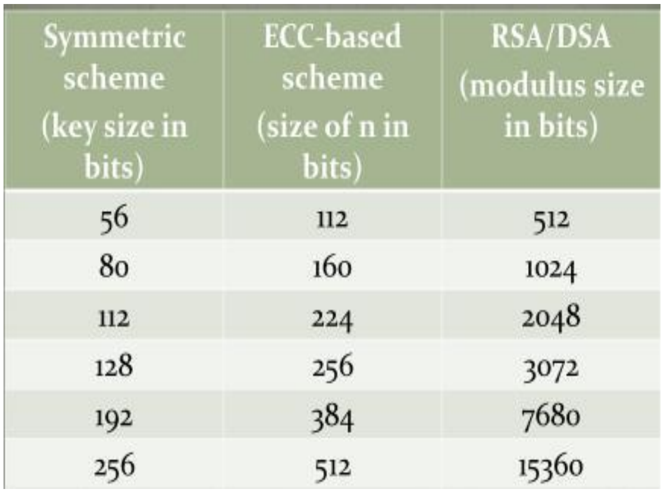


**Fig. 1. Real Elliptic Curve**

**Table 1. Comparable Key Sizes**



| Symmetric scheme (key size in bits) | ECC-based scheme (size of n in bits) | RSA/DSA (modulus size in bits) |
|---|---|---|
| 56 | 112 | 512 |
| 80 | 160 | 1024 |
| 112 | 224 | 2048 |
| 128 | 256 | 3072 |
| 192 | 384 | 7680 |
| 256 | 512 | 15360 |

## III. TECHNIQUES USED

Here, the spatio recurrence restriction based DWT and a mathematical procedure generally connected to observe the sign preparing practices like computerized watermarking, face acknowledgement, fingerprinting and so on to be specific [5-9] SVD is presented.

### *B.1. Discrete Wavelet Transform (DWT)*

The essential thought of wavelet hypothesis was specified by Gabor in 1945. The fundamental weakness of Fourier change is that it doesn't give any data in regards to time restriction of segments. Wavelets empower us to disintegrate the picture in both spatial furthermore, fleeting areas. 2-D wavelet changes can be shown using

2-D scaling capacity Φ(x,y) and three 2-D wavelets

$\Psi^H(x,y), \Psi^V(x,y), \Psi^D(x,y)$ capacity. The discrete wavelet change of a picture f(x,y) of size M×N is given by:

$$W_{\emptyset}(j_0,m,n) = \frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\emptyset_{j0,m,n}(x,y) \qquad (2)$$

$$W_{\varphi}^{i}(j,m,n) = \frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\varphi_{j,m,n}^{i}(x,y) \qquad (3)$$

Where i = {H,V,D} and j0 is a random scale.

WΦ(j0,m,n) defines the low frequency coefficients of f(x,y) at the scale j0 and WiΨ(j,m,n) defines the horizontal, vertical and the diagonal details for the scale j ≥ j0.

With the assistance of DWT, a picture can be deteriorated into 4 groups to be specific low recurrence band and 3 high recurrence band along diverse headings. The low recurrence band contains normal data and most extreme vitality of the picture, while the high recurrence groups contains the subtle elements of the picture. [14]

### ***B.2. Singular Value Decomposition(SVD)***

SVD is a huge method in direct variable based math to break down the matrices and has been connected to numerous picture preparing practices like Image compression [2], face acknowledgement [3], image improvement [3], watermarking [5-9] and so on. SVD divides a matrix of size M×N into 3 different matrices, U, S and V separately, such that:

$$[U\ S\ V] = \mathrm{svd}\ (A) \qquad (4)$$

Where the size of U is M×M and the size of V is N×N and both are unitary and orthogonal matrices and S is an orthogonal matrix of size M×M. So,

$U=[u_1, u_2, \ldots\ldots, u_r, u_{r+1}, \ldots\ldots., u_m]$

are the column vectors forming an orthonormal set i.e.

$$u_i^t\ u_j = \begin{cases} 1 & \text{if i=j} \\ 0 & \text{otherwise} \end{cases} \quad for\ i = 1,2,\ldots\ldots\ldots, m \qquad (5)$$

Similarly, V is an orthogonal matrix so,

$V=[v_1, v_2, \ldots\ldots v_r, v_{r+1}, \ldots\ldots, v_n]$ are the column vectors forming an orthonormal set i.e.

$$v_i^t\ v_j = \begin{cases} 1 & \text{if i=j} \\ 0 & \text{otherwise} \end{cases} \quad for\ i = 1,2,\ldots\ldots\ldots, n \qquad (6)$$

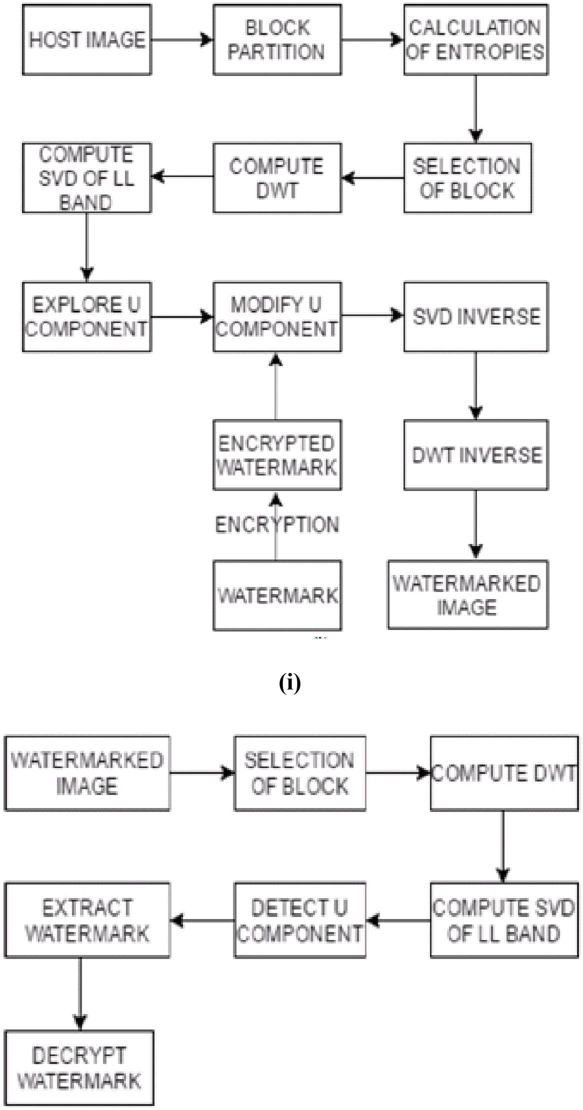
## IV. PROPOSED TECHNIQUE

1. Encryption

Here, an ECC centered encryption technique is used to encrypt the watermark. In the proposed encryption algorithm, the watermark is a binary image of size 32 * 32.

2. Watermarking

Here, a DWT-SVD centered watermarking plan is used that explores U part acquired in the wake of captivating the SVD of low frequency band under various threshold standards. Fig. 2 explains step wise procedure on how the embedment and extraction is done of the watermark. In this scheme, cover image is a gray scale image of size 512*512 and watermark is 32*32 bit binary image.



**(i)**

**(ii)**

**Fig. 2. Flow Chart of proposed Watermarking Scheme. (i) Embedding of Watermark (ii) Extraction of Watermark**

The embedment of algorithms involves the following steps:

### *A. Embedment of Watermark*

1) The cover image is distributed into 4*4 blocks which are not overlapped.

2) We calculate the values of visual entropy and edge entropy for each block and arrange them in ascending order so as to choose the correct number of blocks which is equal to the number of watermarked bits.

3) First level DWT is performed to the chosen blocks of cover image so as to get 4 bands, first being approximate band sA, second the horizontal component sH, third the vertical component sV and the last one diagonal component sD.

4) The band with low frequency, sA is taken and SVD is applied on it so as to break the sA into 3 components which are U, S and V i.e.

$$sA' = U' * S * V' \qquad (7)$$

5) Now, we insert binary image watermark in chosen coefficients of the 1st column of the U element as per the equation:

If watermark=1 bit, then

$$U'(1,1)= - \left| |U(1,1)| + (Th - \frac{Diff}{2}) \right| \qquad (8)$$

$$U'(2,1)= - \left| |U(2,1)| - (Th - \frac{Diff}{2}) \right| \qquad (9)$$

If watermark=0 bit, then

$$U'(1,1)= - \left| |U(1,1)| - (Th - \frac{Diff}{2}) \right| \qquad (10)$$

$$U'(2,1)= - \left| |U(2,1)| + (Th - \frac{Diff}{2}) \right| \qquad (11)$$

Where, Th stands for threshold value,

Difference = $| U(1,1) - U(2,1) |$ and U' is the watermarked element.

6) We perform inverse SVD on separate block which is used for inserting the watermark bit so as to get the low frequency watermarked band i.e.

$$sA' = U'*S*V' \qquad (12)$$

Where sA' is the approximate watermarked band.

7) We perform inverse DWT so as to get the watermarked image.

8) For calculating the brilliance and imperceptibility of the watermarked image we compute the value of PSNR between watermarked image and cover image.

### *B.) Extraction of Watermark*

1) Watermarked image is distributed into 8*8 blocks which are non-overlapping in nature.
2) Correct no. of blocks used in implanting procedure are selected based on the human system.
3) First level DWT is applied to individually chosen block of watermarked image so as to get f approximate band sA', horizontal component sH', vertical component sV' and the last diagonal component sD'.
4) Low frequency sub-band, sA' is taken and SVD is applied on it so as to break the sA' into 3 components U', S', V' i.e.

$$[U'S'V'] = \text{svd}\ (\text{sA}') \qquad (13)$$

5) For the extraction of watermark bits, first and second coefficient of the first column of U’ are studied.

If ( │ U(1,1) - U(2,1) │) > 0
Watermark = 1 bit
Else
Watermark = 0 bit.

6) Using these watermarked bits thus got in step 5 we form a vector which is then transformed into a matrix so as to get a watermarked image.

## V. EXPERIMENTAL RESULTS

Various trials are done to assess the execution of the projected watermarking calculation on distinctive compositions of dim scale pictures of size $512\times512$ like Lena, extension, pepper, plane, goldhill utilizing Matlab stage. The consequences of three gray scale cover pictures goldhill, lena and pepper appeared in Fig. 3 are exhibited and an examination is done to demonstrate the relevance of projected plan with the plan projected in [11] and [13]. The binary image of size $32\times 32$ to be specific AU is appeared in Fig. 4 is utilized as a watermark as a part of our experiment. The watermark image is then encrypted before embedding it into the host image to get the best results. The encrypted watermark image is shown in Fig. 5.

(i) (ii)

(iii)

**Fig. 3. (i) Host image (Goldhill), (ii) Lena (iii) Pepper**

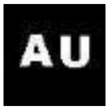


**Fig. 4. Watermark image of 32×32 b its**

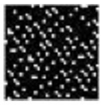


**Fig. 5. Encrypted Watermark image**

**The quality of watermark image is evaluated by PSNR which is well-defined by the equation:**

$$\boldsymbol{PSNR = 10log_{10}\,255/MSE\,(db)} \qquad \textbf{(14)}$$

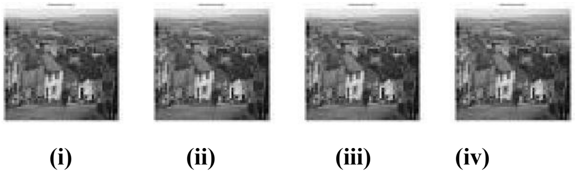
Normalized Correlation is calculated so as to compare the recovered watermark and the original watermark

**NC is given by:**

NC= corr2(Watermarked image, Original image) (15)

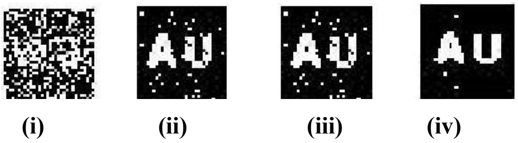
Fig. 5, 7 and 9 depicts the watermarked images of goldhill, lena and pepper at the various thresholds i.e.

**Th = {0.002, 0.012, 0.02 and 0.04}**



**(i) (ii) (iii) (iv)**

**Fig. 6. Watermarked goldhill images at (i) Th = 0.002 (ii) Th = 0.012 (iii) Th = 0.02 (iv) Th = 0.04**

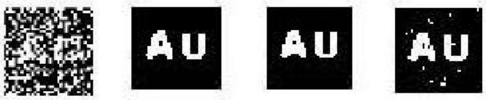


**(i) (ii) (iii) (iv)**

**Fig. 7. goldhill.jpg: Watermark Extraction at (i) Th = 0.002 (ii) Th = 0.012 (iii) Th = 0.02 (iv ) Th= 0.04**

**(i) (ii) (iii) (iv)**

**Fig. 8. Watermarked lena images at. (i) Th = 0.002 (ii) Th = 0.012 (iii) Th = 0.02 (iv) Th = 0.04**

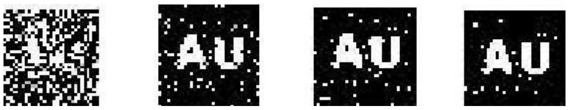


**(i) (ii) (iii) (iv)**

**Fig. 9. lena.jpg: Watermark Ext raction at (i) Th = 0.002 (ii) Th = 0.012 (iii) Th = 0.02 (iv) Th = 0.04**

**(i) (ii) (iii) (iv)**

**Fig. 10. Watermarked pepper images at (i) Th = 0.002 (ii) Th = 0.012 (iii) Th = 0.02 (iv) Th = 0.04**



**(i) (ii) (iii) (iv)**

**Fig. 11. Pepper.jpg: Watermark Extract ion images at (i) Th = 0.002 (ii) Th = 0.012 (iii) Th = 0.02 (iv ) Th = 0.04**

Figure 6, 8 and 10 demonstrates that no optical excellence distinction exists between the cover picture and watermarked pictures at diverse thresholds. Here, at limit esteem Th=0.002 and Th=0.02, the modified image resembles the original one as measured by high PSNR esteem. At Th=0.012 and Th=0.04, an adequate twisting in the visual nature of watermarked picture is identified. From the distinctive sorts of coarse pictures utilized as a part of our investigation, we watch that after a specific breaking point of threshold value, the nature of watermarked picture is misshaped. Table II demonstrates indistinctness of watermark embedded in the pictures appeared in fig. 6, 8 and 10. It is tough to differentiate between the host and the watermarked image when the PSNR value is high.

**TABLE II: Performance Comparision of PSNR (DB) Watermarked Lena Image Before Attacks at Various Threshold Values and Technique Projected in [11] and [13]**

| Threshold values | Chih-ChinLai [11] ('Lena.jpg') | Rajesh Mehta[13] ('Lena.jpg') | Ours |
|---|---|---|---|
| 0.002 | 61.69 | 62.0861 | 68.7505 |
| 0.012 | 49.37 | 52.2112 | 57.7010 |
| 0.02 | 44.75 | 47.9580 | 53.4209 |
| 0.04 | 38.51 | 42.0212 | 47.4723 |
| Average | 48.58 | 51.0691 | 56.8361 |

**TABLE III: Performance Comparison of PSNR (DB) Watermarked Pepper Image before Attacks at Various Threshold Values and Technique Projected in [11] and [13]**

| Threshold values | Chih-Chin Lai [11] ('Pepper.jpg') | Rajesh Mehta[13] ('Peppers.jpg) | Ours |
|---|---|---|---|
| 0.002 | 56.20 | 60.0818 | 67.6331 |
| 0.012 | 50.20 | 52.1603 | 58.1501 |
| 0.02 | 45.73 | 48.2494 | 53.9740 |
| 0.04 | 39.61 | 42.4164 | 48.0732 |
| Average | 47.94 | 50.7270 | 56.9576 |

**TABLE IV. Performance Comparision of PSNR (DB) Watermarked Goldhill Image before Attacks at Various Threshold Values and Technique Projected in [11] and [13]**

| Threshold values | Chih-Chin Lai [11] ('Goldhill.jpg') | Rajesh Mehta{13] ('Goldhill.jpg) | Ours |
|---|---|---|---|
| 0.002 | NA | NA | 62.5262 |
| 0.012 | NA | NA | 54.7038 |
| 0.02 | NA | NA | 50.8407 |
| 0.04 | NA | NA | 45.1625 |
| Average | NA | NA | 53.3083 |

The proposed watermarking scheme has turned out to be very robust as certified by carrying out various image handling processes on the modified image and then the watermark is extracted from the images after attacks. Various image processing operations like median filtering, JPEG compression, cropping and addition of guassian noise were applied on the watermarked Lena, Goldhill and Pepper under various thresholds Th = 0.012 and Th = 0.04.

**TABLE V: NC after various atta ks at Th = 0.012**

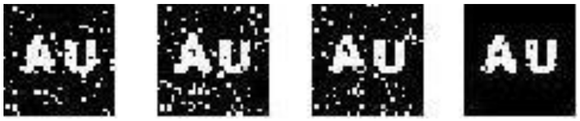
| Attacks | NC (lena.bmp) | NC (pepper.bmp) | NC (goldhill.jpg) |
|---|---|---|---|
| White | 0.9565 | 0.7600 | 0.8387 |
| Noise | | | |
| Gaussian | 0.9413 | 0.7024 | 0.7160 |
| Noise | | | |
| JPEG | 0.7850 | 0.7591 | 0.7141 |
| Cropping | 0.9119 | 0.9635 | 0.7612 |
| Average | 0.8986 | 0.7962 | 0.7575 |

**TABLE VI: NC after various attacks at Th = 0.04**

| Attacks | NC (lena.jpg) | NC (pepper.jpg) | NC (goldhill.jpg) |
|---|---|---|---|
| White | 1 | 0.8918 | 0.9867 |
| Noise | | | |
| Gaussian | 0.9654 | 0.8325 | 0.9365 |
| Noise | | | |
| JPEG | 0.9955 | 0.9288 | 0.9437 |
| Cropping | 0.9119 | 0.9635 | 0.7612 |
| Average | 0.9682 | 0.9041 | 0.9070 |

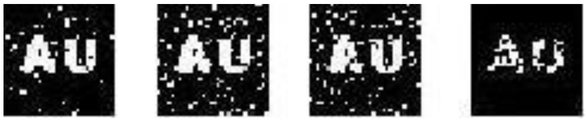
**(i) (ii) (iii) (iv)**

**Fig. 12 For lena image: At Th=0.012, extracted watermarks after various attacks (i) White Noise (ii) Gaussian Noise (iii) JPEG Compression (iv) Cropping**



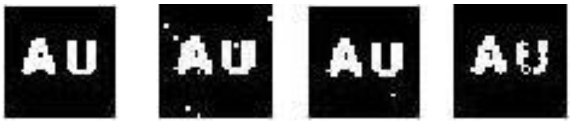
**(i) (ii) (iii) (iv)**

**Fig. 13. For pepper image: At Th=0.012, extracted watermarks after various attacks (i) White No ise (ii) Gaussian Noise (iii) JPEG Co mpression (iv) Cropping**



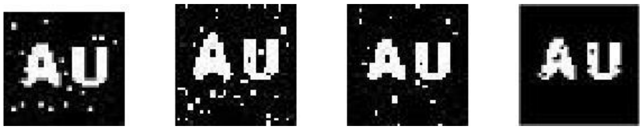
**(i) (ii) (iii) (iv)**

**Fig. 14. For goldhill image: At Th=0.012, extracted watermarks after various attacks (i) White No ise (ii) Gaussian Noise (iii) JPEG Co mpression (iv) Cropping**



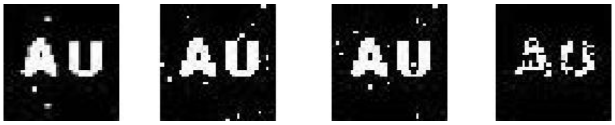
**(i) (ii) (iii) (iv)**

**Fig. 15. For pepper image: At Th=0.04, ext racted watermarks after various attacks (i) White No ise (ii) Gaussian Noise (iii) JPEG Co mpression (iv) Cropping**



**(i) (ii) (iii) (iv)**

**Fig. 16. For pepper image: At Th=0.04, ext racted watermarks after various attacks (i) White No ise (ii) Gaussian Noise (iii) JPEG Co mpression (iv) Cropping**



**(i) (ii) (iii) (iv)**

**Fig. 17. For goldhill image: At Th=0.04, ext racted watermarks after various attacks (i) White No ise (ii) Gaussian Noise (iii) JPEG Co mpression (iv) Cropping**

## VI. ALGORITHM CONTRAST

Here we have compared the schemes projected by Chih-Chin Lai [11] in 2011 and Rajesh Mehta, Navin Rajpal [13] in 2013 with our projected watermarking scheme. Table II shows that the PSNR computed by projected watermarking technique at distinct threshold standards is superior to [11] and [13]. Greater the PSNR, greater is the indistinctness of inserted watermark and better is the nature of the watermarked picture.

## VII.CONCLUSION

An image watermarking calculation taking into account ECC, DWT and SVD is displayed. The optical trademark of human beings is utilized to choose the apt implanting image blocks and the similar blocks are utilized as a part of extracting procedure. The proposed plan encrypts the watermark which is to be embedded and then misuses the components of DWT to remove the low recurrence band. More prominent PSNR value at various thresholds illustrates that the nature of the watermarked image picture is better. Strength of the proposed watermarking scheme can also be seen as jpeg images are used which compressed images, hence lossy in nature are. But, using the proposed scheme, we can see that the results which we got are better than the results got in earlier schemes in which bmp images were used which are binary images. Strength of the projected calculation is confirmed by the abstraction of watermark against picture handling processes like Gaussian noise, jpeg compression, white noise and cropping. To demonstrate the predominance, the projected plan is contrasted with the plan in [11] and [13].

## REFERENCES

[1] R.Dhanalakshmi and K.Thaiyalnayaki "Dual Watermarking Scheme with Encryption", (IJCSIS) International Journal of Computer Science and Information Security,pp. 248-253, Vol. 7, No. 1, 2010

[2] I.J. Co x., J. Kilian, F.T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for Multimedia," IEEE Transactions on Image Processing, pp. 1673 - 1687, Vol. 6, Issue 12, 1997

[3] H.C. Andrews and C.L. Patterson, "Singular value decomposition and digital image processing, "IEEE Trans. On Acoustics, Speech and Signal Processing, vol. ASSP-24, no. 1, pp. 26-53, 1976.

[4] X.Y. Wang, Pan-Pan Niu, H.Y. Yang, "A robust content based image watermarking using local invariant histogram," Multimedia Tools Appl., Vol. 54, pp. 341-363, 2011.

[5] B.Y. Lei, I.Y.Soon and Zhen Li, "Blind and robust audio watermarking scheme based on SVD-DCT," Signal Processing vol. 91, 1973-1984, 2011.

[6] X.Y. Wang and H. Zhao, "A novel synchronization invariant audio watermarking scheme based on DWT and DCT," IEEE Trans. On Signal Processing vol. 12, no. 54, pp. 4835-4840, 2006.

[7] Hongqing Zhu, Min Lu and Yu Li, "The RST invariant digital ima ge watermarking using radon transform and complex moments," Digital signal Processing vol. 20, pp. 1612-1628, 2010.

[8] Saeid Bakhtiari, Subariah Ibrahim, Mazleena Salleh, Majid Bakhtiari "JPEG Image Encryption with Elliptic Curve Cryptography" International Symposium on Biometrics and Security Technologies (ISBAST), pp. 144 - 149, 2014

[9] M. barni, F. Bartolini and A. Piva, "Improved wavelet based watermarking through pixel wise masking," IEEE Trans. on Image Processing, vol. 10, pp. 783-791, 2001.

[10] Mohmmad-Reza and F.M. Bayat, "Robust dynamic block based image watermarking in DWT domain," Procedia computer science, vol. 3, pp. 238-242, 2011.

[11] Chih-Chinlai, "An improved SVD based watermarking scheme using human visual characteristics," Optics Communications vol. 284, iisue 4, pp. 938–944, 2011

[12] Vivekanand Bhatt K., I. Senagupta and A. Das, "An adaptive audio watermarking based on singular value decomposition in wavelet domain," Digital signal Processing vol. 20, pp. 1547-158, 2010.

[13] Rajesh Mehta and Navin Rajpal "A Hybrid Semi -Blind Gray Scale Image Watermarking Algorithm Based on DWT-SVD using Human Visual System Model", pp. Pages: 163 – 168, 2013

[14] S.G.Mallat, "A theory of mult iresolution signal decomposition: the wavelet representation," IEEE Trans. On Pattern Analysis and Machine Intelligence vol. 11, no. 7, pp. 674-693, 1989.