# Real Time Hybrid Digital Watermarking Based On Key Dependent Basis Function

**Anjietha Khanna**

Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology
Jaipur-302020, India

***Abstract –*** In this paper, hybrid approach is introduced where a process known as 'watermark' is enabled to mark digital pictures with undetectable secrete information that are invisible by using principal component analysis and discrete wavelet transform to provide a complete copyright protection system. The concept of key dependent basis function and its application is introduced to secure robust watermarking for copyright protection and to design a secure public black-box watermark detectors which shows high imperceptibility and performance where no noticeable difference is seen between watermarked and original image. Thereby, it overcomes a possible security weakness of non-adaptive as well as global schemes that execute watermark patterns with a small number of publicly known basis function. Projection of image is embedded within the watermark onto the secret set of key dependent basis function i.e. patterns. Conclusively, we proposed a candidate for a watermarking scheme that enables the construction of secure public watermark detector.

***Index Terms –*** Digital watermarking, Discrete Wavelet Transform, Principal Component Analysis, Key Dependent Basis Function

## I. INTRODUCTION

The reproduction, manipulation and the distribution of digital multimedia (images, audio and video) via networks becomes faster and easier as the proprietors and creators of the digital products are aware of illegal copying of their products. Therefore, security and copyright protections are important issues pertaining to multimedia applications and services [1].

Earlier, the watermarking techniques were proposed for these aforesaid purposes in which the copyright information was embedded into multimedia data for protecting the ownership. Consequently, research is now being focused on watermarking schemes to protect multimedia information. The most suitable technology that can serve this purpose is none other than digital watermarking. Multifarious watermarking schemes have been proposed to camouflage copyright marks and other information in digital applications.

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Computer techniques can easily manipulate and store the digital data efficiently and with a high quality. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. A watermarking is adding 'ownership' information in multimedia contents to prove the authenticity along with embedding a data which is an unperceivable digital code, namely the watermark that carries information about the copyright status of the work to be protected while continuous efforts are being made to device an efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations. The abrupt increase in the interest of watermarking is most likely due to the increase in concern over IPR. Basically, the watermarking of videos, still image and audio demonstrate certain common fundamental concepts. Thus, watermarking techniques may be relevant in numerous areas which may include copy protection, copyright protection, fingerprinting and temper detection et-al [1][2][3]. The manner in which information is embedded, watermarking schemes can be classified either as spatial domain (the watermarking system directly changes the main data elements, wiz pixels in an image to hide the watermark data) or transformed domain (the watermarking system alters the frequency transforms of data elements to hide the watermark data). The last technique has proved to be more robust than the spatial domain watermarking [4].

Several reversible transforms are used to transfer an image to its frequency representation like discrete cosine transform (DCT), discrete wavelet transform (DWT) or discrete fourier transform (DFT). Even though spatial domain based techniques cannot sustain most of the common attacks like compression, low pass or high pass filtering et al, researchers present spatial domain technique too [4].

Since monetary impact of some of the application areas are very high and till now no successful algorithm seems to be available to prevent illegal copying of the multimedia contents. The ultimate goal of this paper work is chosen to develop watermarking schemes for images which can sustain the known attacks and various image manipulation operations. This paper is designed to overcome the following issues:

**Issue 1**- Till now there is no 'Generic' nature in the watermarking algorithms available. More precisely, if certain approach is applicable for a gray level image, the same approach does not work for the other formats of an image.

**Issue 2**- Even if gray color image watermarking algorithms are extended for RGB color images, the maximum work has been done for (y-luminance) color channel only because human eyes are less sensitive to detect the changes in (y-luminance) color channel. Attack impact free analysis, i.e., which color channel may be affected by a particular attack, has been carried out [6][7]. Therefore, apart from choosing digital image watermarking as a major problem, we have chosen to identify the suitability of a color channel with respect to attack for multicolor channel images. We also decided to explore the ways such that attack impacts may be minimized before the watermark embedding process.

**Issue 3**- Predominantly in research papers, once the watermarking scheme is acknowledged, it is applied to all test images. As each image is different and has its peculiar characteristics and after embedding the watermark data by a particular watermarking scheme, its performance against a particular attack may not be similar with other image. No study is conducted to make the embedding scheme based on some image characteristics. Therefore, we have resolved to establish the relationship between the performance of watermarking scheme and the color image characteristics.

**Issue 4**- Mostly watermarking schemes are developed in a way that first a scheme is developed based on the extension of earlier presented one and then check its performance against the common image manipulations and known attacks. There are huge financial implications of watermarking schemes, but no scheme has been developed, which is by design, resistant to at least one attack, to ensure that, a particular attack cannot be conducted by an attacker. Therefore, we decided to design watermarking schemes such that inherent nature can be embedded to guarantee that at least one serious attack having most financial implication cannot be conducted on watermarked images.

The paper has been organized as following sections: section II discuss about the proposed work, section III presents the experimental results and section IV draws the conclusion and future work.

## II. PROPOSED WORK

The proposed approach towards the scheme of hybrid digital watermarking is based on discrete wavelet transform and principal component analysis.

### A. Discrete Wavelet Transform

Discrete wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible. There is a significant high time differentiated rate in high frequency parts of signals. Also there is match able good frequency differentiated rate in its low frequency part. It can filter the information from signal significantly. The concept of DWT in image processing is to multi-differentiate and decompose the image into sub image of different spatial domain and independent frequency district [5][6] and then transform the coefficient of sub-image.

After the original image has been DWT transformed, it is fragmented into 4 frequency districts namely one low frequency district (LL) and three high frequency districts (LL, HL, HH). The sub-level frequency district information can be obtained by transforming the information of low frequency district through DWT. A two dimensional image after three times DWT decomposed can be shown as Fig. 1, low-pass filter is represented by 'L' and 'H' represents high-pass filter. A decomposed original image can be obtained of frequency districts of LL1, HL1, LH1, HH1 and sub-level frequency district information of LL2, HL2, LH2, HH2 can also be obtained by decomposing low frequency district information i.e. LL1. And thus 'n' level of original images can be obtained by wavelet transformation.

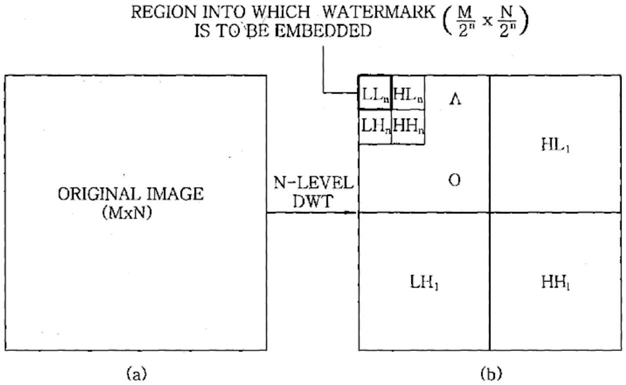

REGION INTO WHICH WATERMARK IS TO BE EMBEDDED $\left(\frac{M}{2^n} \times \frac{N}{2^n}\right)$
ORIGINAL IMAGE (MxN)
N-LEVEL DWT
$LL_n$
$HL_n$
$LH_n$
$HH_n$
A
O
$HL_1$
$LH_1$
$HH_1$
(a)
(b)

Fig.1 Fragmentation of LL sub-band to 'n' non overlapping sub-blocks each of dimension n x n using n-level DWT

### B. Principal Component Analysis

Principal component analysis is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of uncorrelated variables called principal components (major components) which can be achieved by eigenvalue decomposition of a data covariance matrix or singular value decomposition of a data matrix for each attribute[8].It is desired that the number of principal components is less than or equal to the number of original variables. PCA is a method of recognizing patterns in data and expressing the data in a manner so as to highlight their similarities and differences. As it is hard to find patterns in data of high dimension where the merits of graphical representation are not available, the PCA is therefore a powerful tool for data analysis. The next major advantage of PCA is that once these patterns in the data have been identified, the compression of data by reducing the number of dimensions, without much loss of information can be done. The PCA thus plots the data into a new coordinate system where the data with maximum covariance are plotted together and is known as first principal component. Similarly, there are second and third principal component and so on. The maximum energy concentration lies in the first principal component. The PCA does not have a fixed set of basis function but it has basis functions which depend on the data set which is not there in other linear transformation. The key ingredient is the combined data set normally distributed, therefore guaranteed to be independent. The method is mostly used as a tool in exploratory data analysis and for making predictive models.

### *C. Algorithm And Block Diagram For Embedding And Extracting Watermark*

The block diagram to represent the algorithm for embedding and extracting the watermark using DWT and PCA is shown in Fig. 2.

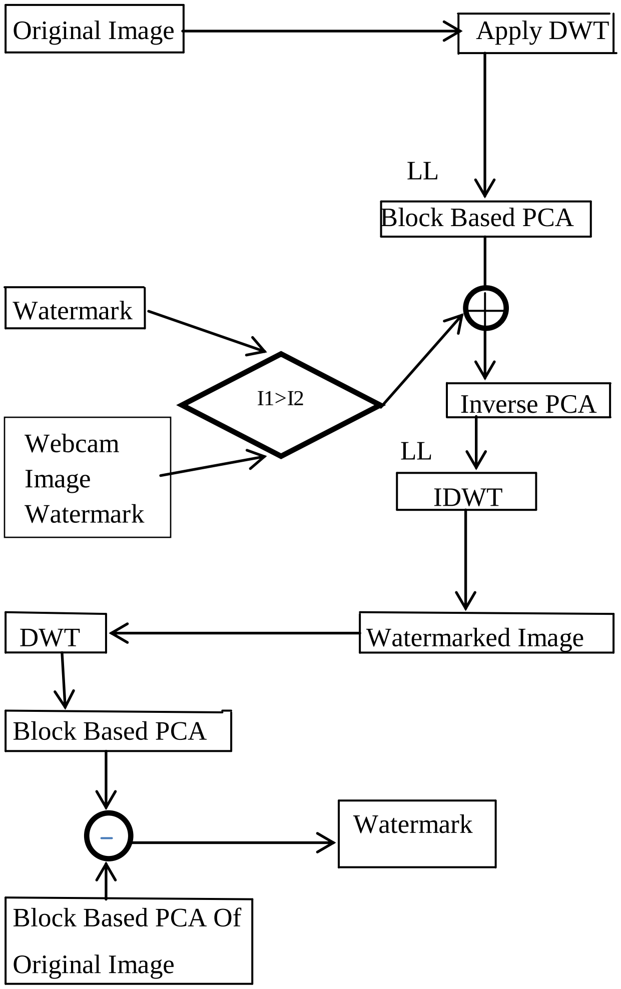


Fig. 2 Block Diagram Of Watermarking

Algorithm 1:

1) Embedding Procedure

Step 1: Click a picture through a webcam known as webcam image watermark.

Step 2: Calculate the intensities of watermark image and webcam image watermark.

Step 3: Whose so ever intensity is greater will be embedded in the original image.

Step 4: Convert the n × n binary watermark logo into a vector W = { w1, w2 , ……, wn × n } of '0's and '1's.

Step 5: Transform image from RGB to YUV color format.

Step 6: Apply 1-level DWT to the luminance (Y component) of image to obtain four sub-bands LL, LH, HL and HH of size N x N.

Step 7: Fragment the LL sub-band into k non-overlapping sub-blocks each of dimension n × n (of the same size as the watermark logo).

Step 8: Algorithm 2 is used for embedding with strength α into each sub-block by first obtaining the principal component scores for watermark bits. The general form for embedding is carried out as equation.

$$Score_i = Score_{i\,+}\, \alpha\, W \qquad (1)$$

Where $Score_i$ represents the principal component matrix of the ith sub-block.

Step 9:Obtain inverse PCA is applied on the modified PCA components of the sub-blocks of the LL sub-band to obtain the modified wavelet coefficients.

Step10:Apply inverse DWT to obtain the watermarked luminance component of the image. Then convert the image back to its RGB components.

2) Extraction Procedure

Step 1: Divide the watermarked (and possibly attacked) image into distinct frames and convert them from RGB to YUV format.

Step 2: Choose the luminance (Y) component of a image and apply the DWT to decompose the Y component into the four sub-bands LL, HL, LH, and HH of size N×N.

Step 3: Divide the LL sub-band into n × n non overlapping sub-blocks.

Step 4: Put PCA to each block in the chosen sub-band LL by using Algorithm 2.

Step 5: Provided from the LL sub-band, the watermark bits are extracted from the principal components of each sub-block as in equation 2.

$$W_i' = \frac{(Score_i' - Score_i)}{\alpha} \qquad (2)$$

Where $W_i$' is the watermark extracted from the ith sub-block.

**Algorithm 2:**

The LL sub-band coefficients are transformed into a new coordinate set by calculating the principal components of each sub-block (size n x n).

Step 1: Each sub-block is converted into a row vector $D_i$ with n2 elements (i=1, 2… k).

Step 2: Compute the mean $\mu_i$ and standard deviation $\sigma_i$ of the elements of vector $D_i$ .

Step 3: Compute $Z_i$ according to the following equation

$$Z_i = \frac{(D_i - \mu_I)}{\sigma_i} \qquad (3)$$

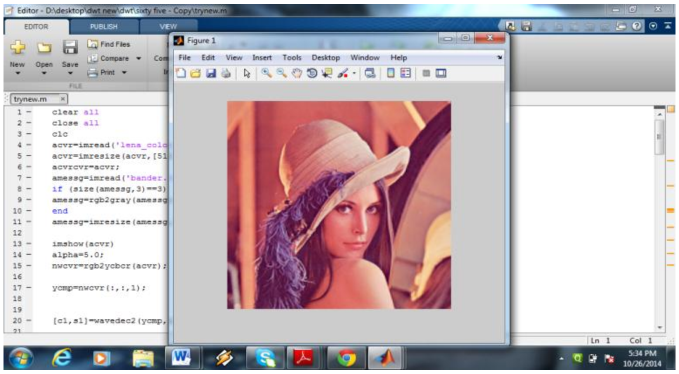
Here $Z_i$ represents a centered, scaled version of $D_i$, of the same size as that of $D_i$.
Step 4: Apply principal component analysis on $Z_i$ (size 1 x n2) to obtain the principal component coefficient matrix coeffi (size n2 × n2).
Step 5: Calculate vector $Score_i$ as

$$Score_i = Z_i \text{ X } Coeffi_i \qquad (4)$$

Where $Score_i$ represents the principal component scores of the ith sub-block.

## III. EXPERIMENTAL RESULTS

This proposed work is applied to an image 'lena_color_256.tif' using a watermark logo 'bander.tif' or webcam image watermark shown in fig. 5 depending on the intensities of watermark. The RGB watermark is converted to binary before embedding. Fig.3 shows the cover image and fig.4 shows the watermark logo and fig 5 shows the webcam acquisition image i.e.' watermark.jpg' which after embedding results into a fig.6 known as watermarked image i.e. named as watermarked_bander.bmp. Fig 7 shows us the actual extracted watermark. By ranging the value of key dependent basis function i.e. $\alpha$, the visibility of the watermark can be seen. Therefore, this algorithm device the whole range i.e. it achieves the target of both invisible and visible watermarking.



```
clear all
close all
clc
acvr=imread('lena_colo
acvr=imresize(acvr,[51
acvrcvr=acvr;
amessg=imread('bander.
if (size(amessg,3)==3)
amessg=rgb2gray(amessg
end
amessg=imresize(amessg

imshow(acvr)
alpha=5.0;
nwcvr=rgb2ycbcr(acvr);

ycmp=nwcvr(:,:,1);


[c1,s1]=wavedec2(ycmp,
```

Fig. 3 Cover Image 'lena_color_256.tif'

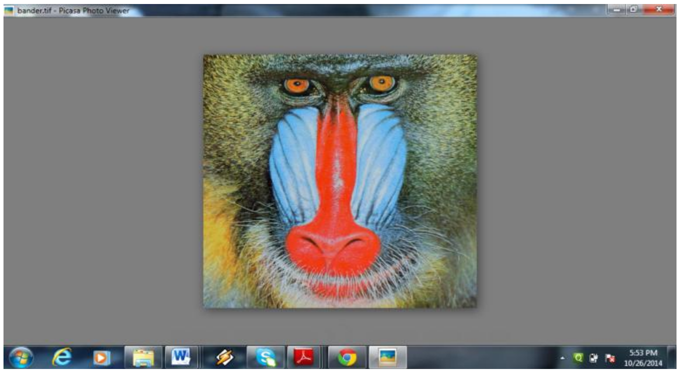
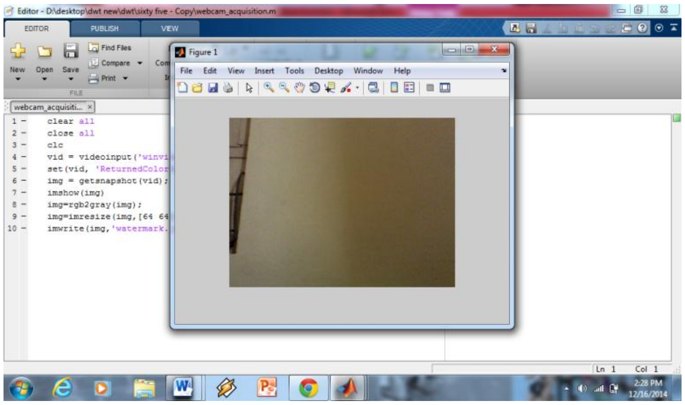
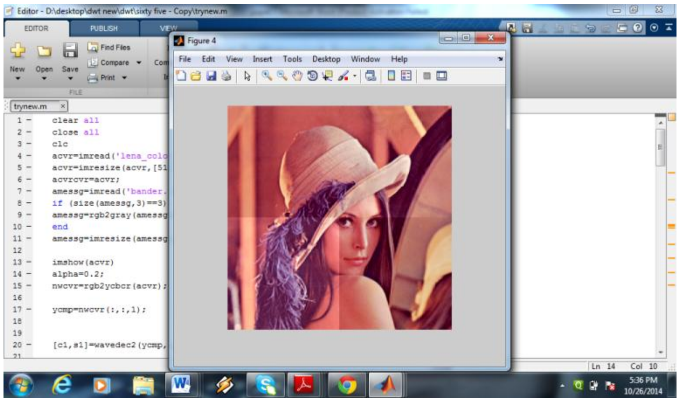


Fig. 4 Watermark logo 'bander.tif'



```
clear all
close all
clc
vid = videoinput('winvi
set(vid, 'ReturnedColor
img = getsnapshot(vid);
imshow(img)
img=rgb2gray(img);
img=imresize(img,[64 64
imwrite(img,'watermark.
```

Fig. 5 Webcam Image Watermark 'watermark.jpg'



```
clear all
close all
clc
acvr=imread('lena_colo
acvr=imresize(acvr,[51
acvrcvr=acvr;
amessg=imread('bander.
if (size(amessg,3)==3)
amessg=rgb2gray(amessg
end
amessg=imresize(amessg

imshow(acvr)
alpha=0.2;
nwcvr=rgb2ycbcr(acvr);

ycmp=nwcvr(:,:,1);


[c1,s1]=wavedec2(ycmp,
```

Fig. 6 Watermarked Image 'Watermarked_bander.bmp'

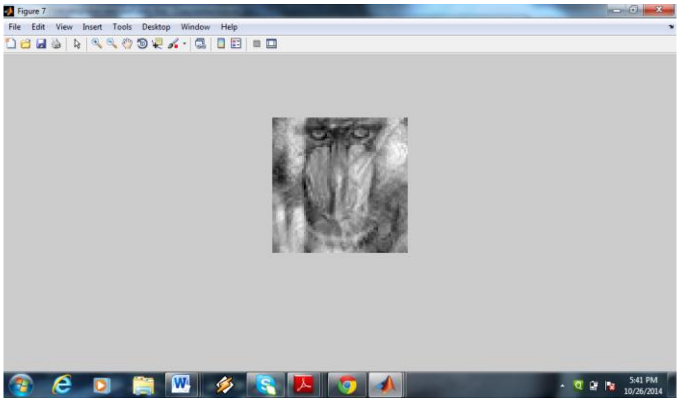


Fig.7 Extracted Watermark

The MSE (Mean Square Error) and NC (Normalized Coefficients) values are calculated for the watermarking procedure. And the criterion of good watermarking technique is, lower should be the MSE value and higher should be the NC value. MSE represent the similarity index of original image in comparison to watermarked image. While NC represent the index that shows the detrition or damage of extracted watermark when compared to original watermark which was used for hiding in the previous stage.

Resemblance is seen in watermarked image or attacked frame to cover i.e. original image. Better resemblance better will be the watermarking by using this approach in efficient way.

*1) PSNR* **-** The Peak Signal To Noise Ratio is used to compute deviation of the watermarked as well as attacked image from the original image and is denoted as :

$$\text{PSNR} = 10\ \text{Log}_{10}\,(255^2/\text{MSE}) \qquad (5)$$

measured in dB(decibel's) units. Where, MSE is found between the original and distorted image(mxn) as:

$$\text{MSE} = 1/(m*n)\sum\sum[I(i,j) - I'(i,j)]^2 \qquad (6)$$

The original and watermarked images are represented as I and I' respectively.

*2) NC* – The normalized coefficients gives a criteria and measure of the robustness of watermarking. NC can be formulated as

$$\text{NC}= \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)}\ \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W'(i,j)}} \qquad (7)$$

W and W' represent the original and extracted watermark respectively.

The forthcoming plot fig.7 represents the PSNR and NC curve with respect to $'\alpha'$ ranging from 1 to 10.

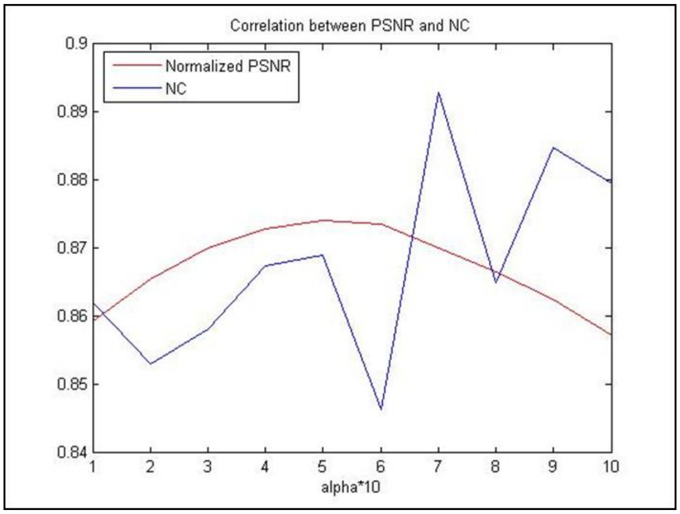


Fig. 7 Correlation between PSNR and NC wrt $\alpha$

## IV CONCLUSION AND FUTURE SCOPE

The watermarking algorithm using DWT and PCA has been devised as a whole range i.e. it is suitable for the invisible as well as visible watermarking by ranging the value of $\alpha$ from 1 to 10 respectively which is robust and shows high imperceptibility to the various attacks without much degradation in the image quality.

As a future work, the video frames can be subject to scene change analysis to embed an independent watermark in the sequence of frames constituting a scene and repeating these steps for all the scenes within a video itself. This process will go further to fight against electronic copyright infringement and illegal use.

## ACKNOWLEDGEMENT

This research paper is made possible through the help and support from everyone including teachers, parents and friends. I would like to thank Ms. Richa Rawal for her encouragement, support and advice.

## REFERENCES

[1]Yeo and M.M. Yeung"*Analysis and synthesis for new digital video, image applications*," icip, International Conference on Image Processing, vol 1, (ICIP'97), pp.1,1997.

[2]W.Bender, D.Gruhl, N.Morimoto, and A. Lu."*Techniques for data hiding*," IBM System Journal, Vol. 35.(3/4), 1996, pp. 313-336.

[3]M.Arnold,M.Schmucker, and S.D.Wolthusen,"*Techniques and application of Digital Watermarking and Content Protection*", Eds.Northwood ,Artech House, 2003.

[4] I.J.Cox, J.Kilian, T.Leighton and T.Shamoon, "*Secure Spread Spectrum watermarking for Multimedia*," IEEE Tras. on Image Processing , Vol. 6,No12, 1997, pp. 1673-1687.

[5] Potdar, Vidysagar and Han, Song and Chang, Elizabeth, "*A survey of digital image watermarking techniques*", Proceeding of 3rd IEEE-International Conference on Industrial Informatics, Frontier Technologies for the Future of Industry and Business, pp. 709-716, Perth, WA, Aug 10, 2005.

[6]F. Bossen M. Kutter, F. Jordan, "*Digital signature of color images using amplihlde modulation*," in Proc. of SPlE storage and retrieval for image and video databases, San lose, USA, vol. 3022-5, February 1997, pp. 518-526.

[7]M. Kutter and S. Winkler, "*A vision-based masking model for spread-spectrum image watermarking*," IEEE Trans. Image Processing, vol. 11, pp. 16-25, Jan. 2002.

[8]Hotelling,H. (1936). Relations between two sets of variates. Biometrika,27,321Abdi.H.,&Williams,L.J.(2010)."*Principal*

*component analysis*”. Wiley Interdisciplinary Reviews: Computational Statistics, 2: 433– 459 doi:10.1002/wics.101.

## AUTHORS

**First Author** – Anjietha Khanna, M.Tech, Rajasthan Technical University, anjiethakhanna@gmail.com.