

# Performance Analysis of Watermarking using Kronecker Product of Orthogonal Transforms and Wavelet Transforms

Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu

**Abstract—** This paper proposes a digital image watermarking of still images using self-kronecker product of orthogonal transforms and Singular Value Decomposition. Singular Value Decomposition is used due to its high stability and high image energy compaction in few numbers of singular values. Kronecker product of two transforms helps us to focus on only global features and not the local features of an image. In proposed method, both these transforms are kept same to generate the transform matrix. 256x256 transform matrix is generated using kronecker product of two 16x16 matrices. Sinusoidal transforms DCT, DST, Real Fourier Transform, Sinecossine transform and non-sinusoidal transforms Walsh, Haar, Discrete Kekre Transform (DKT) and Slant transform are explored to generate transform matrix using self kronecker product. Using self kronecker product improves the performance against compression attack by 27-83%, against noise addition attack, 25% to 100 % and for resizing attack self kronecker product improves the robustness over self-wavelet transforms by 34-100%. For histogram equalization performance improvement from 5 to 34% is observed.

**Index Terms—** Watermarking, Kronecker product, wavelet transform, Singular Value Decomposition, Real Fourier Transform, Sinecossine transform, Discrete Kekre Transform.

## 1 INTRODUCTION

Increased popularity of internet to exchange data has also increased the need to protect the data from illegal modifications and claiming. Hiding information of owner of data into it is the most popular way to avoid illegitimate alterations to data. By extracting the owner's information intact at the receiving end confirms the legal source of received data. This overall process of hiding owner's information secretly and verifying the legal alterations to received data is achieved by digital watermarking.

Watermarking can be applied to any digital contents like images, audio files, videos, text etc. for images, watermarking can be conducted by altering pixel intensity values to desirable extent such that existence of watermark is hidden. This is known as spatial domain watermarking. On the other hand, image can be first converted into its frequency components with suitable transform and then these frequency components can be suitably altered to hide the watermark. This is known as frequency or transform domain watermarking. Frequency domain watermarking helps to scatter the watermark information throughout the host image and makes its position in host difficult to detect. This makes it more robust than spatial domain watermarking where position of watermark in host belongs to certain locality.

In this paper a transform domain watermarking method is proposed. Transform matrix used here are generated by taking kronecker product of existing orthogonal transforms with themselves. Thus we name them as self kronecker product

transform. Robustness of proposed method is assessed against various attacks on watermarked images and also compared with the performance of wavelet transforms generated from the same orthogonal transforms. Singular Value Decomposition is used in both the cases to enhance the robustness.

Remaining paper is organized as follows: Section 2 gives an overview of available watermarking techniques in literature. Section 3 describes the proposed method. Section 4 presents the results of proposed method against attacks such as compression, cropping, noise addition, resizing and histogram equalization and also provides the comparison of self kronecker product transforms and wavelet transforms presented in [1]. Section 5 ends the paper with appropriate conclusions.

## 2 REVIEW OF LITERATURE

In literature exhaustive work has been done using transforms in watermarking field. DCT [2,3,4], DFT[5,6,7,8], Discrete Wavelet Transforms [9,10,11] are some frequently used transforms in watermarking of images. Combining two or more transforms is also a widely used trend in watermarking for improved robustness. Jiansheng, Sukang and Xiaomei proposed such DCT-DWT based invisible and robust watermarking scheme in which Discrete Cosine transformed watermark is inserted into three level wavelet transformed host image [12]. Surya Pratap Singh, Paresh Rawat, Sudhir Agrawal also proposed a DCT-DWT based watermarking technique in which scrambled watermark using Arnold transform is subjected to DCT and inserted into HH3 band of host image[13]. Yet another joint DCT-DWT based watermarking scheme [14] is proposed by Saeed K. Amirgholipour and Ahmad R. Naghsh-Nilchi. Another combined DWT-DCT based watermarking with low frequency watermarking and weighted correction is proposed by

- Dr. Tanuja Sarode is currently working as Associate Professor in computer engineering dept. at TSEC in Mumbai University, India  
E-mail: tanuja\_0123@yahoo.com
- Ms. Shachi Natu is currently pursuing Ph. D. program in computer engineering dept. at MPSTME in NMIMS University and working as Assistant Professor at TSEC in Mumbai University, India  
E-mail: shachi\_natu@yahoo.com

Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshui Hoque and Md. Iqbal Hasan Sarkar in [15]. In their proposed method, watermark bits are embedded in the low frequency band of each DCT block of selected DWT sub-band. The weighted correction is also used to improve the imperceptibility. In [16], Zhen Li, Kim-Hui Yap and Bai-Ying Lei proposed a DCT and SVD based watermarking scheme in which SVD is applied to cover image. By selecting first singular values macro block is formed on which DCT is applied. Watermark is embedded in high frequency band of SVD-DCT block by imposing particular relationship between some pseudo randomly selected pairs of the DCT coefficients. Some more watermarking methods using singular value decomposition (SVD) are proposed in [17, 18, 19]. Furthermore, it has been shown that SVD-based watermarking algorithms are very robust against a wide range of attacks. Xi-Ping and Qing-Sheng Zhu [20] have proposed a wavelet based method using sub-blocks of image. Instead of applying wavelet transform on whole image, it was applied to local sub-blocks. These sub-blocks were randomly extracted from original image. Watermark was embedded into part of frequency coefficients of these sub-bands by computing their statistical characteristics. A Mansouri, A Mahmoudi Aznaveh, F Torkamani Azar [21] have proposed a method using Complex Wavelet Transform (CWT) and singular value decomposition (SVD). The watermark was embedded by combining singular values of watermark in LL band of transformed image. The method proposed by them is non-blind watermarking because singular values of original image are required in extraction phase. Rashmi Agarwal and K. Venugopalan [22] have proposed a SVD based method for watermarking of color images. Each plane of color image is separately treated for embedding and extracting process. Different scaling factors were used to test the robustness of their method. Satyanarayana Murty. P. and P. Rajesh Kumar [23] have proposed a hybrid DWT-DCT-SVD based approach. HL frequency band was selected by them for embedding purpose. Method proposed in this paper is motivated by their work. Satendra Kumar, Ashwini Kumar Saini, Papendra Kumar [24] have also proposed a watermarking scheme based on discrete wavelet transform and singular value decomposition. They have used three level wavelet transform and then by modifying singular values of cover image, watermark is embedded into it. Medium frequency bands i.e. HL3 and LH3 were preferred for embedding. PSNR and Normalized Cross Correlation (NCC) values were used to measure the effectiveness of the method. Krishnamoorthi and Sheba Kezia [25] proposed a watermarking technique based on orthogonal polynomial based transformation for copyright protection of digital images. A visual model was used to determine strength of watermarking. This visual model was used to generate Just Noticeable Difference (JND) by analyzing low level image characteristics like texture, edges and luminance of cover image in polynomial based transformation domain. Ko-Ming-Chan and Long-Wen Chang [26] have proposed a watermarking system which embeds two different watermarks -robust and fragile into spatial and frequency domain separately. Robust watermark is embedded in wavelet coefficients of LL band whereas fragile watermark is

embedded in least significant bits of watermarked image. Advanced encryption standard- Rijndael block cipher was used to make watermarking technique public. Veysel Atlantas, A Latif Dogan, Serkan Ozturk [27] proposed a DWT-SVD based watermarking scheme using Particle Swarm Optimizer (PSO). Singular values of each sub-band of cover image are modified by different scaling factors. Modifications were further optimized using PSO to obtain highest possible robustness.

### 3 PROPOSED METHOD

In the proposed method a new transform is generated from existing orthogonal transforms by taking its kronecker product itself. The sinusoidal orthogonal transforms used to generate hybrid transform are DCT, DST, Real Fourier transform and sinecosine transform. Among non-sinusoidal transforms, Haar, Walsh, Discrete Kekre Transform (DKT) and Slant transform are used to generate hybrid transform.

After generating the above explained transform, it is applied to image columnwise and row wise separately. From column transformed image, middle frequency band is chosen for watermark embedding. This middle frequency band in case of column transformed image are nothing but some middle rows of host. In case of row transform, middle column correspond to middle frequency bands. Coefficients of this band are sorted based on their energy value. Watermark image is subjected to singular value decomposition and the singular value matrix corresponding to energy of image is obtained. By taking into account high energy compaction provided by SVD, it was found that only first 30 singular values pack almost 99.997% energy of image. Thus instead of embedding all 128 singular values, embedding only 30 values is preferred. To embed these 30 values, 30 middle frequency rows are selected. After testing many possible consecutive middle 30 rows, rows 101-130 in transformed host were found suitable. To bridge the difference between energy values of middle frequency band and energy packed in first 30 singular values, these singular values are adaptively scaled. Scaling factor is obtained from first singular value and first transform coefficient of middle frequency of host. Scaled singular values are placed such that first two singular values are placed at the place of first two highest coefficients of middle frequency band and then remaining values are placed consecutively. Inverse transform taken after replacing host coefficients by singular values of watermark gives watermarked image. Similar procedure is applied to row-wise transformation. The only difference is instead of middle rows, middle columns 101-130 are selected for embedding watermark.

While recovering watermark, first column/row self kronecker transform is applied on watermarked image. Middle frequency region is extracted. From this region we need to extract singular values of watermark in order to reconstruct it. Thus by using the index of sorted coefficients singular values are extracted. These singular values are scaled up by using the same scaling factor which was derived in embedding process. Inverse SVD is applied to scaled up singular value to get the watermark. Quality of recovered watermark perceived by Human Visual System is measured to

determine the robustness of proposed method. Therefore, Mean Absolute Error (MAE) between embedded and extracted watermark is computed. Smaller MAE means better robustness. MAE is average of absolute difference between pixels of an image.

The proposed method is performed on 5 host images a

watermark embedded in them. Average MAE between embedded and extracted watermark over 5 host images is computed for each attack.

Fig. 1 below shows the set of 5 host images and watermark image used for experimentation.

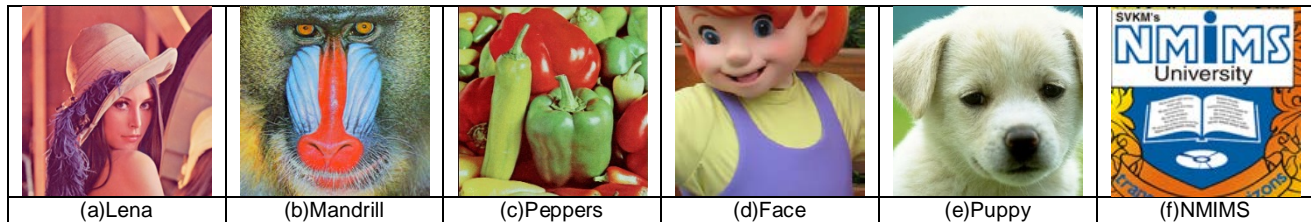


Fig. 1 (a)-(e) Set of host images (f) watermark image

## 4 RESULTS OF PROPOSED WATERMARKING METHOD

In this section results of proposed watermarking method after performing various attacks on watermarked images are given. Before moving ahead with results of various attacks, NMIMS watermark obtained by using only first 30 singular values is shown along with original NMIMS watermark image is shown in Fig. 2. A sample watermarked image Mandrill with NMIMS watermark embedded into it is also shown in

Fig. 2 MAE between original host and watermarked image is displayed below the image which corresponds to imperceptibility. Fig. 3 also shows the extracted NMIMS watermark when watermarked image is not subjected to any attack. MAE between embedded and extracted watermark is shown below it and it corresponds to robustness of the proposed method.

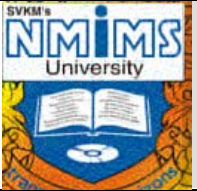
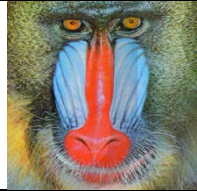
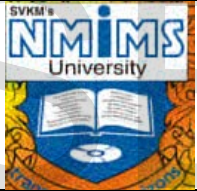
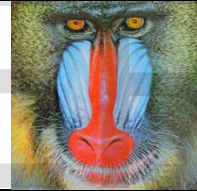
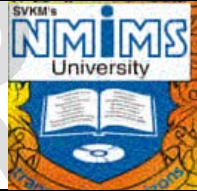
|  |  |  |   |  |
|--|--|--|---|--|
|  |  |  |  |  |
| MAE=11.475   | MAE=0.326  | MAE=0  | MAE=0.239   | MAE=0  |
| (a) Compressed watermark with 30 singular values                                   | (b) Watermarked image using column transform                                       | (c) Watermark extracted from column transformed Mandrill                           | (d) Watermarked image using row transform   | (e) Watermark extracted from row transformed Mandrill                                |

Fig. 2 (a) Embedded Watermark NMIMS obtained from first 30 singular values. (b)-(c) Watermarked Mandrill and extracted watermark using column self kronecker transform of DCT (e)-(f) Watermarked Mandrill and extracted watermark using row self kronecker transform of DCT

### 4.1 Compression attack

The most obvious attack on any digital data transmitted over network is compression to have optimal use of available bandwidth. Hence in the proposed method, compression attack is implemented using three different mechanisms. These three mechanisms are compression using transforms, compression using Vector quantization and JPEG compression. In transform based compression, DCT, DST, Walsh, Haar and DCT wavelet transform are

used to compress the watermarked images. In compression using Vector Quantization, Kekre's Fast Codebook Generation (KFCG) algorithm [28] is used with codebook size 256 to compress the watermarked images. JPEG compression is performed with quality factor 100. Fig. 3 shows watermarked Mandrill image after compressing using DCT. The watermarked image shown is obtained using column version and row version of self kronecker product of DCT.

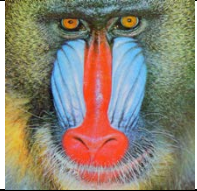
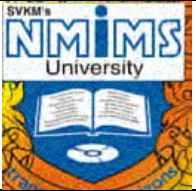
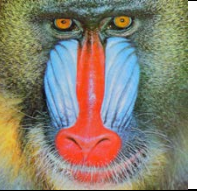
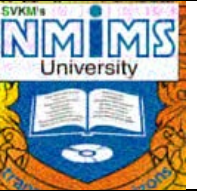
|   |   |  |   |
|---|---|--|---|
|  |  |  |  |
| MAE=2.894   | MAE=2.182   | MAE=2.211  | MAE=4.552   |

Fig. 3 (a)-(b) Watermarked Mandrill after compression using DCT and extracted watermark from it using column version of self kronecker of DCT (c)-(d) Watermarked Mandrill after compression using DCT and extracted watermark from it using row version of self kronecker of DCT



Fig. 3 shows that MAE between embedded and extracted watermark for compression attack using DCT is less for column version of DCT self kronecker product.

Fig. 4 shows another example result images for VQ based compression. Watermarked Mandrill image compressed

using Vector Quantization and extracted watermark from it where embedding of watermark is done using column and row version of self kronecker of DCT.

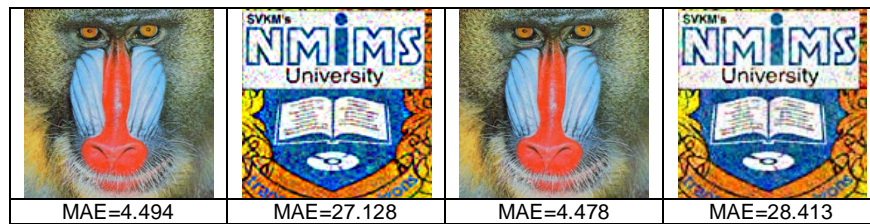


Fig. 4 (a)-(b)Watermarked Mandrill after compression using VQ and extracted watermark from it using column version of self kronecker of DCT (c)-(d)Watermarked Mandrill after compression using VQ and extracted watermark from it using row version of self kronecker of DCT

From Fig. 4 it is observed that column version of self kronecker product of DCT gives slightly better MAE between embedded and extracted watermark against VQ based compression. Table 1 shows the average MAE over 5 hosts against various types of compression attack using column version of self kronecker product of DCT, DST, Real Fourier Transform, Sinecosine transform, Walsh, Haar, DKT and Slant. Smallest value for specific type of compression is highlighted

and displayed in bold. It can be observed that DKT self kronecker product gives higher MAE values among other transforms against all types of compression except VQ based compression. From Table 1 it can be said that proposed method using self kronecker product of orthogonal transforms is highly robust against compression except JPEG and VQ compression. Similar observations are noted from Table 2 where transform matrix is applied row wise.

Table 1. MAE between embedded and extracted watermark using self kronecker product of various transforms column wise against compression attack.

| Compression using | MAE between embedded and extracted watermark using column version of Self kronecker of |        |        |            |        |        |        |        |
|-------------------|--|--------|--------|------------|--------|--------|--------|--------|
|                   | DCT  | DST    | RFT    | Sinecosine | Walsh  | Haar   | DKT    | Slant  |
| DCT               | 1.257  | 0.296  | 1.078  | 0.677      | 1.703  | 2.059  | 9.620  | 1.446  |
| DST               | 1.257  | 0.292  | 1.061  | 0.669      | 1.752  | 2.108  | 9.638  | 1.429  |
| Walsh             | 1.525  | 1.509  | 1.172  | 1.683      | 0      | 1.195  | 9.770  | 1.378  |
| Haar              | 1.693  | 3.157  | 3.422  | 3.363      | 2.521  | 1.683  | 2.213  | 1.059  |
| DCT wavelet       | 1.101  | 2.221  | 2.513  | 2.386      | 9.457  | 8.350  | 28.331 | 2.114  |
| JPEG              | 44.302   | 45.527 | 44.285 | 46.393     | 43.766 | 42.068 | 47.213 | 38.034 |
| VQ                | 41.030   | 37.876 | 42.346 | 36.870     | 41.050 | 26.982 | 29.148 | 31.665 |

Table 2. MAE between embedded and extracted watermark using self kronecker product of various transforms row wise against compression attack.

| Compression using | MAE between embedded and extracted watermark using row version of Self kronecker of |        |        |            |        |        |        |        |
|-------------------|---|--------|--------|------------|--------|--------|--------|--------|
|                   | DCT   | DST    | RFT    | Sinecosine | Walsh  | Haar   | DKT    | Slant  |
| DCT               | 1.816   | 0.633  | 2.300  | 0.638      | 3.319  | 3.512  | 9.860  | 1.253  |
| DST               | 1.793   | 0.623  | 2.355  | 0.634      | 3.339  | 3.555  | 9.897  | 1.246  |
| Walsh             | 2.436   | 1.716  | 2.212  | 1.876      | 1.064  | 1.946  | 11.602 | 1.401  |
| Haar              | 3.167   | 3.820  | 4.288  | 3.376      | 3.127  | 1.078  | 3.001  | 1.329  |
| DCT wavelet       | 1.546   | 3.478  | 2.767  | 3.736      | 10.375 | 12.344 | 35.333 | 1.679  |
| JPEG              | 45.332  | 48.178 | 45.286 | 47.699     | 45.223 | 41.596 | 51.090 | 35.042 |
| VQ                | 40.291  | 37.364 | 41.880 | 36.648     | 42.796 | 32.226 | 33.773 | 27.238 |

This behaviour of proposed method is compared with our previous work in which wavelet transform is used to embed the watermark. These wavelet transform matrices were generated using same existing orthogonal transform matrices explored here. Kekre's wavelet transform generation algorithm was used to generate these wavelet transform matrices. For e.g. DCT wavelet matrix of size 256x256 was generated using two DCT matrices of 16x16 sizes each. Graphs in following Fig. 5 show the comparison of self wavelet and

Self-kronecker product against compression attack when used column-wise to embed the watermark. From Fig. 5 it can be seen that the transform generated from self kronecker product of orthogonal transform matrix is more robust against compression attack. Especially self kronecker of DST and self kronecker of Sinecosine drastically improves the robustness as compared to DST wavelet and Sinecosine wavelet respectively. Similar observations are also noted for row version of self kronecker product

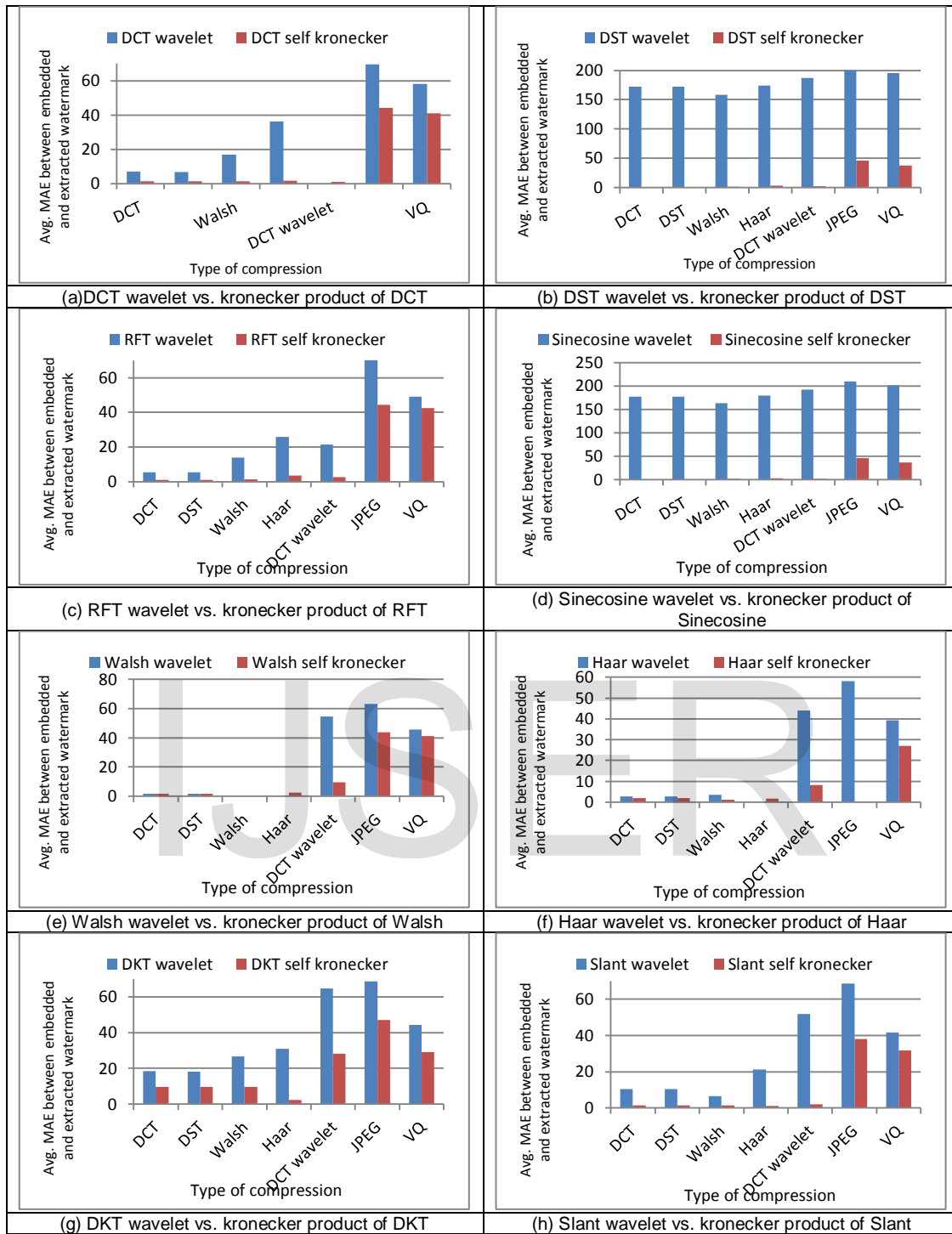


Fig. 5 Comparison of MAE between embedded and extracted watermark against compression attack using self wavelet and self kronecker product to embed the watermark.

From Fig. 5 it can be seen that the transform generated from self kronecker product of orthogonal transform matrix is more robust against compression attack. Especially self kronecker of DST and self kronecker of Sinecosine drastically improves the robustness as compared to DST wavelet and Sinecosine wavelet respectively. Similar observations are also noted for row version of self kronecker product.

## 4.2 Cropping attack

Fig. 6 shows watermarked Mandrill image where 32x32 square is cropped at center and extracted watermark from it using column and row version of self kronecker product of DCT.

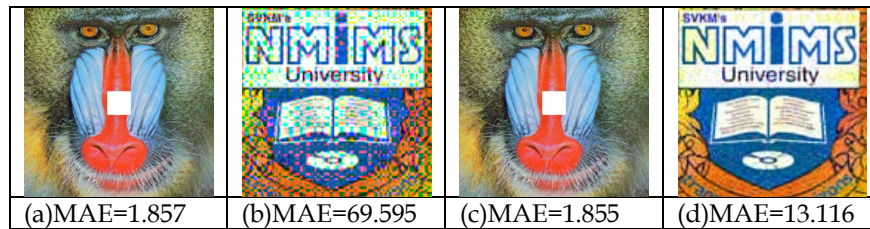


Fig. 6 (a)-(b)Watermarked Mandrill after cropping at center and extracted watermark from it using column version of self kronecker of DCT (c)-(d)Watermarked Mandrill after cropping at center and extracted watermark from it using row version of self kronecker of DCT

Fig. 6 shows that robustness shown by row version of DCT self kronecker product is three times better than column version.

Table 3 and Table 4 show average MAE values between embedded and extracted watermark over 5 host images using column and row versions of self kronecker product of various sinusoidal and non-sinusoidal transforms respectively. As can be seen from Table 3, self kronecker product of orthogonal

transforms cannot withstand against cropping attack. However, self kronecker of DKT, Walsh and Haar show acceptable robustness against 16x16 cropping at corner, 32x32 cropping at corner and 32x32 at centre respectively. Similarly from Table 4 it can be concluded that in row version, self kronecker product of DKT and Slant give acceptable robustness against 16x16 cropping at corner and that of Haar gives strong robustness against cropping 32x32 at centre.

Table 3. MAE between embedded and extracted watermark using self kronecker product of various transforms column wise against cropping attack.

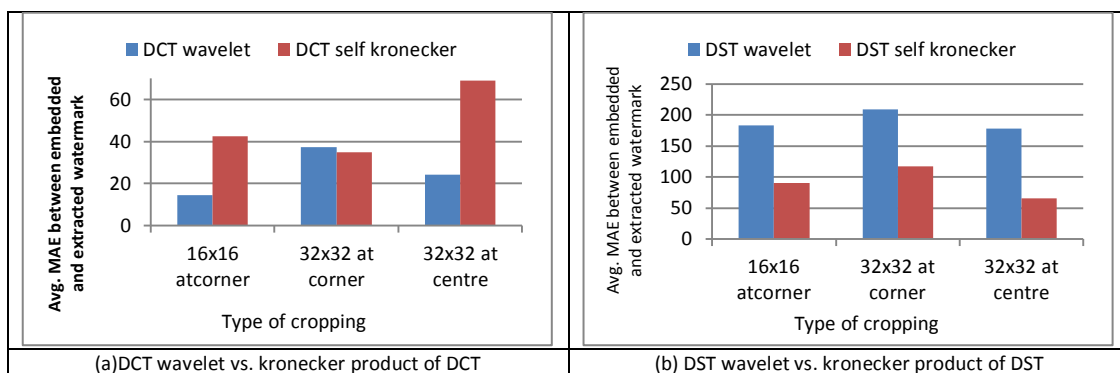
| Cropping type    | MAE between embedded and extracted watermark using column version of Self kronecker of |         |        |            |         |         |        |         |
|------------------|--|---------|--------|------------|---------|---------|--------|---------|
|                  | DCT  | DST     | RFT    | Sinecosine | Walsh   | Haar    | DKT    | Slant   |
| 16x16 at corners | 42.474   | 89.787  | 81.868 | 101.767    | 58.454  | 132.102 | 14.662 | 131.904 |
| 32x32 at corners | 34.779   | 117.495 | 57.650 | 116.716    | 27.485  | 280.589 | 49.186 | 277.859 |
| 32x32 at centre  | 68.999   | 65.978  | 81.745 | 64.708     | 109.976 | 0.775   | 36.685 | 61.026  |

Table 4. MAE between embedded and extracted watermark using self kronecker product of various transforms row wise against cropping attack.

| Cropping type    | MAE between embedded and extracted watermark using row version of Self kronecker of |         |        |            |        |         |        |         |
|------------------|---|---------|--------|------------|--------|---------|--------|---------|
|                  | DCT   | DST     | RFT    | Sinecosine | Walsh  | Haar    | DKT    | Slant   |
| 16x16 at corners | 55.123  | 85.365  | 52.871 | 95.223     | 53.575 | 76.915  | 20.492 | 13.417  |
| 32x32 at corners | 42.480  | 107.602 | 55.107 | 120.481    | 46.467 | 259.424 | 61.011 | 82.933  |
| 32x32 at centre  | 63.310  | 50.820  | 61.452 | 49.809     | 42.045 | 2.273   | 93.397 | 121.096 |

Fig. 7 shows the comparison of self wavelet and self kronecker of various orthogonal transforms against cropping attack when applied columnwise to embed the watermark. As can be seen from Fig. 7, self kronecker of DST and Sinecosine improves the performance by reducing the MAE between embedded and extracted watermark. For self kronecker

product of other transforms robustness drastically falls when applied column-wise. Similar observations are also noted for rowwise application of transform matrix generated from self kronecker product of orthogonal transforms. Thus self-wavelet transform is more robust than self kronecker product.



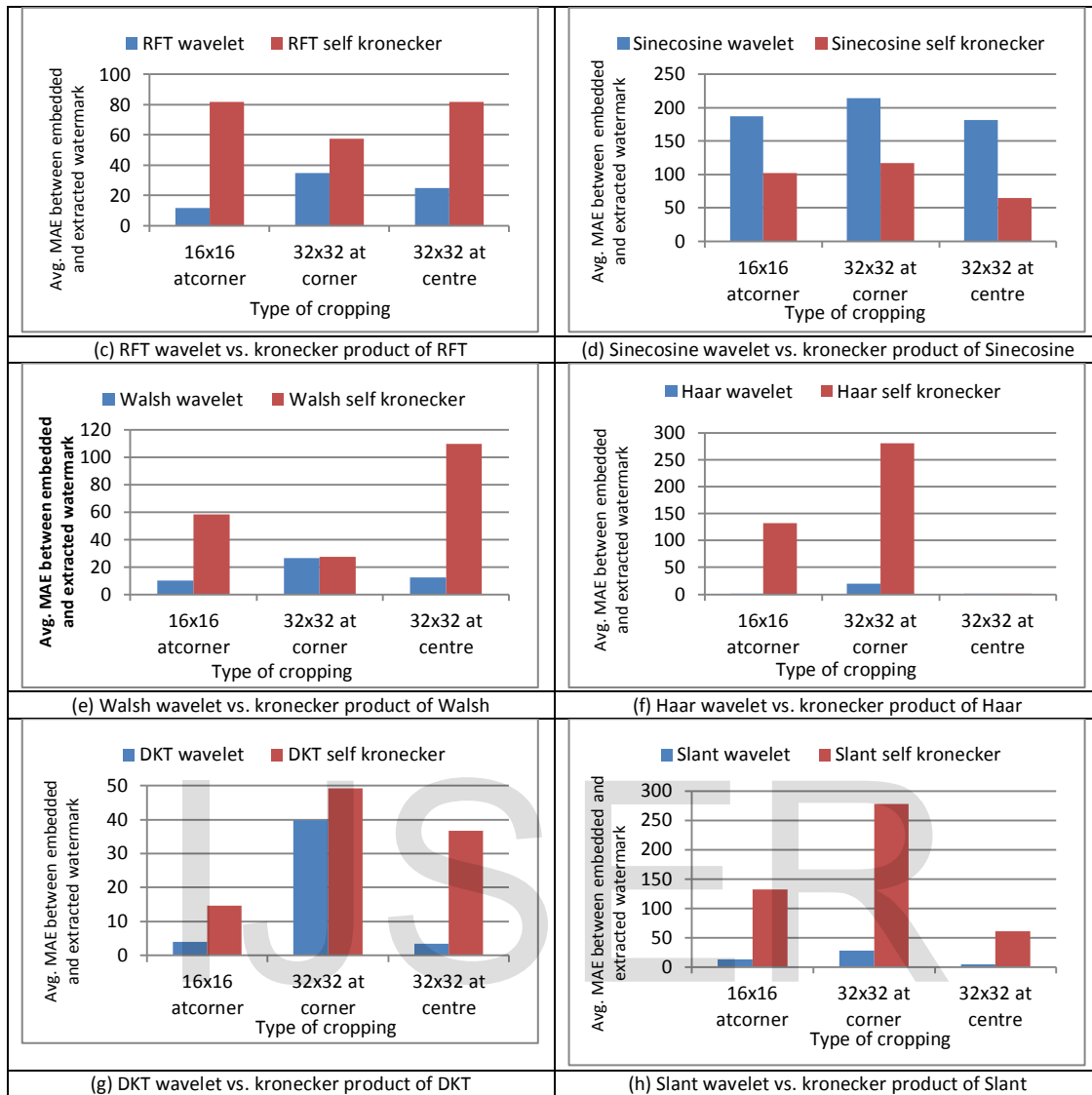


Fig. 7 Comparison of MAE between embedded and extracted watermark against cropping attack using self wavelet and self kronecker product to embed the watermark.

### 4.3 Noise addition attack

Two types of noises are added to watermarked images namely Gaussian distributed runlength noise and binary distributed runlength noise. Gaussian distributed run length noise is having discrete magnitude between +2 to -2. Binary distributed runlength noise has discrete magnitude 0 or 1. Binary distributed run length noise with different run lengths (1-10, 5-50 and 10-100) is added to the watermarked images.

Fig. 6 shows the performance of column and row version of self kronecker product of DCT against Gaussian distributed run length noise addition attacks for watermarked Mandrill image with NMIMS watermark embedded in it. From Fig. 8, we can say that column and row versions of self kronecker product of DCT perform almost equally well in terms of robustness for Gaussian distributed run length noise attack.

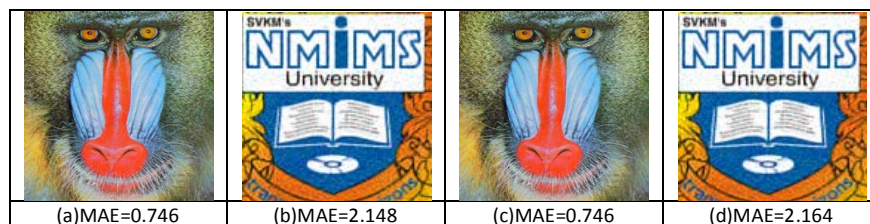


Fig. 8 (a)-(b) Watermarked Mandrill after adding Gaussian distributed run length noise and extracted watermark from it using column version of self kronecker of DCT (c)-(d) Watermarked Mandrill after adding Gaussian distributed run length noise and extracted watermark from it using row version of self kronecker of DCT

Table 5 shows average MAE values between embedded and extracted watermark against noise addition attack. These values are calculated over 5 host images using column and row versions of self kronecker product of various sinusoidal and non-sinusoidal transforms. Table 6 shows the MAE values for row version of self kronecker product. From Table 5 and

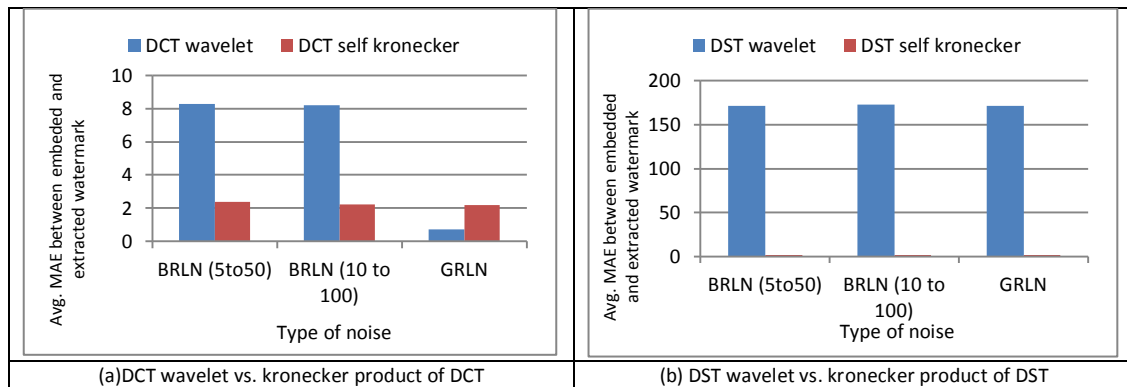
Table 6 we can see that the MAE values obtained by all explored self kronecker product of transforms are small and give good quality of extracted watermark. Performance of self kronecker product of orthogonal transforms is compared with that of self wavelet transform in the graphs shown in Fig. 9.

Table 5. MAE between embedded and extracted watermark using self kronecker product of various transforms column wise against noise addition attack.

| Noise type                                 | MAE between embedded and extracted watermark using column version of Self kronecker of |       |       |            |       |       |       |       |
|--|--|-------|-------|------------|-------|-------|-------|-------|
|  | DCT  | DST   | RFT   | Sinecosine | Walsh | Haar  | DKT   | Slant |
| Binary distributed Run Length noise (1-10) | 0  | 1.081 | 0     | 1.114      | 0     | 0     | 0     | 0     |
| Binary distributed Run Length noise (1-10) | 2.373  | 1.708 | 2.199 | 1.838      | 2.358 | 1.894 | 1.743 | 1.582 |
| Binary distributed Run Length noise (1-10) | 2.216  | 1.791 | 1.983 | 1.765      | 2.354 | 2.258 | 1.690 | 1.583 |
| Gaussian distributed run length noise      | 2.181  | 1.602 | 2.227 | 1.517      | 2.022 | 2.539 | 1.383 | 4.321 |

Table 6. MAE between embedded and extracted watermark using self kronecker product of various transforms row wise against noise addition attack.

| Noise type                                 | MAE between embedded and extracted watermark using row version of Self kronecker of |       |       |            |       |       |       |       |
|--|---|-------|-------|------------|-------|-------|-------|-------|
|  | DCT   | DST   | RFT   | Sinecosine | Walsh | Haar  | DKT   | Slant |
| Binary distributed Run Length noise (1-10) | 4.193   | 3.331 | 5.172 | 3.578      | 4.675 | 5.109 | 2.919 | 2.611 |
| Binary distributed Run Length noise (1-10) | 4.917   | 3.281 | 4.821 | 3.168      | 4.725 | 4.521 | 4.034 | 3.420 |
| Binary distributed Run Length noise (1-10) | 3.747   | 2.080 | 3.137 | 2.263      | 3.169 | 3.379 | 4.371 | 3.547 |
| Gaussian distributed run length noise      | 1.862   | 0.996 | 1.748 | 1.077      | 1.488 | 1.589 | 1.999 | 1.382 |





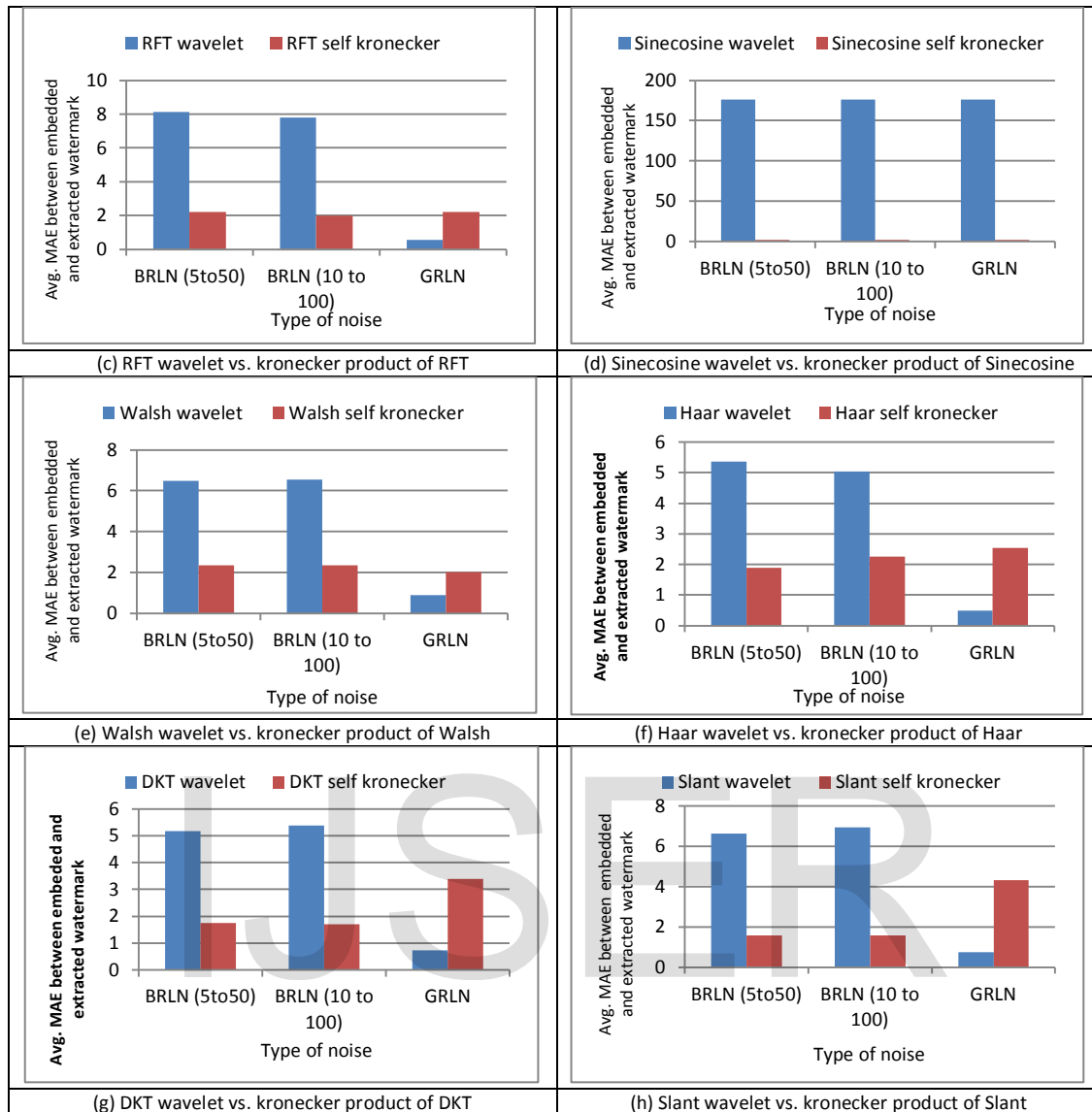


Fig. 9 Comparison of MAE between embedded and extracted watermark against Noise addition attack using self wavelet and self kronecker product to embed the watermark.

From Fig. 9 we can say that when self kronecker product of orthogonal transforms is used to embed the watermark, it significantly improves the performance of proposed method against noise addition attack. This improvement is observed for binary distributed run length noise with run 5-50 and 10 to 100 by all explored self kronecker products of orthogonal transforms. For Gaussian distributed run length noise, self wavelet comes out to be more robust except for kronecker product of DST and sinecosine. In case of DST and Sinecosine self kronecker, sudden decrease in MAE is observed.

#### 4.4 Resizing attack:

Resizing of images is performed using three different techniques. In first approach, bicubic interpolation method is used to double the size of watermarked and then to reduce

back to its original size. In second approach transform based zooming [29] is used to double and then to reduce the watermarked image to its original size. Various orthogonal transforms like DFT, DCT, DST, Real Fourier Transform and Hartley transform are used to resize the image. In third approach grid based interpolation [30] is used to perform the resizing. From such zoomed-reduced watermarked image watermark is extracted. Fig. 10 shows watermarked Mandrill after zooming and then reducing using grid based interpolation along with extracted watermark from it. Both column and row version self kronecker product results are shown. An important observation is noted in transform based resizing that extracted watermark shows highest correlation with embedded watermark with MAE value zero.

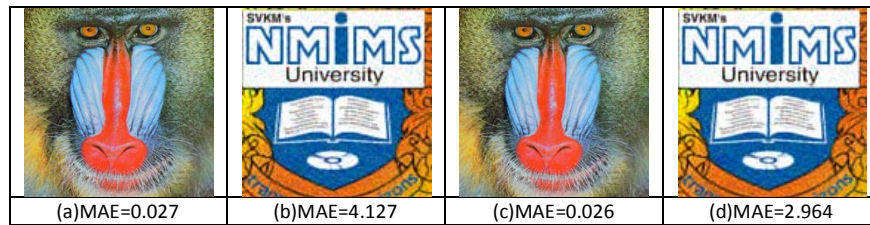


Fig. 10 (a)-(b) Watermarked Mandrill after resizing using Grid based interpolation and extracted watermark from it using column version of self kronecker of DCT (c)-(d) Watermarked Mandrill after resizing using Grid based interpolation and extracted watermark from it using row version of self kronecker of DCT

From Fig. 10 it is observed that row version of self kronecker of DCT is more robust than column version against resizing using Grid based interpolation and performs equally well for imperceptibility.

Table 7 and Table 8 show average MAE values between embedded and extracted watermark against resizing attack averaged over five host images using column and row versions of kronecker products of various transforms.

Table 7. MAE between embedded and extracted watermark using self kronecker product of various transforms column wise against resizing attack.

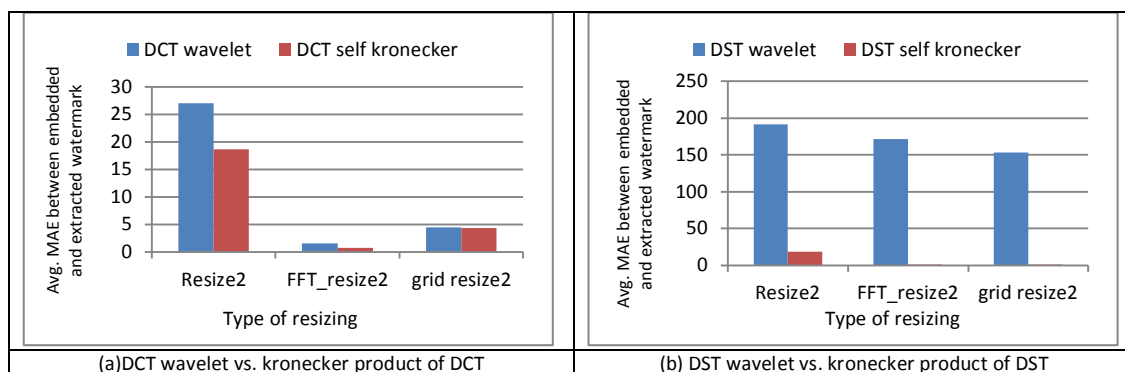
| Resizing type                 | MAE between embedded and extracted watermark using column version of Self kronecker of |        |        |            |        |        |        |        |
|-------------------------------|--|--------|--------|------------|--------|--------|--------|--------|
|                               | DCT  | DST    | RFT    | Sinecosine | Walsh  | Haar   | DKT    | Slant  |
| Bicubic Interpolation         | 18.668   | 18.457 | 18.085 | 19.071     | 19.019 | 17.566 | 23.142 | 15.745 |
| Transform based zooming (DFT) | 0.678  | 0.533  | 0.732  | 0.494      | 0.718  | 0.704  | 0.544  | 0.553  |
| Grid interpolation            | 4.367  | 1.313  | 3.953  | 1.221      | 9.188  | 4.379  | 1.831  | 3.844  |

Table 8. MAE between embedded and extracted watermark using self kronecker product of various transforms row wise against resizing attack.

| Resizing type                 | MAE between embedded and extracted watermark using row version of Self kronecker of |        |        |            |        |        |        |        |
|-------------------------------|---|--------|--------|------------|--------|--------|--------|--------|
|                               | DCT   | DST    | RFT    | Sinecosine | Walsh  | Haar   | DKT    | Slant  |
| Bicubic Interpolation         | 19.045  | 19.469 | 18.434 | 19.962     | 19.389 | 17.773 | 25.481 | 14.322 |
| Transform based zooming (DFT) | 0.911   | 0.633  | 0.719  | 0.605      | 0.711  | 0.919  | 0.539  | 0.699  |
| Grid interpolation            | 4.602   | 1.396  | 3.920  | 1.472      | 9.337  | 4.250  | 1.639  | 3.538  |

From Table 7 and Table 8 it is observed that column as well as row version of self kronecker product show strong robustness against transform based resizing. In the table MAE values for resizing using DFT are shown. For other transforms used for resizing MAE values observed are zero. Next to transform based resizing, high robustness is shown

against resizing using Grid based interpolation. Quite less robustness is observed against resizing using bicubic interpolation. Performance of wavelet transforms and self kronecker product against resizing attack are compared in the following Fig. 11.



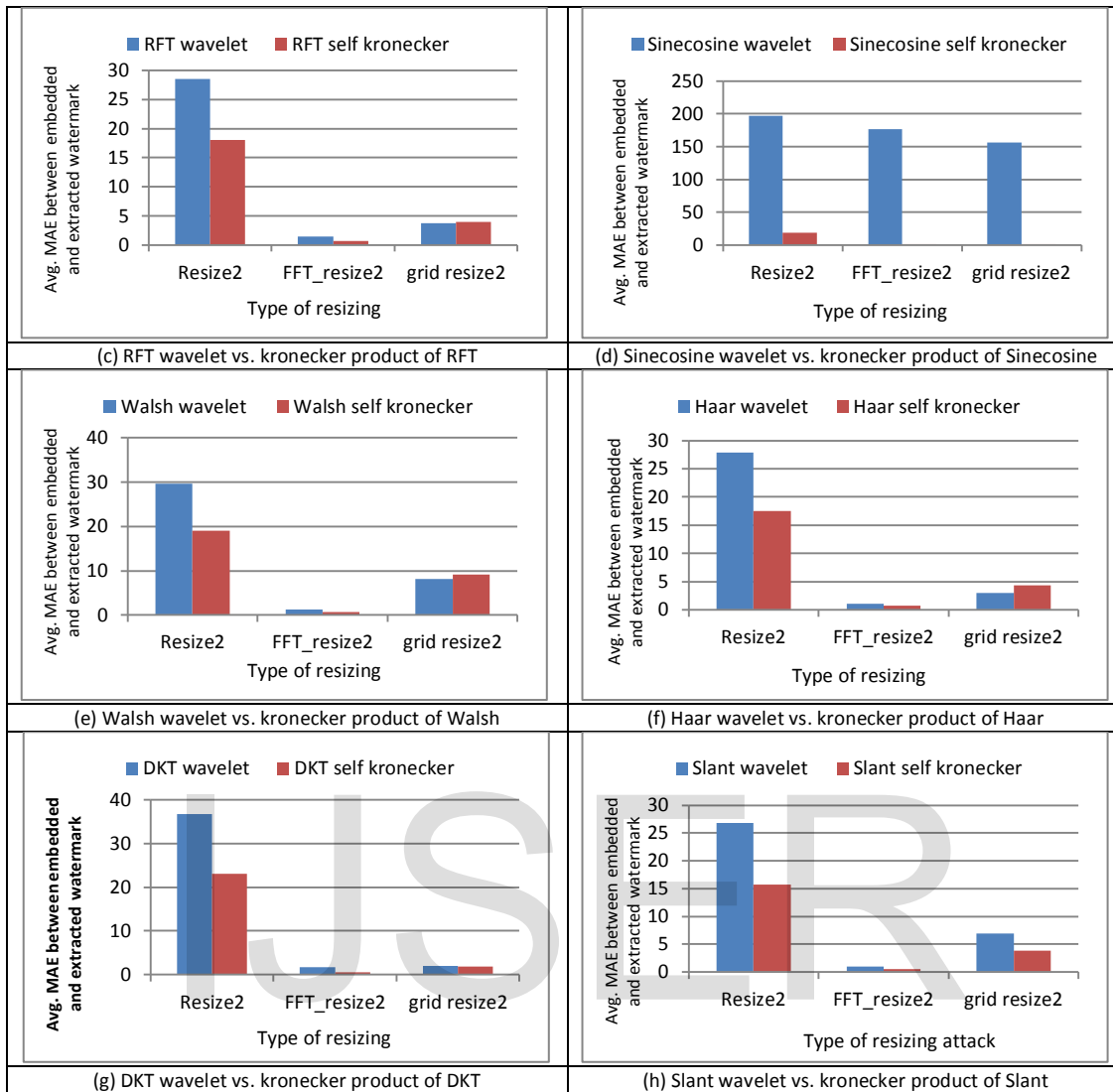


Fig. 11 Comparison of MAE between embedded and extracted watermark against Resizing attack using self wavelet and self kronecker product to embed the watermark.

#### 4.5 Histogram equalization attack:

Watermarked images are subjected to histogram equalization and watermark is extracted from them. Fig. 12 shows histogram equalized Mandrill with NMIMS watermark embedded into it for both column and row versions of self kronecker product of DCT. Fig. 12 shows that column version

of DCT self kronecker is better in robustness against histogram equalization. However, overall performance shows that proposed method has poor robustness against histogram equalization. Also the performance of self kronecker product is found to be slightly better than self-wavelet used to embed the watermark.

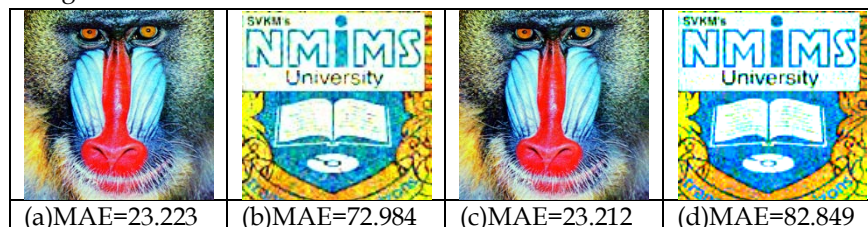


Fig. 12 (a)-(b) Watermarked Mandrill after histogram equalization and extracted watermark from it using column version of self kronecker of DCT (c)-(d) Watermarked Mandrill after histogram equalization and extracted watermark from it using row version of self kronecker of DCT

## 5 CONCLUSIONS

In this paper a watermarking using self kronecker product of orthogonal matrix is proposed. Kronecker product is a special

case of wavelet transform where contribution of local features of an image is made zero and only global properties make their appearance. Self kronecker product where two component transforms selected are same gives better

robustness against various attacks like image compression, noise addition, resizing and histogram equalization. It does not survive cropping attack except the kronecker product of Haar. Quantitatively, using self kronecker product improves the performance against compression attack by 27-83%. For noise addition attack, this improvement ranges from 25% to 100 %. For resizing attack self kronecker product improves the robustness over self-wavelet transforms by 34-100%. For histogram equalization performance improvement from 5 to 34% is observed.

## References

- [1] H. B. Kekre, Tanuja Sarode, Shachi Natu, "Performance comparison of watermarking using SVD with orthogonal transforms and their wavelet transforms", International journal of image, graphics and signal processing, submitted for publication.
- [2] Wai Chu, "DCT-Based Image Watermarking Using Subsampling", IEEE transactions on multimedia, vol. 5, no. 1, pp. 34-38, March 2003.
- [3] Adrian G. Bor\_s and Ioannis Pitas, "Image watermarking using block site selection and DCT domain constraints", Optics Express, Vol. 3, No. 12, pp.512-523, 1998.
- [4] Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and Vineeth Sarma Venugopala Sarma, "A Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking", International Journal of Computer Theory and Engineering, Vol. 2, No. 4, pp. 647-653, August 2010.
- [5] Tsui, Tsz Kin, Xiao-Ping Zhang, and Dimitrios Androustos. "Color image watermarking using multidimensional Fourier transforms." Information Forensics and Security, IEEE Transactions on 3, no. 1, pp. 16-28, 2008.
- [6] Ramkumar, Mahalingam, Ali N. Akansu, and A. Aydin Alatan. "A robust data hiding scheme for images using DFT", In IEEE Proceedings of International Conference on Image Processing, vol. 2, pp. 211-215. 1999.
- [7] Premaratne, P., and C. C. Ko, "A novel watermark embedding and detection scheme for images in DFT domain", In Seventh International Conference on Image Processing and Its Applications, IET, 1999. (Conf. Publ. No. 465), vol. 2, pp. 780-783.
- [8] Kitamura, Itaru, Satoshi Kanai, and Takeshi Kishinami, "Copyright protection of vector map using digital watermarking method based on discrete Fourier transform", In Geoscience and Remote Sensing Symposium, 2001. IEEE 2001 International, vol. 3, pp. 1191-1193.
- [9] Dr. B. Eswara Reddy, P. Harini, S. Maruthu Perumal & Dr. V. Vijaya Kumar, "A New Wavelet Based Digital Watermarking Method for Authenticated Mobile Signals", International Journal of Image Processing (IJIP), Volume (5): Issue (1), pp. 13-24, 2011.
- [10] Nagaraj V. Dharwadkar & B. B. Amberker, "Determining the Efficient Sub band Coefficients of Biorthogonal Wavelet for Grey level Image Watermarking", International Journal of Image Processing Volume (4): Issue (2), pp. 89-105.
- [11] Yiwei Wang, , John F. Doherty, and Robert E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE transactions on image processing, vol. 11, no. 2, pp.77-88, February 2002.
- [12] Mei Jiansheng, Li Sukang, Tan Xiomeri, "A digital watermarking algorithm based on DCT and DWT", Proc. of International symposium on web information systems and applications, pp. 104-107, May 2009.
- [13] Surya pratap Singh, Paresh Rawat, Sudhir Agrawal, "A robust watermarking approach using DCT-DWT", International journal of emerging technology and advanced engineering, vol. 2, issue 8, pp. 300-305, August 2012.
- [14] Saeed Amirgholipour, Ahmed Naghsh-Nilchi, "Robust digital image watermarking based on joint DWT-DCT", International journal of digital content technology and its applications, vol. 3, No. 2, pp. 42-54, June 2009.
- [15] Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshin Hoque, Md. Iqbal Hasan Sarkar, "Combined DWT-DCT based digital image watermarking technique for copyright protection", In proc. of International conference on electrical and computer engineering, pp. 458-461, Dec 2012.
- [16] Zhen Li, Kim-Hui Yap and Bai-Ying Li, "A new blind robust image watermarking scheme in SVD-DCT composite domain", in proc. of 18th IEEE international conference on image processing, pp. 2757-2760, 2011.
- [17] R. Liu and T. Tan, A SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121-128, 2002.
- [18] P. Bao and X. Ma, Image adaptive watermarking using wavelet domain singular value decomposition, IEEE Trans. Circuits and Systems for Video Technology, vol. 15, no. 1, pp. 96-102, 2005.
- [19] E. Ganic and A. M. Eskicioglu, Robust DWT-SVD domain image watermarking: Embedding data in all frequencies, Proc. of the Workshop on Multimedia and Security, vol. 1, pp. 166-174, 2004.
- [20] Xi-Ping and Qing-Sheng Zhu, "A robust wavelet-domain watermarking algorithm for color image", Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, pp.13-16 August 2006.
- [21] A Mansouri, A Mahmoudi Aznavah, F Azar, "SVD-based digital image watermarking using complex wavelet transform", Sadhana, Vol. 34, Part 3, pp. 393-406, June 2009.
- [22] Rashmi Agarwal, K. Venugopalan, "Digital watermarking of color images in the singular domain", IJCA Special issue on "Computational Science- New Dimensions & Perspectives, pp. 144-149, 2011.
- [23] S. Murty, Dr. Rajesh Kumar, "A Robust Digital Image Watermarking Scheme using Hybrid DWT-DCT-SVD Technique", IJCSNS, Vol.10, No.10, pp. 185-192, Oct 2010.
- [24] Satendra Kumar, Ashwini Saini, Papendra Kumar, " SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform", IJCA, Vol. 45No. 10, pp.7-11, May 2012.
- [25] R. Krishnamoorthi, Sheba Kezia, "Image Adaptive Watermarking with Visual Model in Orthogonal Polynomials based Transformation Domain", IJICE, 5:2, pp. 146-153, 2009.
- [26] Ko-Ming Chan, Long-wen Chang, "A Novel Public Watermarking System based on Advanced Encryption System", IEEE Proc.of 18th International Conference on Advanced Information Networking and Application, 2004.
- [27] Veysel Aslantas, A. Latif Dogan and Serkan Ozturk, "DWT-SVD based image watermarking using particle swarm optimizer", Proc. of IEEE International Conference on Multimedia and Expo, pp. 241-244, 2008.
- [28] Kekre, H. B., and Tanuja K. Sarode, "Fast Codebook Generation Algorithm for Color Images using Vector Quantization", International Journal of Computer Science and Information Technology 1.1: 7-12, 2009.
- [29] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Image Zooming using Sinusoidal Transforms like Hartley, DFT, DCT, DST and Real Fourier Transform", International journal of computer science and information security Vol. 12 No. 7, 2014.
- [30] H. B. Kekre, Tanuja Sarode, Sudeep Thepade, "Grid based image scaling technique", International Journal of Computer Science and Applications, Volume 1, No. 2, pp. 95-98, 2008.