# PSNR VALUE OF DIGITAL IMAGE WATERMARKING BY USING SINGULAR VALUE DECOMPOSITION-DISCRETE COSINE TRANSFORMATION

**Vikas Chaubey[1], Chetan Kumar[2]**

*[1]MTech. Scholar, [2]Associate Professor, Dept of Computer Science & Engineering, KITE, Jaipur, Rajsthan, India*
***vikash.0213@gmail.com, chetanmnit@yahoo.in***

## Abstract

*Digital Watermarking technique is now day needs to provide more robust for any image and also safe from many type of attack. Because every day by day need of multimedia techniques improve so another hand also creating of duplication problem. In this paper literature survey many techniques discuss year by year using for solving this problem. But according to my survey hybrid digital image watermarking using of Singular Value Decomposition and Discrete Cosine Transformation algorithm is best .by using of this hybrid digital watermarking possible to harmless our image from many type of attack and less PSNR value when you return back image same position. We are also calculating the value of Correlational Coefficient on different step size step.*

***Keywords:*** *Peak Signal noise ratio, Watermarking, Attacks, Singular Value Decomposition, Discrete Cosine Transformation.*

----------***----------

## 1. INTRODUCTION

Day by day it has been seen a quick growth of network multimedia systems. This has led to an growing awareness of how easy it is becoming to repeat the data. The ease with which perfect copies can be made may lead to large-scale unauthorized copying, which is a great concern to the image, music, film, and book. A digital data can be easily transmitted, received, duplicated or modified by using the Internet. The copyright protection of digital data is an important legal issue [1]. There are various processes are used for copyright protection of digital data. The Digital watermarking is new and most common technique for copyright protection and considered as a possible solution. Watermarking is very similar to steganography in a number of respects. Both pursue to embed information inside a cover message with little to no degradation of the cover-object. Watermarking techniques can be classified according to the type of watermark presence used, i.e., Watermark may be a visually recognizable logo or a sequence of random numbers. Another organization is based on the domain which the watermark is applied.

## 2. LITERATURE SURVEY:

### 2.1 ATTACKS ON DIGITAL WAVELET IMAGE WATERMARKS:

In 2008 Andreja Sam covic, Jan Turan, Introduced many method come in plan for hiding copyright character and many other information in digital images. Watermarking is a power schemes for protection of ownership right on digital image. If any processing that harm detection of the communication of the material transported by the watermark is in watermarking technology called an attack. Some attacks are tried on a watermarking based on wavelets. Actually there is business similar the photography, music and video industry that can't accepts this principle since they skill basic content and therefore have to stick with old-style copyright enforcement to guarantee income. as we know now days audio, video and other mechanism become present in digital form, may be ease with perfect copies can be made will lead to big-scale unofficial copying which will undermine the music, film, book and software publishing industries. The fast growth of digital technology makes the development of reliable and robust technology for protecting digital static picture, audio and video from piracy a urgently difficulty.

Piracy attacks include illegal access to transmitted data in networks, data content modification, manufacture and retransmission of prohibited copies. The effect of such attacks strength be very big in financial and term of security [2].

We are first discuss two aims or purpose for an attack against a watermark image: first Hostile or Malicious attacks, is an attempt to weaken, remove or adjust the watermark and second Coincidental attacks, which can happen throughout common image processing and not target at altering with the watermark. The harsh term attack can be easily justified: an

efficient image compression has to overpower perceptually unrelated material- the invisible watermark. A wide-ranging of attacks has been designated in the literature [4]. Four type of attacks can be invoked to enter a watermarking system: Removal attacks, Geometrical attacks, Cryptographic attacks and Protocol attacks. The attack is positive if the watermarking can't be finding anymore, but the image is still understandable and can be used for specific determined purpose. And many such attack actions have proposed Lossyimage compression, Addition of Gaussian noise, De-noising Filtering, Median filtering and blurring, Signal enhancement

### 2.1.1 ADDITIVE WATERMARKINGWAVELET ALGORITHM

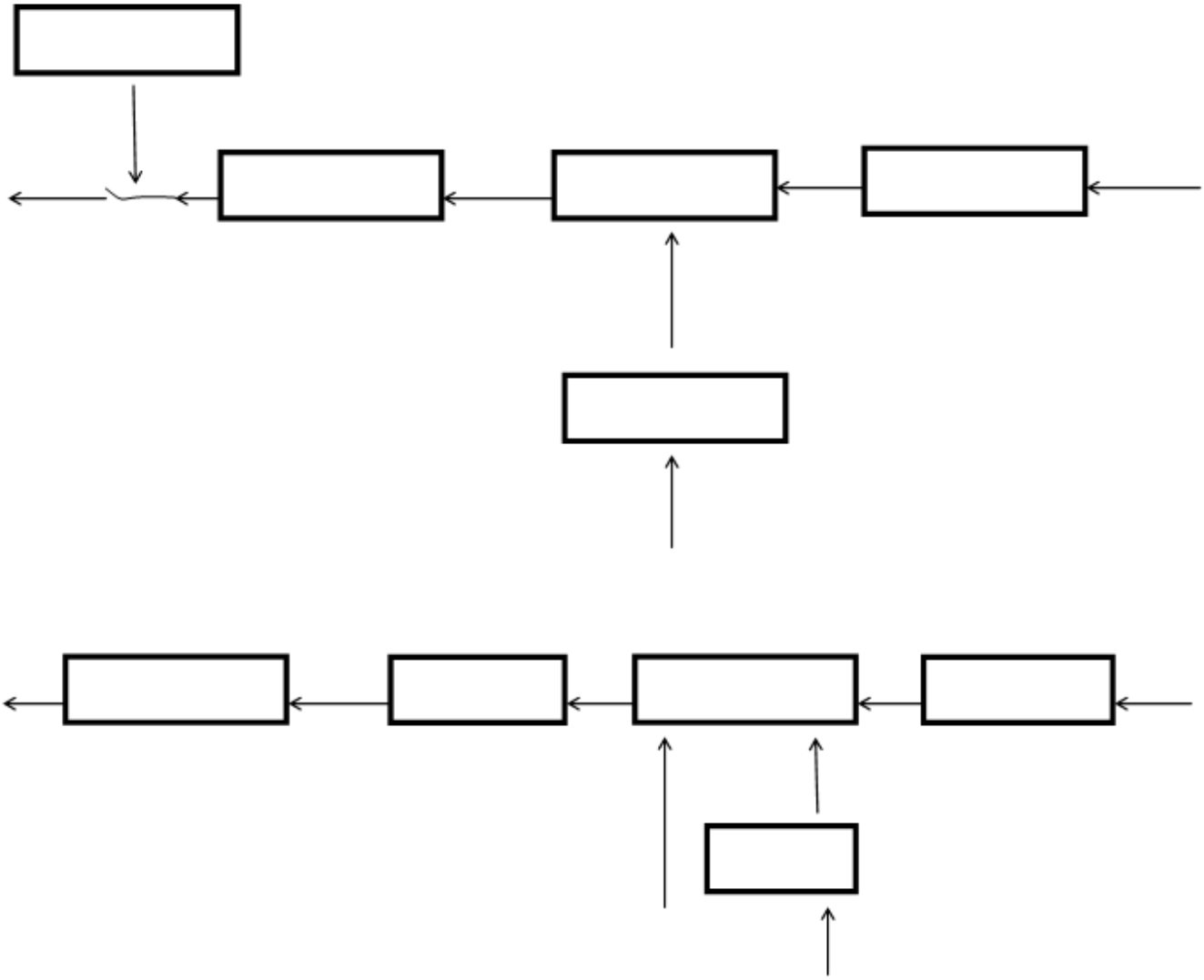


**Fig1:** Embedded System of Block diagram

The watermarking is using into two method watermarking embedding and watermarking extraction. At the opening of embedding procedure a bipolar arrangement of bits is transformed into a new arrangement w(1), . . .,w(L) by swapping -1 by 0, where L is the length of the arrangement and w(k) 2 {1, -1} (k =1, . . . ,L). The new arrangement is used as the watermark. The original image I is decomposed into two levels of the DWT decomposition [3]. The decomposition is completed using the Haar wavelet filters. The watermark is added to L major coefficients in all of the complete sub bands (HLi, LHi, HHi ,i = 1, 2) of the DWT decomposition. HL1 ,LH1 , and HH1 signify the high frequency ranges, while HL2 , LH2 , and HH2 signify the middle frequency ranges of the image processed. Let f(m, n) denote the set of L largest DWT coefficients at the position (m, n) in any of sub band matrices

(HLi , LHi ,HHi , i = 1, 2). The embedding procedure is completed according to the following formula:

F′(m, n) = F(m, n) + alfa · F(m, n)w(k) , k = 1, . . . ,L where alfa is the strength of the watermark controlling the level of the watermark f′(m, n) is modified coefficient at the position (m, n) in any of sub band matrices.

The watermarked image Iw is gotten by applying the inverse DWT (IDWT). The position vectors of altered coefficients in all sub bands are kept in secret and used in extraction procedure as a secret key. The upper part of Fig. 1 shows the block-diagram of the embedding procedure. The lower part of the Fig. 1 represents the finding procedure. In the watermark extraction procedure (see lower part of the Fig. 1) both the received image Ir and the original image I are decomposed into levels of the DWT decomposition. By this the received image Ir is possibly modified by attacks. It is assumed that the original image I is existing in the extraction procedure, ie that is used as an input to this procedure. When images are decomposed using the DWT the positions of the reformed coefficients in the sub bands of the original and received images are considered according to the secret key generated in the embedding procedure [6]. This set of selected DWT coefficients will be represented with f(m, n) and fr(m, n), respectively. The position (m, n) signifies the particular position in the sub band. The extraction procedure is described by the following formula:

Wr(k) = Fr(m, n) − F(m, n)__alfa · F(m, n)_ where wr is the extracted watermark.

The extracted watermark is further transformed as follows:
We(k) = SignWr(k)_ After extraction of the watermark we the bit stream is reconstructed by similar trading as at the beginning (0 is replaced by -1).

### 2.2. Robustness Of The Digital Image Watermarking Techniques Against Brightness And Rotational Attack:

In 2009 Harsh K Verma, AbhishekNarain Singh, Raman Kumar, Introduced in the area of multimedia propose a many services in transport, transmission and manipulation of data. Day by day increasing of technology there are many problem in authentication of data, no one want to use licensed and protection against illegal use of data. Many type of technology have been designed and implementation for stop the unlawful use of data. In this technique compare the robustness of three different watermarking systems against rotation attacks. The robustness of the watermarked image has been verified on the parameters of Peak Signal to Noise Ratio.

#### 2.2.1 Watermark Embedding And Extraction:

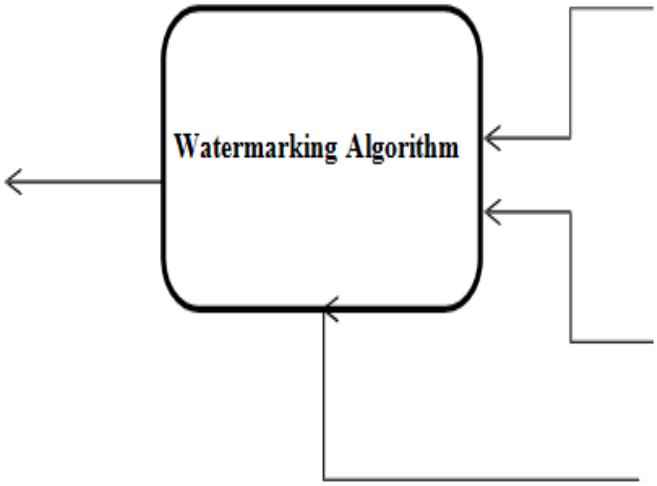



Fig1:WatermarkedEmbeddedProcess

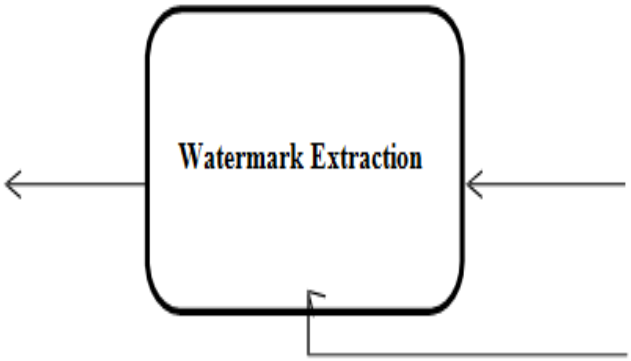



**Fig2:**WatermarkedExtractionProcess

### 2.2.2 Watermarking Techniques:

Spatial Domain, Frequency Domain and Wavelet Domain [6] these three types of watermarking techniques have been chosen for the experiment.

### 2.2.2.1 CDMA Spread Spectrum Watermarking in Spatial Domain

The algorithm of the above method is given below:

### A. To embed the watermark:

a. Convert the original image in vectors.
b. Set the gain factor k for embedding.
c. Read in the watermark message and reshape it into a vector.
d. For each value of the watermark, a PN sequence is generated using an independent seed.
e. Scatter each of the bits randomly throughout the cover image.
f. When watermark contains a '0', add PN sequence with gain k to cover image.

i. if watermark(bit) = 0 .
watermarked_image=watermarked_image + k*pn_sequence.
ii. Else if watermark (bit) = 1.
watermarked_image=watermarked_image + pn_sequence.

g. Process the same step for complete watermark vector.

### B. To recover the watermark:

a. Convert back the watermarked image to vectors.
b. Each seed is used to generate its PN sequence.
c. Each sequence is then correlated with the entire image. i. If ( the correlation is high)
That bit in the watermark is set to "1"
ii. Else
That bit in the watermark is set to "0" .
d. Process the same step for complete watermarked vector.
e. Reshape the watermark vector and display recovered watermark.

### 2.3 Digital image watermarking using dwtand svd:

In 2010 Chih-Chin Lai, Member, IEEE, and Cheng-Chih Tsai Introduced in area of developing a Digital Image Watermarking method is to fulfill noiselessness and robustness requirements. The watermark is not embedded directly on the wavelet coefficients but rather than on the origins of singular values of the cover image's Discrete Wavelet Transformation sub bands. The proposed approach is able to stand a variety of image-processing attacks. The domain in which is using these method are distributed into two type first one is spatial-domain and second one is transform-domain. Spatial-domain component of the original image is straightforward techniques. The spatial-domain methods are generally breakable to image processing operations or other attacks. and another one transform-domain method embed the watermark by modulating the magnitude of coefficients in a transform domain, such as DCT,DWT and SVD[7][8]. Transformation-domain techniques can produce more information embedding and robustness against many common attacks, the computational cost higher the Spatial-domain watermarking methods.

### Proposed DWT-SVD Watermarking Scheme:

The proposed DWT-SVD watermarking scheme is formulated as given here.

### A) Watermark embedding:

1) Use one-level Haar DWT to decompose the cover image A into four sub bands (i.e., LL, LH, HL, and HH).
2) Apply SVD to LH and HL sub-bands, i.e., Ak= UkSk V kT, k= 1, 2 (1) where k represents one of two sub-bands.
3) Divide the watermark into two parts: W = W1 +W2, where Wkdenotes half of the watermark.
4) Modify the singular values in HL and LH subbands with half of the watermark image and then apply SVD to them, respectively, i.e., Sk+ αWk= UkWSkW V kT W
Where α denotes the scale factor. The scale factor is used to control the strength of the watermark to be inserted.
5) Obtain the two sets of modified DWT coefficients, i.e., A∗k= UkSkW V kT, k= 1, 2.
6) Obtain the watermarked image AW by performing the inverse DWT using two sets of modified DWT coefficients and two sets of non-modified DWT coefficients.

### B) Watermark extraction:

1) Use one-level Haar DWT to decompose the watermarked (possibly distorted)
Image A∗W into four sub-bands: LL, LH, HL, and HH.
2) Apply SVD to the LH and HL sub-bands, i.e.,
A∗k W = U∗kS∗k W V ∗kT, k= 1, 2.
Where k represents one of two sub-bands
3) Compute D∗k= UkWS∗k W V kTW ,k = 1, 2.
4) Extract half of the watermark image from each subband, i.e.,
W∗k= (D∗k − Sk)/α, k = 1, 2.)
5) Combine the results of Step 4 to obtain the embedded watermark: W∗= W∗1 +W∗2.

### 2.4 Digital Watermarking Algorithm Based On Singular value Decomposition And Arnold Transformation:

In 2012 DivyaSaxena, Introduced in area of watermarking process is use for hiding undisclosed information for labeling of digital image. We are using the embedding and extracting which is based on SVD and Arnold transformation. The embedded position is selected according to the secret key which is obtained during the course of the scrambling degree

calculation in Arnold transform. The experimental results show the proposed method has high Peak Signal Noise Ratio and NC results under general image processing. And Arnold transform method of results is useful for digital image processing.

### 2.4.1 ARNOLD TRANSFORM:

To confirm the security and improve the robustness of the proposed watermarking scheme, the watermark should be pre-processed before embedded into the original image. Due to the periodicity process of the Arnold transform, the image can be easily recovered after the permutation concept. So, the Arnold transform is applied to the original image watermark.

Let us consider the size of original image is N*N, (i, j)T and it's coordinate of the watermark image's pixel.(i',j')T and these coordinate are gained after transform. Arnold transform can be expressed as

$$\begin{matrix} i' \\ j' \end{matrix} = \begin{matrix} 1 & 1 \\ 1 & 2 \end{matrix} \begin{matrix} i \\ j \end{matrix} \text{ (mod N)}$$

Where i,j €{ 0,1,…N-1} and

$$W = \begin{matrix} 1 & 1i \\ 1 & 2j \end{matrix} \text{ is input, } \begin{matrix} i' \\ j' \end{matrix} \text{ is output.}$$

### 4.1.2 PROPOSED ALGORITHM:

### A. Watermark Embedded Algorithm:

1) Step-1 Divided the original image, which has embedded watermark, in to the sub block 256*256 .
2) Step-2 after that apply SVD process to each sub band in original image (Ai,j )

$$Ai,j = Ui,j * Si,j * VT\ i,j$$

3) Step-3 Then apply the Arnold transform on watermark image (W) and change the watermark image to the Arnold scrambling.
4) Step-4 Add the watermark W into the matrix S, and perform SVD on the new matrix:

$$Si,j = Si,j * @Wi,j$$

Where
Si,j :represent the Watermarked SVD coefficients.
Si,j : represent the original image SVD coefficients.
@: represent an intensity parameter of image watermark.
Wi,j: represent the Arnold scrambling coefficients of the watermark image .
5) Step-5 in this step Obtain the watermarked image Aw by multiplying the matrices. After that Arnold transform, convert Ui,j and Vij into one-dimensional sequence respectively to compose the embedding watermark W. S i,j is kept as the secret key.

$$Awi,j = Ui,j * S\ i,j * V^T\ i,j$$

### B. Watermark Extraction Algorithm:

1) Step-1 First of all divided the Watermarked image in to the sub block 256*256 .
2) Step-2 Then apply SVD process to each sub band in watermarked image (Awi,j)

$$A^w i,j = Ui,j * S\ i,j * V^T i,j$$

3) Step- 3 After that extract the Singular values from each sub band:

$$S^w i,j = (Sij) - Sij/@$$

4) Step- 4 Construct the coefficient of the subband by using singular vectors $S^w i,j$ and vectors (Uw,j ,Vw,j)computed at the time of embedding process:

$$Aw,j = (Uw,j * Swi,j * Vw,j)$$

5) Step-5 Processing Aw,j with Arnold transform and get the extracted of watermark image.

### 2.5 HYBRID DIGITAL IMAGE WATERMARKING USING SINGULAR VALUE DECOMPOSITION-DISCRETE COSINE TRANSFORMATION:

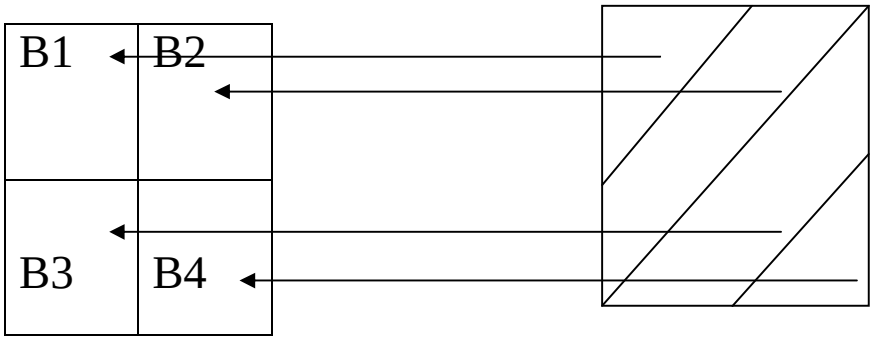
Now its propose method There has been times when any watermarking schemes has a traditional algorithm like decomposing the image with a transform, then encrypting the watermark and then with their embedding algorithm, embed the information. Some schemes were found implementing variations in any available traditional algorithm to achieve robustness and imperceptibility criterion and this gave the idea of using hybrid schemes.

Hybrid watermarking schemes can be described as the schemes which are aimed to minimize the tradeoff between imperceptibility and robustness of watermark by cleverly picking the appropriate transform from the wealth of transforms, previously illustrated ideas, some variations or innovative advancements in them and then finally mixing them in right way to have a good degree of compatibility. To finally have a scheme that has taken the best possible use of available innovations and is capable of showing desired robustness and imperceptibility parameters.

### 2.5.1 An Example Is Discrete Cosine Transformation-Singular Value Decomposition Domain Digital Image Watermarking:

The process of separating the image into bands using the DWT is well-defined. In two-dimensional DWT, each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL sub-band can further be decomposed to obtain another level of decomposition. In two-dimensional DCT, we apply the transformation to the whole image but need to map the frequency coefficients from the lowest to the highest in a zig-zag order to 4 quadrants in order to apply SVD to each block. All the quadrants will have the

same number of DCT coefficients. For example, if the cover image is 256x256, the number of DCT coefficients in each block will be 65,536. To differentiate these blocks from the DWT bands, we will label them B1, B2, B3, B4. This process is depicted in Fig shown below.




In pure DCT-based watermarking, the DCT coefficients are modified to embed the watermark data. Because of the conflict between robustness and transparency, the modification is usually made in middle frequencies, avoiding the lowest and highest bands.

In SVD-based watermarking, several approaches are possible. A common approach is to apply SVD to the whole cover image, and modify all the singular values to embed the watermark data. An important property of SVD-based watermarking is that the largest of the modified singular values change very little for most types of attacks.

We will combine DCT and SVD to develop a new hybrid non-blind image watermarking scheme [28] that is resistant to a variety of attacks. The proposed scheme is given by the following algorithm. Assume the size of visual watermark is nxn, and the size of the cover image is 2nx2n.

### A) Watermark Embedding:

1. Apply the DCT to the whole cover image *A*.
2. Using the zig-zag sequence, map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4.
3. Apply SVD to each quadrant: $A^k = U_A^k \Sigma_A^k V_A^{kT}$, $k$ = 1,2,3,4, where *k* denotes B1,B2,B3 and B4
4. Apply DCT to the whole visual watermark *W*.
5. Apply SVD to the DCT-transformed visual watermark *W*: $W = U_W \Sigma_W V_W^T$.
6. Modify the singular values in each Quadrant $B^k$, $k$ = 1,2,3,4, with the singular values of the DCT-transformed visual watermark: $\lambda_i^{*k} = \lambda_i^k + \alpha_k * \lambda_{wi}\ i = 1 \dots \dots n$Where $\lambda_i^k\ i = 1 \dots \dots n$ are Thesingular values of $\Sigma_A^k$, and$\lambda_{wi} i = 1 \dots \dots n$are the singular valuesof $\Sigma_V$.
7. Obtain the 4 sets of modified DCT coefficients:

$$A^{*k} = U_A^k \Sigma_A^{*k} V_A^{kT}, \qquad k = 1,2,3,4.$$

8. Map the modified DCT coefficients back to their original positions.
9. Apply the inverse DCT to produce the watermarked cover image.

### B) Watermark Extraction:

1. Apply the DCT to the whole watermarked (and possibly attacked) cover image $A^*$.
2. Using the zig-zag sequence, map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4.
3. Apply SVD to each quadrant: $A^{*k} = U_A^k \Sigma_A^{*k} V_A^{kT}$, $k$ = 1,2,3,4.where *k* denotes the attacked quadrants.
4. Extract the singular values from each quadrant $Bk, k$ = 1,2,3,4: $\lambda_{wi}^k = \frac{\lambda_i^{*k} - \lambda_i^k}{\alpha_k}, i = 1, \dots . n$
5. Construct the DCT coefficients of the four visual watermarks using the singular vectors:

$$W^k = U_W^k \Sigma_W^k V_W^k, k = 1,2,3,4.$$

6. Apply the inverse DCT to each set to construct the four visual watermarks.

The DCT coefficients with the highest magnitudes are found in quadrant B1, and those with the lowest magnitudes are found in quadrant B4. Correspondingly, the singular values with the highest values are in quadrant B1, and the singular values with the lowest values are in quadrant B4.

The largest singular values in quadrants B2, B3, and B4 have the same order of magnitude. So, instead of assigning a different scaling factor for each quadrant, we used only two values: One value for B1, and a smaller value for the other three quadrants

### 2.5.2 ADVANTAGE AS SEEN IN THE DESCRIBED HYBRID ALGORITHM:

A comparison of the hybrid DCT-SVD watermarking scheme with a pure SVD based algorithm shows that the proposed scheme performs much better, providing more robustness and reliability

In most DCT-based watermarking schemes, the lowest frequency coefficients are not modified as it is argued that watermark transparency would be lost. In the DCT-SVD based approach, we experienced no problem in modifying the coefficients in quadrant B1.

Watermarks inserted in the lowest frequencies (B1) are resistant to one group of attacks, and watermarks embedded in highest frequencies (B4) are resistant to another group of attacks. The only exception is the rotation attack for which the data embedded in middle frequencies survives better. With different angles, the results may be different. If the same watermark is embedded in four quadrants, it would be extremely difficult to remove or destroy the watermark from all frequencies. So as we have seen the advantages that lead from implementing a hybrid watermarking scheme, we can be pretty sure that thinking in right direction and mixing the available techniques with innovation can result in fairly appreciable and noticeable outcome.

## CONCLUSION AND FUTURE SCOPE

In this paper discuss many latest technologies for improving robust and safe from many geometrical attacks. When any one try for attack than extract the watermarking and find the Peak Signal Noise Ratio value is greater than. The value of after using of Singular Value Decomposition and Discrete Cosine transformation algorithm Peak Signal Noise Ratio is less. by implementation of these two algorithms performing the results on geometrical attacks. And future scope of this technology we are performing many attacks Dither, Gaussian Noise and Average filtering. We are improving the multimedia in digital image, audio, video many digital media in current time use day by day creating of demand of digital technology.

## REFERENCES

[1] R.J. Anderson, and F. Petitcolas,―On the Limits of Steganography‖ , IEEE Journal of Selected Areas in Communications, vol 16, Issue 4, pp 474 – 481, 1998.

[2] -PETITCOLAS, F.—ANDERSON, R.—KUHN, M. : Attacks on Copyright Marking Systems, in Lecture Notes on Computer Science, pp. 218–238, April 1998.

[3] BOJKOVI´C, Z.—SAMˇCOVI´C, A. : XXXVII International Sci-entific Conference on Information, Communication and Energy Systems and Technologies ICEST 2002, Vol. 1, pp. 131–134, Niˇs,Yugoslavia, 1–4 October 2002.

[4] PLA, O.—LIN, E.—DELP, E. : A Wavelet Watermarking Algorithm based on a Tree Structure, in Security, Steganography,and Watermarking of Multimedia Contents, pp. 571–580, 2004.

[5] BARNI, M.—BARTOLINI, F. : Improved Wavelet-Based Watermarking Through Pixel-Wise Masking, IEEE Trans. Image Processing 10 No. 5 (May 2001), 783–791.

[6] CorinaNafornita, "A Wavelet-Based Watermarking for Still Images", Scientific Bulletin of Politehnica University of Timisoara, Trans. on Electronics and Telecommunications, 49(63), special number dedicated to the Proc. of Symposium of Electronics and Telecommunications ETc, Timisoara, pp. 126-131, 22 - 23 October 2004.

[7] R. Liu and T. Tan, “An SVD-based watermarking scheme for protecting rightful ownership,” *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128,Mar. 2002.

[8] A. Nikolaidis and I. Pitas, “Asymptotically optimal detection for additive watermarking in the DCT and DWT domains,” *IEEE Trans. Image Process.*, vol. 12, no. 5, pp. 563–571, May 2003.

[9] F. Hartung , and M. Kutter,―Multimedia Watermarking Techniques‖, Proc. IEEE, vol 87, no.7, pp 1079-1107,1999.