ERTU's Package for Gray Image Watermark Application

Salwa M. Serag Eldin, Salah A. Khamis, Prof. Abdel-Aziz Ibrahim Mahmoud Hassanin, Mohammed A. Alsharqawy

***Abstract*-There are many contents have to be saved from stealing or abused by unauthorized users or groups in media's organization. In this work, watermarking is used for this purpose. A watermarking image that belongs to the organization is inserted into the content needed to be protected to help the owners for detecting any illegal use of it. Transforms like Discrete Cosine Transform (DCT), Discrete Sine Transform (DST) or Discrete Wavelet Transform (DWT) based on Fraction Fourier Transform (FracFT) are used to test which is suitable for the cloud and new tests are proposed to evaluate the performance of watermarking process in both case of embedding and extracting. The embedded factor is also evaluated to determine the best value for Egyptian Radio and Television Union (ERTU)'s cloud and then yield a good agreement which is done in this work. Many attacks are also defined to justify the algorithm's robustness and which can be used to obtain high quality services for the Authorized Groups (AuthGs). The ability to provide these services to AuthGs does not depend on the distance and the connection to the cloud.**

***Index Terms*—Cloud Comuting, ERTU, Gray Image, Watermrking, DCT, DST, DWT, FracFT.**

I. INTRODUCTION

Saving the contents of any cloud using watermarking demands high robustness against any attack. Maintaining these demands requires a good algorithm that can face the problems or attacks besides do the essential purpose which is saving it from any abuse. There is a contribution to protect contents by watermarks using Arabian letters where it has multipoint. From this advantage, it can be embedded 2 Byte instead of one Byte and there is no increase in the payload of the signal and it still maintains its imperceptibility [1]. The Digital Right Management (DRM) is one of aspect that studies how to control the cloud and the contents contained in. one of this contained type is multimedia where encryption, watermarking and distributing through wireless channel like mobile or through internet connection is important issue that many studies are deployed. Applying the management for this multimedia is discussed in [2]. An image watermarking algorithm against geometric attacks is proposed to solve watermarking synchronization problems [3]. A watermarking method of image for copyright protection based on Hadamard transform is proposed. This watermarking method deals with the extraction of the watermark information in the absence of original image, hence the blind scheme is obtained [4]. There is an extensive literature about watermarking algorithms and methods as well as possible attack techniques. [5] collects a part of this vast literature in order to make easier for a non-expert reader about watermarking to have a high-level overview on new trends and technologies related to multimedia watermark algorithms and attacks. A new blind watermarking scheme for Gray scale image is proposed based on contourlet Transform, Singular value decomposition and chaotic cellular automata. A cellular automaton is used to encrypt the watermarking logo to improve the security of watermarked image also used to determine the location of image's block for the watermarking embedding [6]. This paper is organized as follow: Defining the parameters and algorithm used in section II. The numerical results are presented in section III. Finally, in section IV, the conclusion of results is summarized.

II. FORMULATIONS OF PROBLEMS

Watermarking image need to be measured and determined the qualities to decide how much it is effective. In the following, various metrics will be defined and explained to understand why it has been used in evaluation and the factors that must be considered. The normal distribution is measure for probability of the data containing through the image and the distribution of it. It can be described as:

$$\mathbf{f(x)} = \frac{\mathbf{1}}{\boldsymbol{\sigma\sqrt{2\pi}}}\mathbf{e}^{-\frac{(\mathbf{x}-\boldsymbol{\mu})^2}{2\boldsymbol{\sigma}^2}} \tag{1}$$

where the parameter μ in this formula is the mean or expectation of the distribution. The parameter σ is its standard deviation; its variance is therefore σ^2. A random variable with a Gaussian distribution is said to be normally distributed and is called a normal deviate. Spectrogram is a graph which indicates the frequencies of speech versus time. It is used to get visual indication and comparison between the original and processed audio. Distribution of the signal gives the distribution of the signal's amplitude and it becomes a good comparison tool between processed and original speech. Histograms show the distribution of data values across a data range. It may be divided to many categories:

a) Cartesian coordinates: shows the distribution of the elements in Y as a histogram with equally spaced bins between the minimum and maximum values in Y.
b) Matrix input argument: when Y is a matrix, histogram creates a set of bins for each column, displaying each set in a separate color.
c) Specifying number of bins: interpret their second argument in one of two ways as the locations on the axis or the number of bins. When the second argument is a vector x, it specifies the

locations on the axis and distributes the elements in length(x) bins.

d) Using data cursors: when the data cursor tool is used on a histogram plot, it customizes the data tips it displays in an appropriate way. Instead of providing x, y, and z-coordinates, the data tips display the following information: number of observations falling into the selected bin, the x value of the bin's center and the lower and upper x values for the bin

Scatter plots (also called scatter diagrams) are used to investigate the possible relationship between two variables that both relate to the same "event". A straight line of best fit (using the least squares method) is often included. The Scatter diagram helps to identify the existence of a measurable relationship between two items by measuring them in pairs and plotting them on a graph. Things to look for:

a) If the points cluster in a band running from lower left to upper right, there is a positive correlation (if x increases, y increases).
b) If the points cluster in a band from upper left to lower right, there is a negative correlation (if x increases, y decreases).
c) Imagine drawing a straight line or curve through the data so that it "fits" as well as possible. The more the points cluster closely around the imaginary line of best fit, the stronger the relationship that exists between the two variables.
d) If it's hard to see where the draw a line, and if the points show no significant clustering, there is probably no correlation.

FracFT is the generalized form of Fourier transform that is represent tool for time-varying and non-stationary signal processing the classical Fourier Transform is a rotation in time- frequency plane over an angle FracFT is generalized form that corresponds to a rotation over arbitrary angle attack [7-8]. It is defined as:

$$\mathbf{F^p[f(x)] = \int_{-\infty}^{\infty} K_p(x,u) f(x) dx \quad 0 \le |p| \le 2} \quad (2)$$

$$\mathbf{K_\alpha(t,u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}} \; e^{j\left(\frac{t^2+u^2}{2}\right)\cot\alpha - jut\,\csc\alpha} & \text{if } \alpha \text{ is not a multiple of } \pi \\ \delta(t-u) & \text{if } \alpha \text{ is a multiple of } 2\pi \\ \delta(t+u) & \text{if } \alpha+\pi \text{ is a multiple of } 2\pi \end{cases}} \quad (3)$$

Where p is the order of FracFT, α is the rotation angle, also the relationship of p and is $\alpha = \frac{p\pi}{2}$, $K_P(x,u)$ is the kernel function of the FracFT. The DCT and the IDCT of N × N image are defined as [9]:

$$\mathbf{C(u,v) = \frac{2}{N}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos[\frac{\pi(2x+1)u}{2N}]\cos[\frac{\pi(2y+1)v}{2N}]} \quad (4)$$

$$\mathbf{f(x,y) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v)\cos[\frac{\pi(2x+1)u}{2N}]\cos[\frac{\pi(2y+1)v}{2N}]} \quad (5)$$

Where f (x, y) is the pixel intensity at the image location (x,y), and C(u,v) is the DCT coefficient at the transform location (u,v).

$$\mathbf{\alpha(u) = \alpha(v) = \begin{cases} \frac{1}{\sqrt{2}} & u = v = 0 \\ 1 & \text{otherwise} \end{cases}} \quad (6)$$

The DST and the IDST of N × N image are defined as [8]:

$$\mathbf{C(u,v) = \frac{2}{N}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\sin[\frac{\pi(2x+1)u}{2N}]\sin[\frac{\pi(2y+1)v}{2N}]} \quad (7)$$

$$\mathbf{f(x,y) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v)\sin[\frac{\pi(2x+1)u}{2N}]\sin[\frac{\pi(2y+1)v}{2N}]} \quad (8)$$

Where f (x, y) is the pixel intensity at the image location (x, y), and C(u, v) is the DST coefficient at the transform location (u,v).

$$\mathbf{\alpha(u) = \alpha(v) = \begin{cases} \frac{1}{\sqrt{2}} & u = v = 0 \\ 1 & \text{otherwise} \end{cases}} \quad (9)$$

The DWT is performed using multilevel filter banks. The one level of decomposition can mathematically be expressed as follows [9]:

$$\mathbf{y_{high}(k) = \textstyle\sum_n x(k) g(2k-n)} \quad (10)$$

$$\mathbf{y_{low}(k) = \textstyle\sum_n x(k) h(2k-n)} \quad (11)$$

Where yhigh(k) and ylow(k) are the outputs of the high pass an low pass filters, respectively, after subsampling by two. For images, the DWT is performed row by row and then, column by column. The image after wavelet decomposition is divided into four bands; a low frequency band LL, and three high frequency bands LH, HL and HH. Peak Signal to Noise Ratio (PSNR) is the measure for estimate of the quality of reconstructed image with the original one. It is go to by computing, the error between cover image with size (N_1 x N_2) pixel and watermarked image. So Means Square Error MSE is obtained Firstly then gets Root MSE (RMSE) and PSNR in (dB) is given by [10-11]:

$$\mathbf{PSNR = 20\ \log_{10} \frac{\text{max pixel}}{\sqrt{\frac{1}{N_1 N_2 \sum_i \sum_j (h(i,j) - h'(i,j))^2}}}} \quad (12)$$

Where $h(i,j)$ and $h'(i,j)$ are the intensity of the (i,j)th pixel before and after watermarking respectively. Correlation coefficient is used for similarity measurement. It give an indication that how the original and watermarked image are identical. There is of course threshold to decide the presence the watermark absence [9], [12]. It can be calculated as:

$$C = \frac{\sum_{r=1}^{H}\sum_{c=1}^{W}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{\left[\sum_{r=1}^{H}\sum_{c=1}^{W}(I_1(r,c)-\bar{I}_1)^2\right]\left[\sum_{r=1}^{H}\sum_{c=1}^{W}(I_2(r,c)-\bar{I}_2)^2\right]}} \quad (13)$$

Where $I_1(r,c)$ is the value of the pixel at the point (r, c) in the original audio. $I_2(r,c)$is the value of pixel at (r, c) in the encrypted audio, $\bar{I}_1$ is the mean of the original audio and $\bar{I}_2$ is the mean of the encrypted audio that is calculated as follows:

$$\bar{I} = \frac{1}{W*H}\sum_{r=1}^{H}\sum_{c=1}^{W} I(r,c) \quad (14)$$

Similarity is a measure to detect the presence of watermark in the image. It calculates the intensity of the pixel for original and extracted watermark. If the image has not been watermarked, then it can be modeled as zero mean random variable if there is a slight different, then this image has been watermarked. So this metric give an indication for presence or absence of water mark, the degree of similarity give a picture for the amount of information that has been added besides the presence of attacks if any. It is at also considered as a measure for the robustness of the watermark against attack [7]. The layout of the processing is described at Fig. 1 while the Graphical User Interface (GUI) is monitored in Fig. 2.

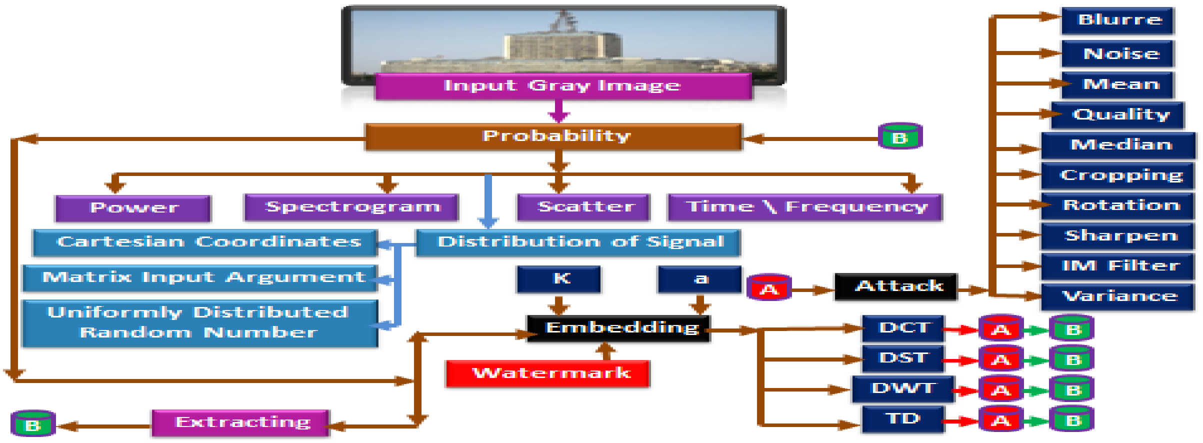


Fig. 1. The layout of processing of the watermarking.

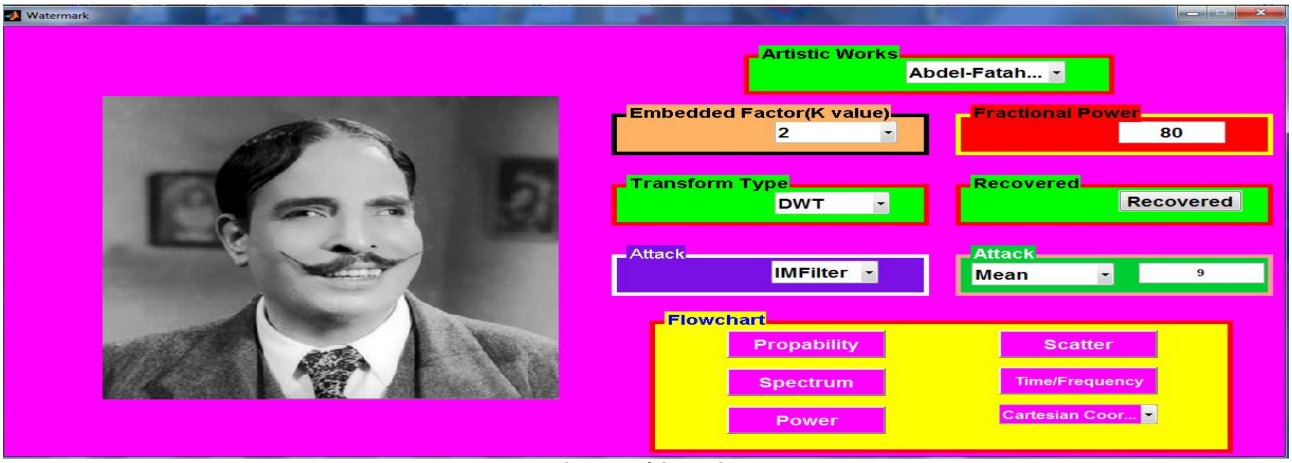


Fig. 2. The GUI of the application.

III. Numerical Results:

In this work, many transforms are used for watermarking embedded or extracted. It is all based on FracFT where it is used besides another transform like (DCT), (DST) or (DWT). After embedding process, many attacks are applied to evaluate the performance of the algorithm where it can be chosen the best for the cloud where it one of the most important application.

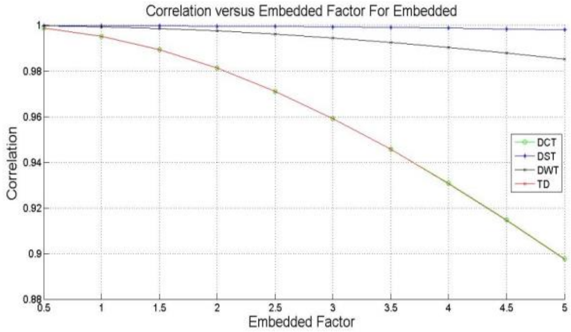
1. Embedded Factor

It is a factor that determines the gain used for embedding watermark image. It is always an integer value. In the process of embedded watermark, the bits of cover image is substituted by other of watermark for one Pixel, there are eight bits to be chosen from for replacing that can be used. Usually Least Significant Bit (LSB) is used. In Fig. 3 and Fig. 4, it determines the effects of embedding factor against the correlation and PSNR respectively. From these figure, it can be realized that PSNR is Deterioration badly after K= 4. In his work K=1 is used for all discrete transforms [11]. The images are used in this work are represented in Fig. 5.

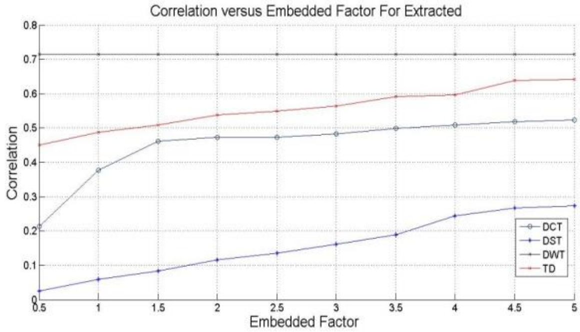
2. Embedding Process

In embedding process, a watermarking image is inserted into the content. Then, the new image is reconstructed to be like the original one containing the watermarking image. PSNR is calculated to indicate how much the two images are identical. The highest PSNR is, the best algorithm is. In Fig. 6, the original image of Ismail Yassen and the watermarked using DCT and DST show the similarity between them but there is a difference in DST case. Abdel-Fattah El

Osarry and DWT watermarked image are displayed and both are alike as seen.

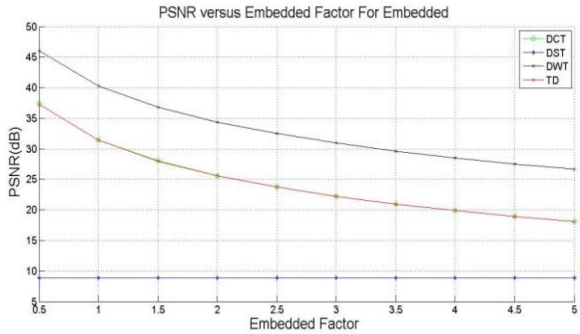


(a)

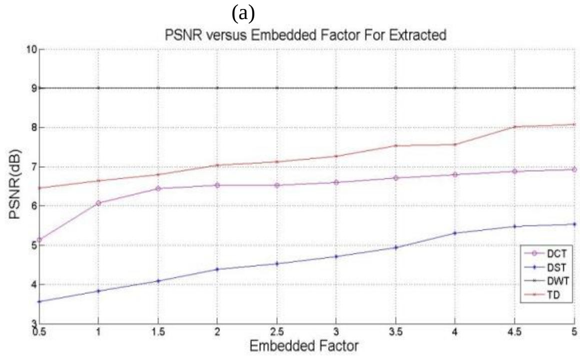


(b)

Fig. 3. The effect of embedded factor correlation PSNR in case of (a) Embedding process (b) Extracting process.



(a)

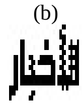


(b)

Fig. 4. The effect of embedded factor versus PSNR in case of (a) Embedding process (b) Extracting process.

(a)

(b)

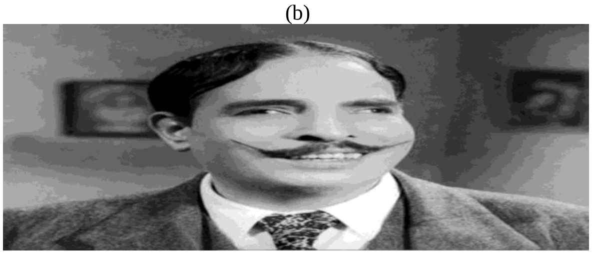


(c)

Fig. 5. The original image that is used (a) Ismail Yassen, (b) Abdel-Fattah El-Osarry and (c) watermark image.

(a)

(b)



(c)

Fig. 6. The watermarked image that is used (a) DCT, (b) DST and (c) DWT.

The probability is a tool to detect the chance of something occurs. It is used to count the possibility of each data in the image. The probability of Ismail Yassen’s image indicate that the data spread across the image and it concentrate from 0 to 250. It is the same case in both DCT and DST. The probabilities are almost the same with some differences in watermarked image. In Abdel-Fattah El-Osarry’s image, the data is concentrated from 0 to 240 which are the same in DWT case. The probabilities for both images are almost alike. It is displayed in Fig. 7.

The spectrogram of the images is represented in Fig. 8. It figures the relation of frequencies with data contained in the image. For Ismail Yassen’s image, DCT and DST, there are some differences in middle data which is lower but still exist in Abdel Fattah El-Osarry and DWT case.

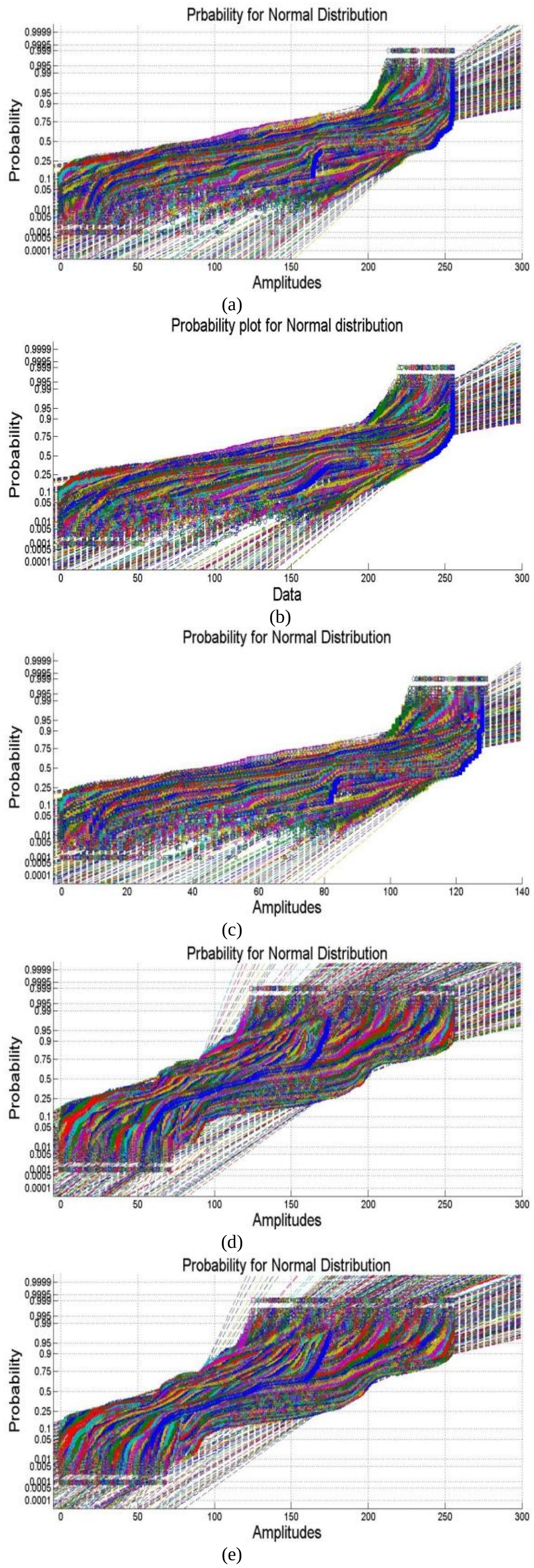


Fig. 7. The probability of the image (a) Ismail Yassen, (b) DCT watermarked image, (c) DST watermarked image, (d) Abdel-Fattah El-Osarry and (e) DWT watermarked image.

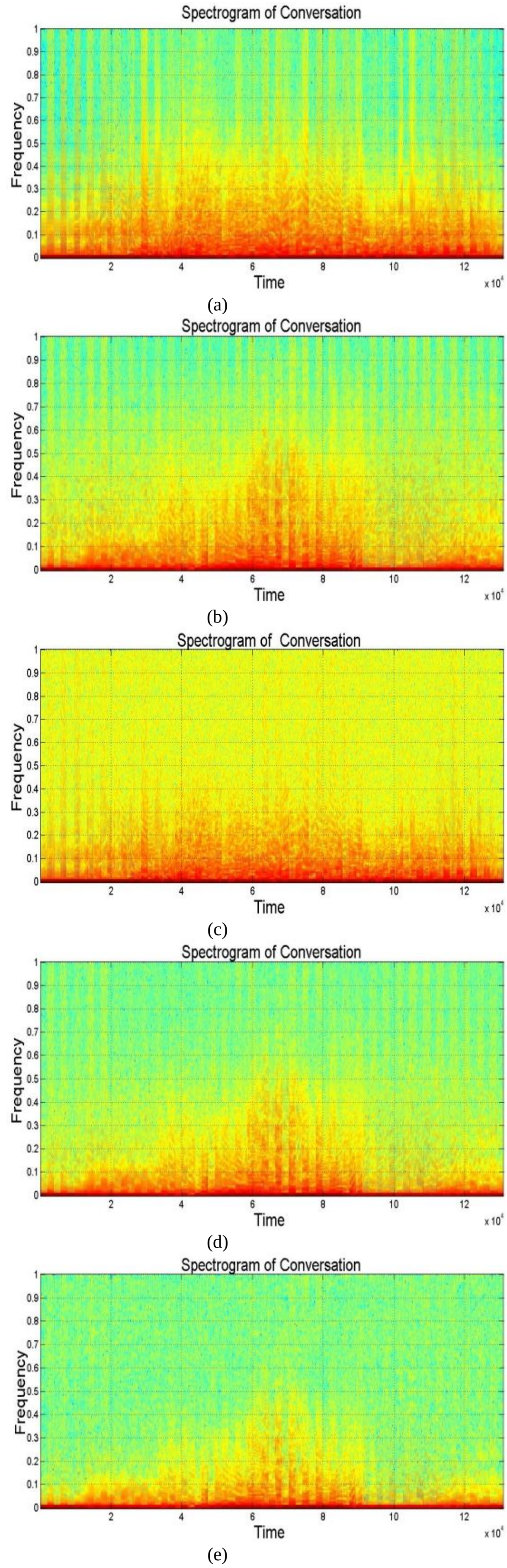


Fig. 8. The spectrogram of the image (a) Ismail Yassen, (b) Abdel-Fattah El-Osarry, (c) DCT watermarked image, (d) DST watermarked image and (e) DWT watermarked image.

Fig. 9 gives the power of images in each case. The power density is used to find out the band of the image and the power for each band. In) Ismail Yassen and DCT and DST images, the similarities are obvious in low frequencies but the differences are existing in high component. DST is more like the original than DCT. It is the same in Abdel-Fattah El-Osarry and DWT where both are almost the same with differences in high frequencies. Fig. 10 give the compared between time and frequencies domain. It can give the band of each case and the differences for all.

The distributions of the images are represented in Fig. 11. For Abdel-Fattah El-Osarry and DWT case, the distributions of both images are concentrated from 60 to 200 and it spread for whole the images. It is as seen is alike. Ismail Yassen and DST and DCT shows similarity between them and the data focus in high data from 170 to 250.

The scatter of the processed image with the original gives an indication for the correlation between them. Fig. 12 shows the scatter of the original image with each case. As shown, the correlation between them is very high and tends to 1.0. From these tests and Table. 1, it can be realized that DWT is more suitable transform than DCT and DST is the worst.

3. Extracting Process

In this case, the inserted image is extracted and the resulted is compared with the original to determine the best algorithm that suit the cloud and give high performance. Fig. 13 shows the extracted watermark where the DWT is more similar to original than DCT and DST is the lowest. The probability of watermark in both original and extracted for each case is given in Fig. 14. The data is concentrated on the low and high value of data for each image. In spectrogram test, it is obvious the differences in frequencies component for each case from the original watermark but has the same manner of distribution as seen in Fig. 15. The power density of each case can be detected from Fig. 16 where it can be distinguish the band of the images and as shown, the DWT is more like the original than other cases besides some changes in high frequencies. The comparison between time domain and frequency domain is presented in Fig. 17 where it can be detect the operating band of images and the differences between them. DWT is more like than others.

The distribution of each image is monitored in Fig. 18 where all data is concentrated in high value of image's data and DWT is still is the most like the original than other transform. The scatter plot gives an indication for the correlation between both the original watermark and the extracted one. All of them have low correlation as represented in Fig. 19. From all tests and Table. 1, it can be realized that DWT is more suitable transform than DCT and DST is the worst.

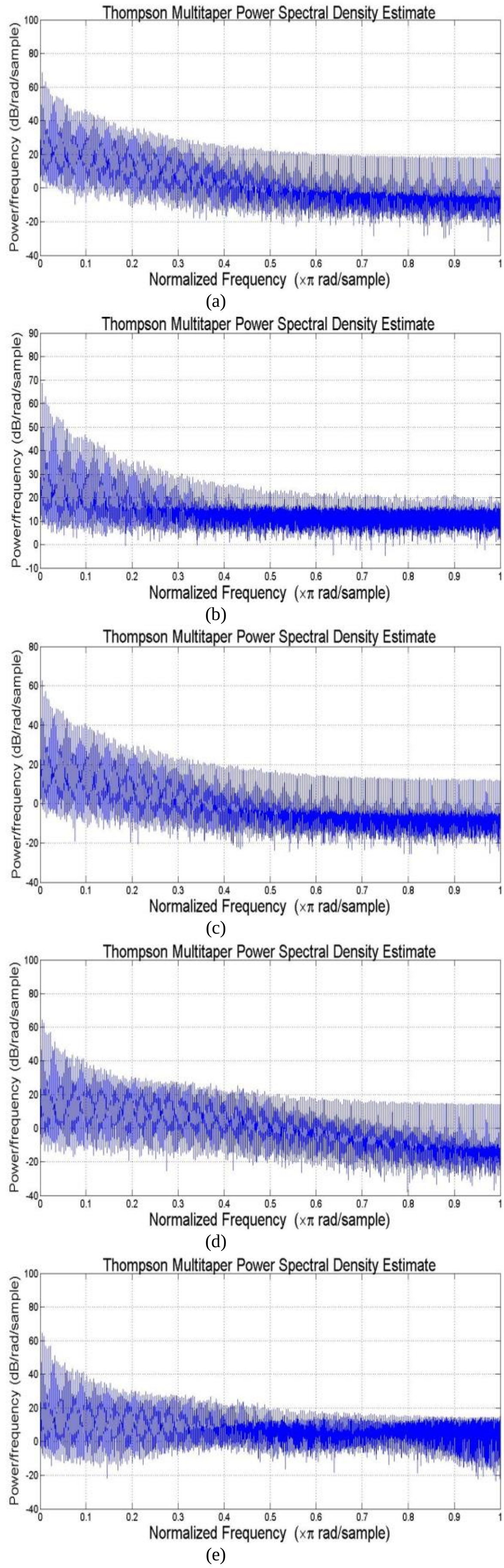
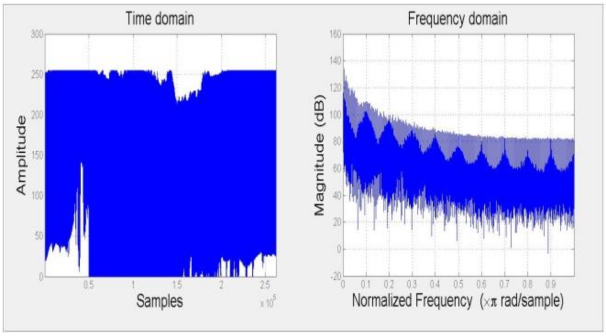
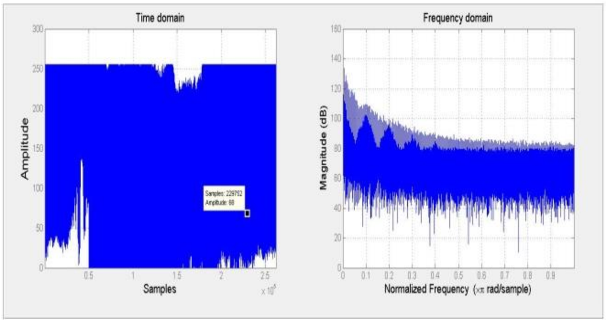


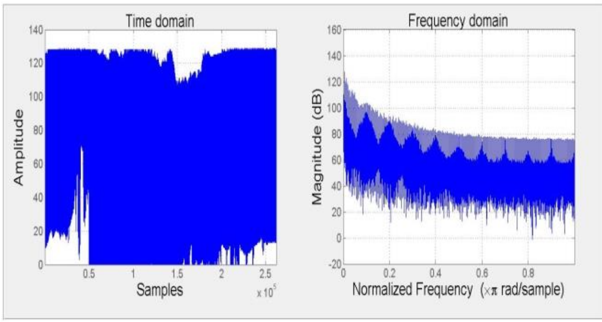
Fig. 9. The power of the image (a) Ismail Yassen, (b) DCT watermarked image, (c) DST watermarked image, (d) Abdel-Fattah El-Osarry and (e) DWT watermarked image.



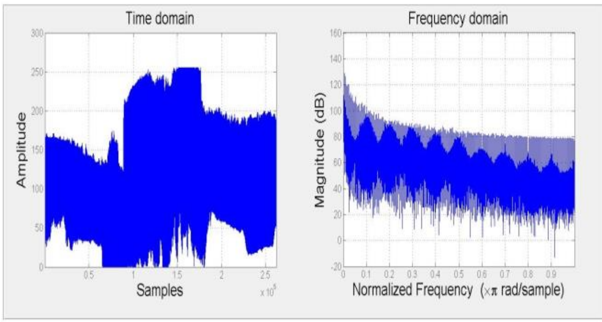
(a)



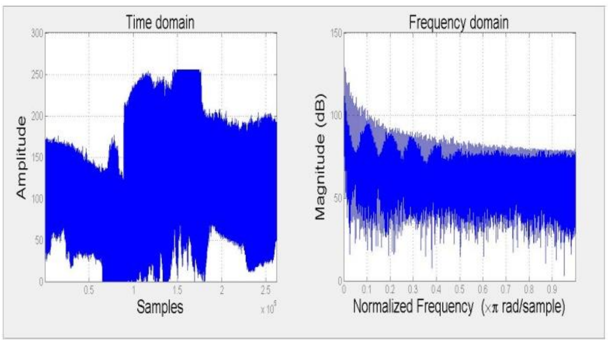
(b)



(c)

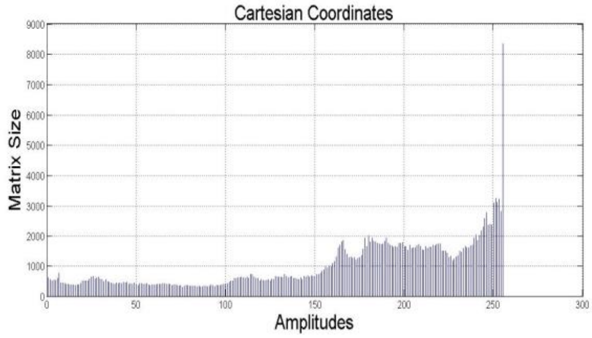


(d)

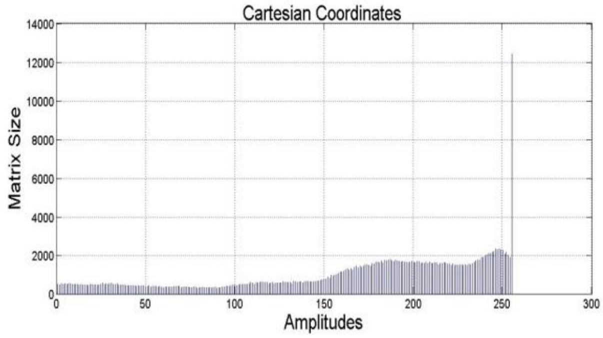


(e)

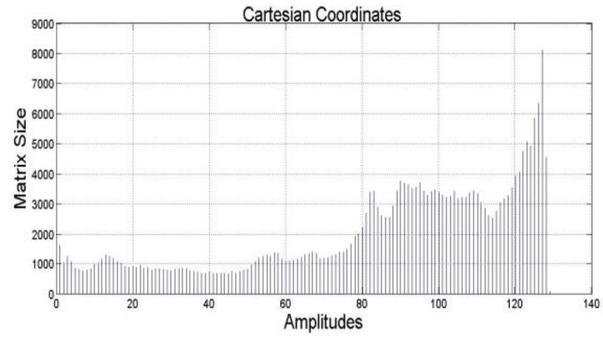
Fig. 10. The Time/Frequency domain of the image (a) Ismail Yassen, (b) DCT watermarked image, (c) DST watermarked image, (d) Abdel-Fattah El-Osarry and (e) DWT watermarked image.



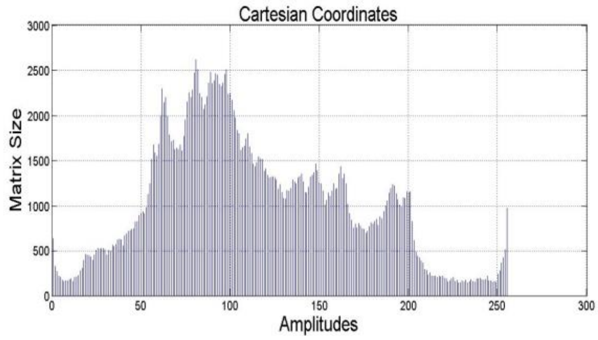
(a)



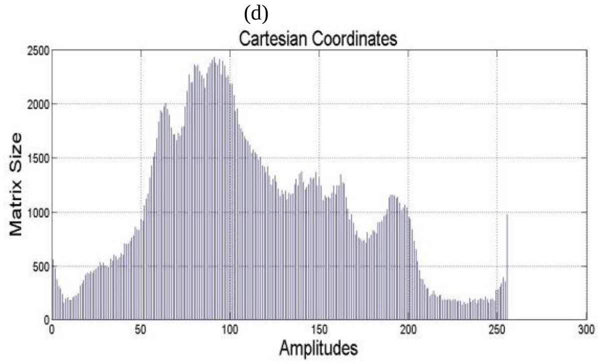
(b)



(c)

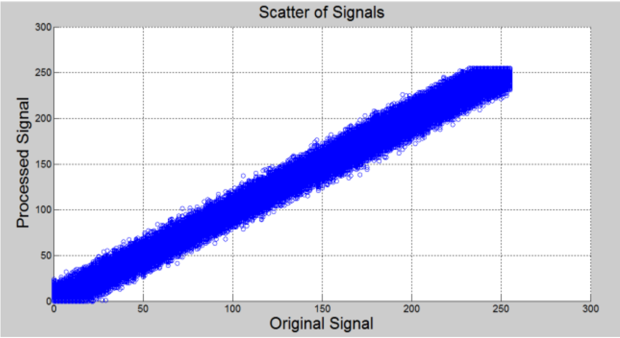


(d)

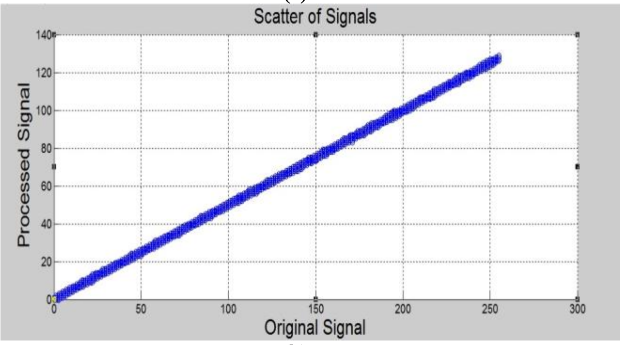


(e)

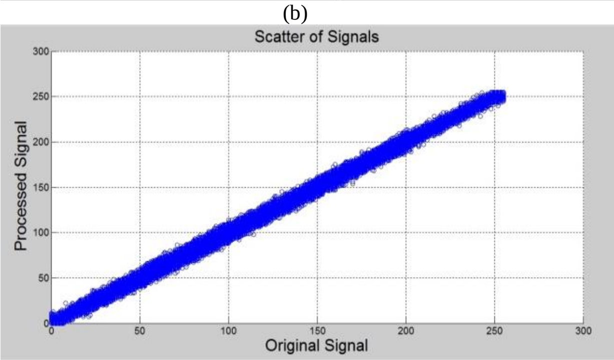
Fig. 11. The distribution of the image (a) Ismail Yassen, (b) DCT watermarked image, (c) DST watermarked image, (d) Abdel-Fattah El-Osarry and (e) DWT watermarked image.



(a)

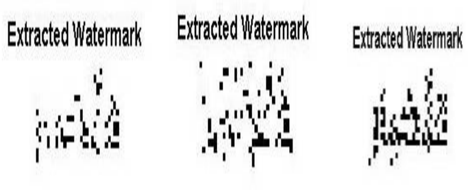


(b)



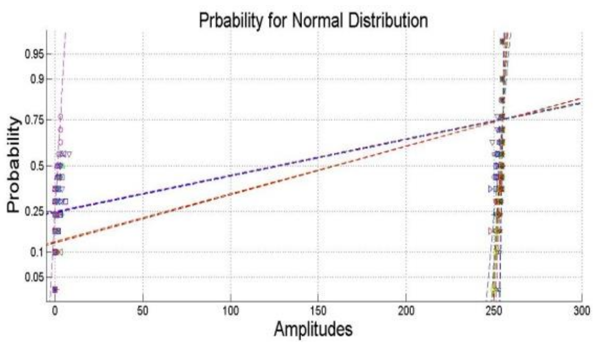
(c)

Fig. 12. The scatter of the original image with (a) DCT watermarked image, (b) DST watermarked image and (c) DWT watermarked image.

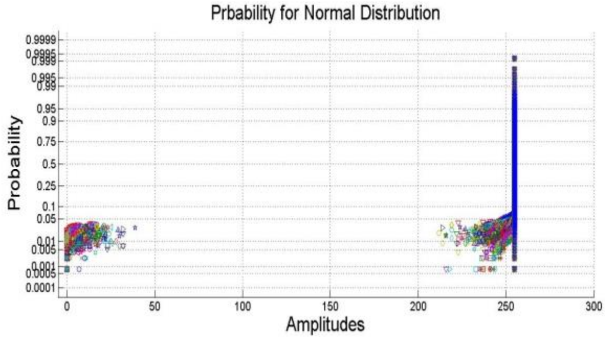


(a) (b) (c)

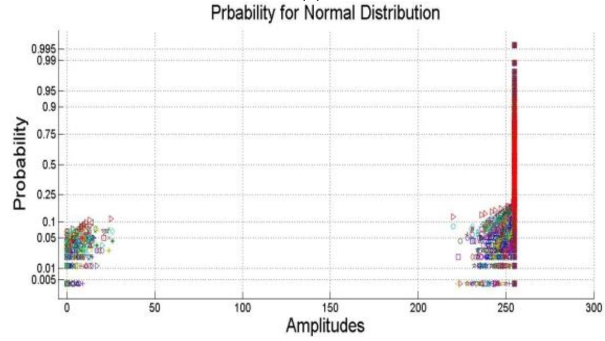
Fig. 13. The extracted watermark image that is used (a) DCT, (b) DST and (c) DWT.



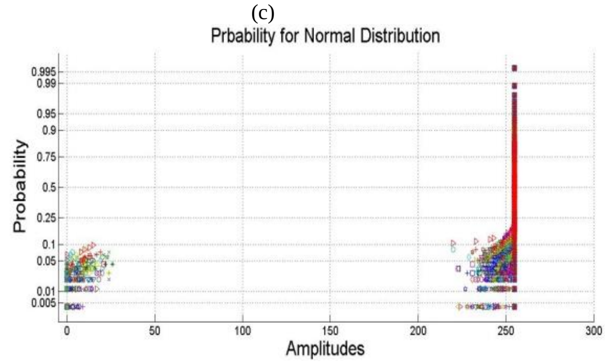
(a)



(b)



(c)



(d)

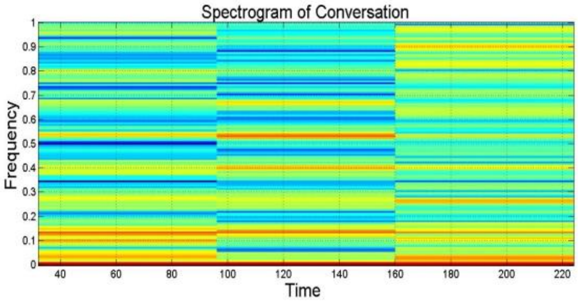
Fig. 14. The probability of watermark image in case of (a) original, (b) DCT, (c) DST and (d) DWT.

4. Attacks:

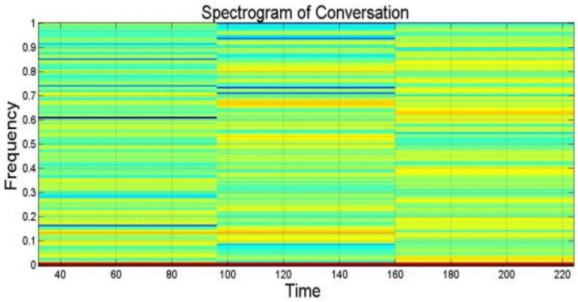
In the following sections, many attacks are applied to watermarked image and test the performance of the algorithm and the resulted image after extracted process. It is done to evaluate the robustness of each transforme aginst the attacks.

4.1 Gaussian Noise Attack:

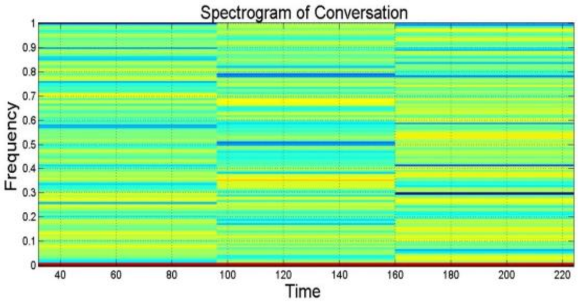
In this attack, the watermarked image is attacked by change the mean value of Gaussian noise with constant variance. In this test, variance is equal to zero. In Fig. 20, it shows the watermarked image after attack by change the mean. The change of watermarked image for each transformed are displayed and the details of the image disspeare largely by increase the value of Gaussian noise mean especially after the value of 0.5. The robustnees is more in DWT than DCT where DST is the lowest. In Fig. 21, the extracted watermark image is displayed in different case of mean for each transform. It displays the effect of Gaussian noise on the extracted watermark imge. The effects are monitored early in DCT and DST where it begin to recognize after mean of 0.5. The correlation between the original and the extracted image is produced in Fig. 22. From the above, it can be realized that DWT has great robustness than DCT and DST is the lowest. It is also the same manner for the correlation and detection of recovered image and extracted watermark. The range of correlation for DWT is higher than DCT and DST is varying across zero value.



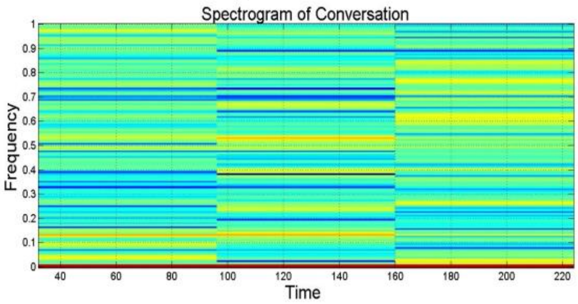
(a)



(b)

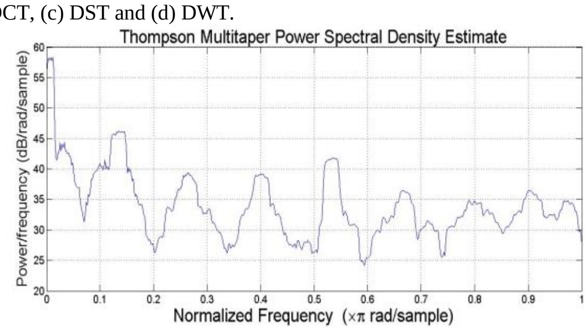


(c)

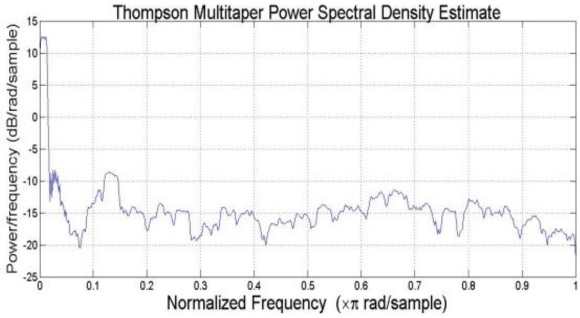


(d)

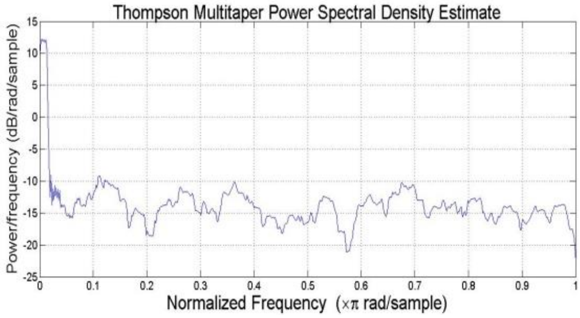
Fig. 15. The spectrogram watermark image in case of (a) original, (b) DCT, (c) DST and (d) DWT.



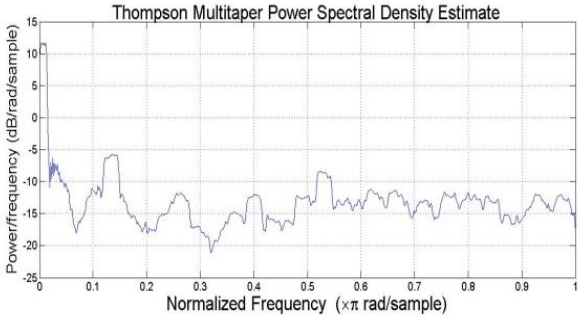
(a)



(b)



(c)



(d)

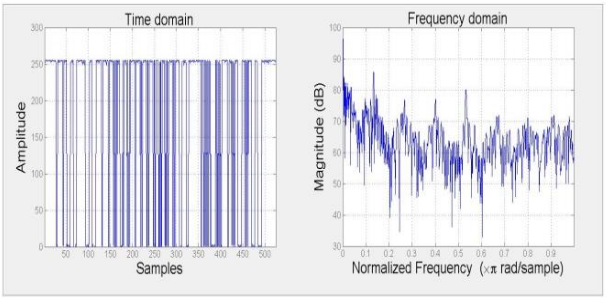
Fig. 16. The power of watermark image in case of (a) original, (b) DCT, (c) DST and (d) DWT.

4.2 Variance Attack:

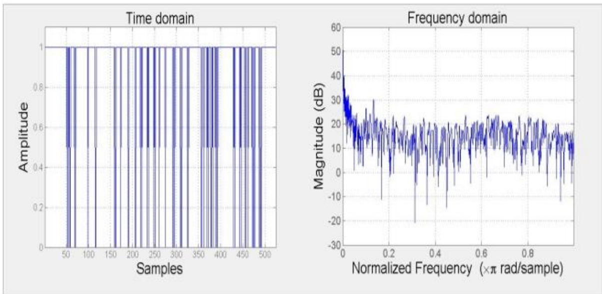
In this attack, the watermarked image is attacked by change the Variance value with constant mean. In this test, mean is equal to zero. In Fig .23, it shows the watermarked image after attack by change the variance. The effects appear for all transforms largely after varriance of 0.3 but DWT gives more effeciency than DCT and DST has bad resopne starting from lower value of varriance. In Fig. 24, the extracted watermark image is displayed in different case of variance. The effects are distinguished early starting from low value of varriance. The effects appear on all transform in noticeable way. The correlation between the original and the extracted image is produced in Fig. 25. From the above, it can be realized that DWT has great robustness than DCT and DST is the lowest. It is also the same manner for the correlation and detection of recovered image and extracted watermark. The range of correlation for DWT is higher than DCT and DST is varying across zero value.

4.3 Cropping Attack:

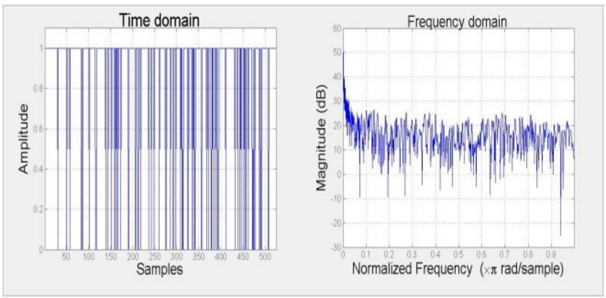
The watermark is embedded usually in linear manner, taking a square part of image may lead to damage a portion and so the recovery of watermark. It is due to damage of pixel result from remove a part of cover image a way. In this attack, the watermarked image is attacked by cut a part from the watermarked image then applies the extracted process. Many size of cropping is applied for this test. In Fig. 26, it shows the watermarked image after attack by change the block size of cropping. The detail of image disappear more by increase the block size of cropping. The large effects started after 256 of block size. In Fig. 27, the extracted watermark image is displayed in different case of cropping for all used transform. The effects of cropping appear early on both DST and DCT where DWT give more robustness. The effects start after block size of 256 The correlation between the original and the extracted image is produced in Fig. 28. From the above, it can be realized that DWT has great robustness than DCT and DST is the lowest. For all case, its correlation drop after block size of 256. DWT has high correlation and the extracted watermark is recognized where DCT has lower correlation and low detection of extracted watermark and DST is worst in both correlation and detection of extracted watermark.



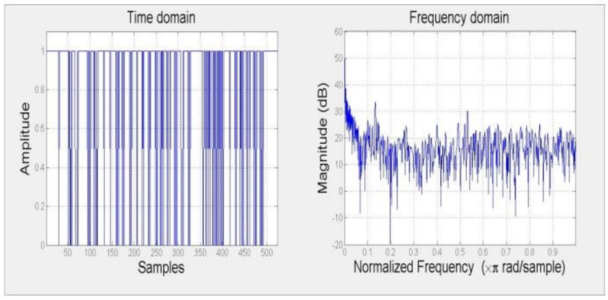
(a)



(b)

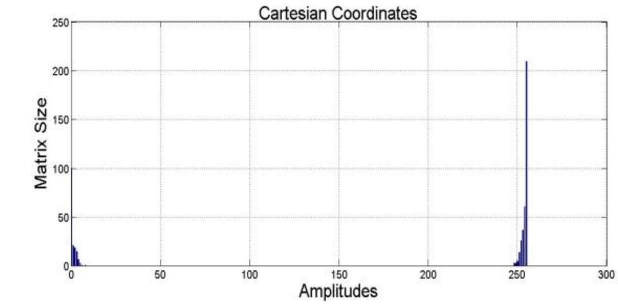


(c)

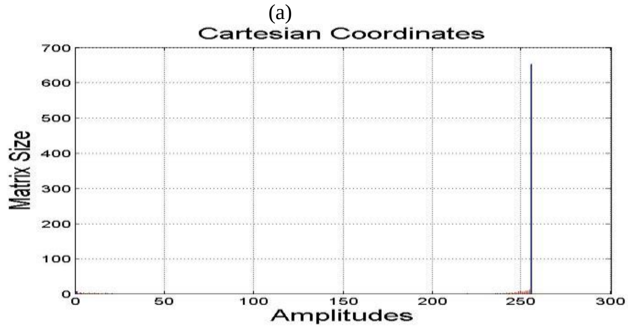


(d)

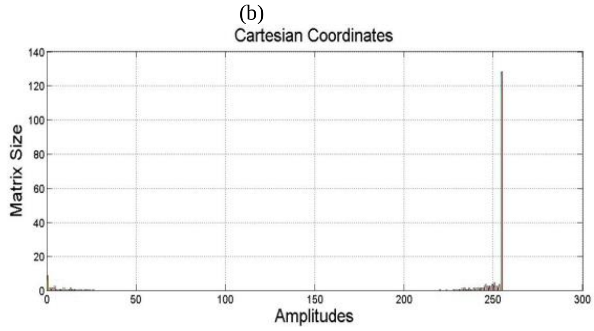
Fig. 17. The Time/Frequency domain of watermark image in case of (a) original, (b) DCT, (c) DST and (d) DWT.



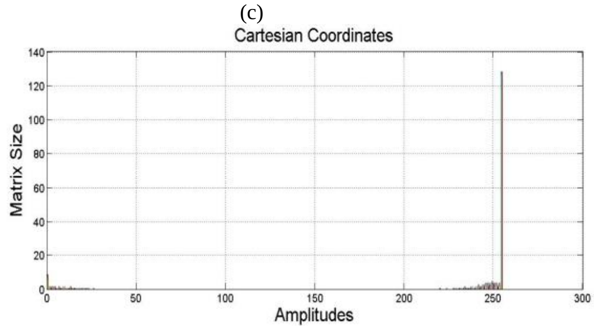
(a)



(b)

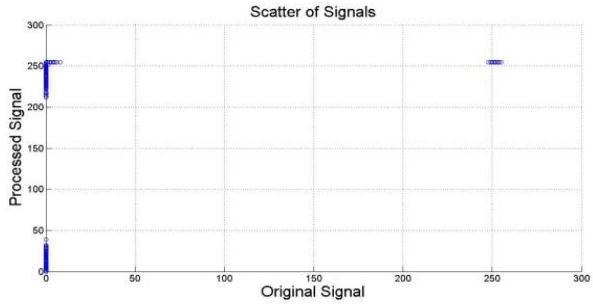


(c)

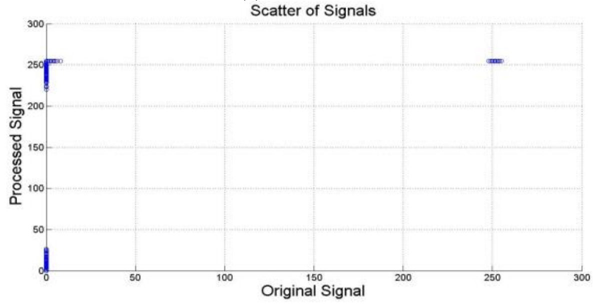


(d)

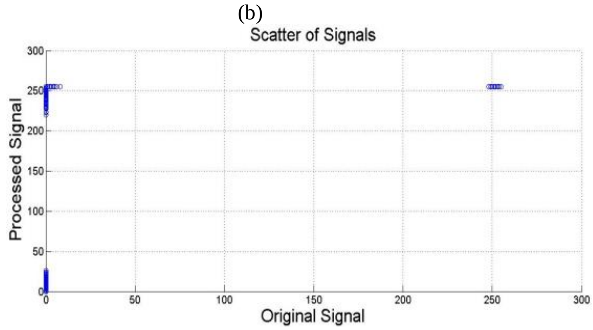
Fig. 18. The distribution of watermark image in case of (a) original, (b) DCT, (c) DST and (d) DWT.



(a)



(b)



(c)

Fig. 19. The scatter of the original watermark with (a) DCT extracted image, (b) DST extracted image and (c) DWT extracted image.

TABLE. 1
PSNR AND CORRELATION FOR WATERMARKED IMAGE IN DIFFERENT TRANSFORM.

Transform	Embedding		Extracting	
	PSNR	Correlation	PSNR	Correlation
DWT	+40.12 dB	0.9994	+ 9.02 dB	0.7141
DCT	+31.44 dB	0.9952	+ 6.07 dB	0.3767
DST	+ 8.85 dB	0.9999	+ 3.83 dB	0.0586

4.4 Compression Attack:

The image needs to be compressed to decrees the size for transmission or storage purpose. The operation destroys the pixel of the image that may be the watermark's pixel. In this attack, the watermarked image is compressed by many qualities and applies the extracted process. Different qualities levels are used to evaluate the performance of the algorithm. In Fig. 29, it shows the watermarked image after attack by change the quality. The effects on the appearance of the image is almost unnoticeable. The performance of each transform is similar to the others. In Fig. 30, the extracted watermark image is displayed in different case of quality. The effects for DCT appears where the extracted watermark started to distinguished after quality of 90%. For DWT, the extracted image is recognized after quality of 80% where the DST has bad response for this attack. The correlation between the original and the extracted image is produced in Fig. 31. From the above, it can be realized that DWT has great robustness than DCT and DST is the lowest. DWT give high correlation for quality of compression 80% where DCT give its high value after 90% of quality and DST give it at 98%. The range of correlation in DWT is higher than DCT and DST is around the zero value.

4.5 Rotation Attack:

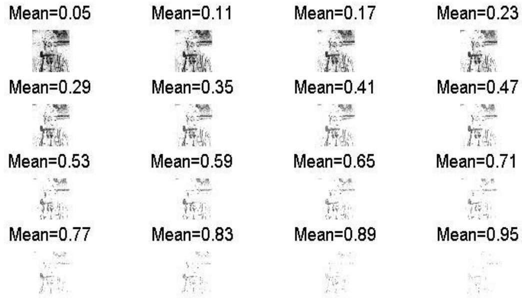
Rotation attack is the process of rotate the image by degree which distort the watermark as the original position is changed. In this attack, the watermarked image is attacked by rotating the image by certain angle. In Fig. 32, it shows the watermarked image after attack by change the rotation angle. It showes the image after ahhack for all used transforms. All of them can be recognized what ever the degree of rotation. In Fig. 33, the extracted watermark image is displayed in different case of rotation angle. The effects of rotation destroy the the extraction process. The extracted image become unrecognized for any degree of rotation except zero degree. It is due to the position change of image pixels. The correlation between the original and the extracted image is produced in Fig. 34. From the above, it can be realized that DWT has great robustness than DCT and DST is the lowest. For all case, any change in rotation angle causes high deterioration in the correlation but in the ideal case DWT has a high correlation. The range of correlation in DWT is higher than DCT and DST is around the zero value.

4.6 Gaussian Low Pass Filter (GLPF) Attack:

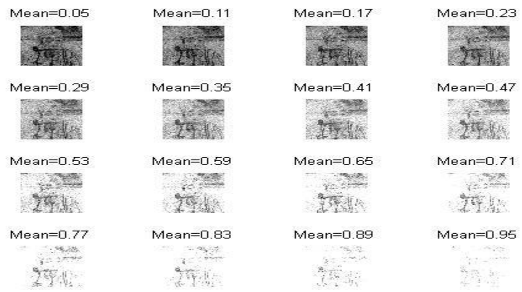
In this attack, the watermarked image is attacked by Gaussian smoothing the image. Gaussian smoothing operator is a 2D convolution operator used to smooth images and reduce the noise contained in an image. It uses a special kernel that represents the shape of a Gaussian, bell-shaped. The idea of Gaussian smoothing is to use this 2D distribution as a `point-spread function, and this is achieved by convolution. In Fig. 35, it shows the extracted image after attack by Gaussian smoothing. In Fig. 36, the extracted watermark image is displayed. From the above, it can be realized that DWT has great robustness; DCT and DST are the lowest. In DWT, the extracted watermark image can be recognized where in both DCT and DST it is undistinguishable

4.7 Blurring Attack:

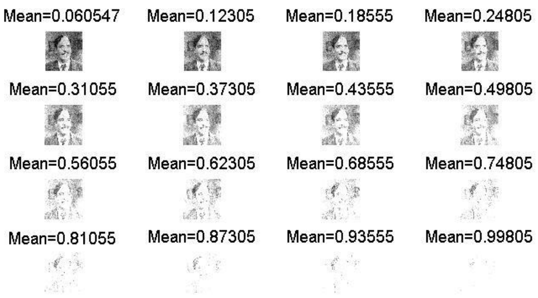
It is the smooth of the image. The smooth can be transited by averaging the pixel until to the hard edge and shaded area. In this attack, the watermarked image is attacked by blurring the image. Motion blurring attack with length is equal to 9 and theta equal to 10. In Fig. 37, it shows the extracted image after attack by blurring. In Fig. 38, the extracted watermark image is displayed. From the above, it can be realized that DWT has great robustness; DCT and DST are the lowest. In DWT, the extracted watermark image can be recognized where in both DCT and DST it is undistinguishable.



(a)

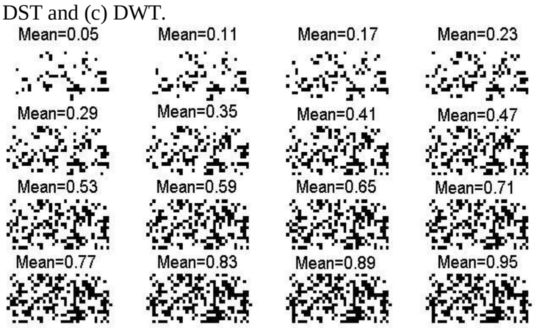


(b)

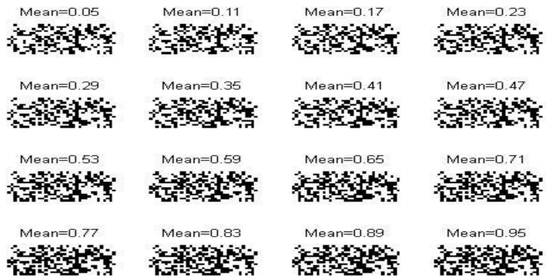


(c)

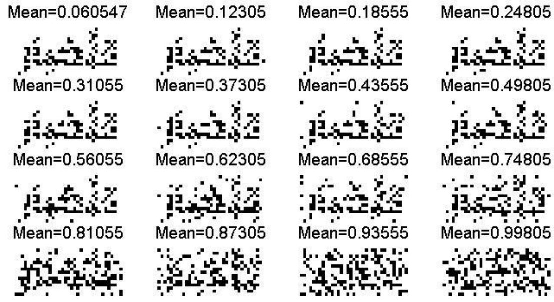
Fig. 20. The watermarked image after Gaussian Noise attack (a) DCT, (b) DST and (c) DWT.



(a)

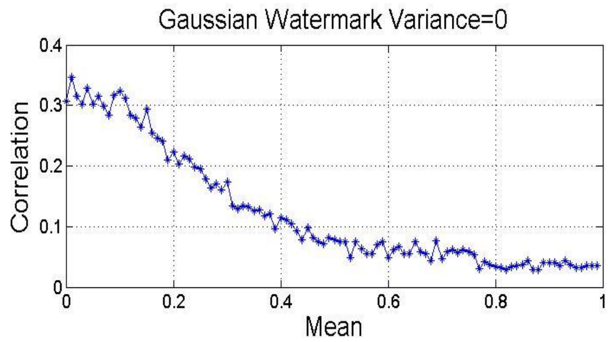


(b)

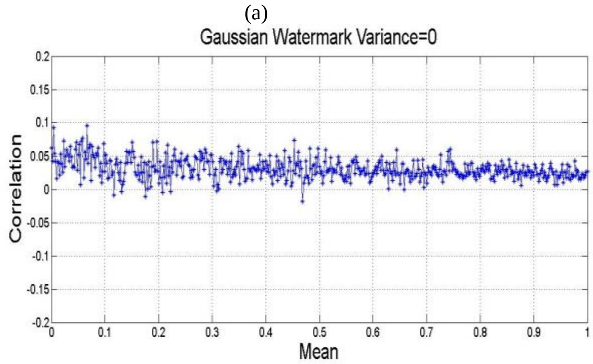


(c)

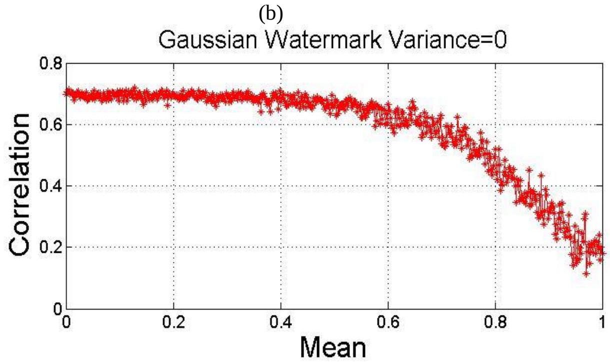
Fig. 21. The extracted watermark image after Gaussian Noise attack (a) DCT, (b) DST and (c) DWT.



(a)

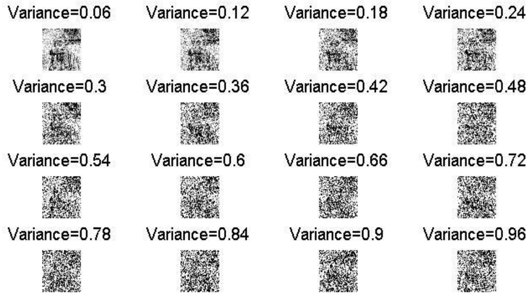


(b)

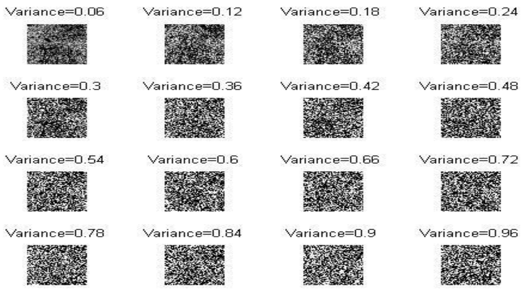


(c)

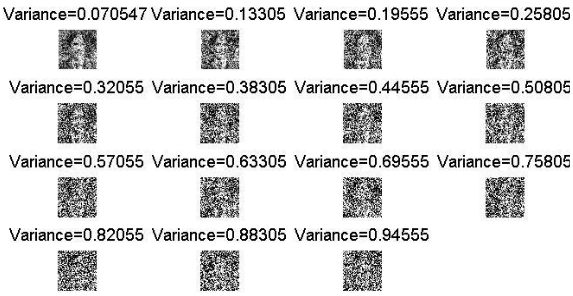
Fig. 22. The correlation coefficient versus mean for Gaussian Noise attack in case of (a) DCT, (b) DST and (c) DWT.



(a)

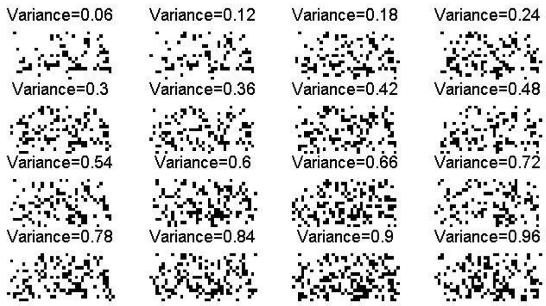


(b)



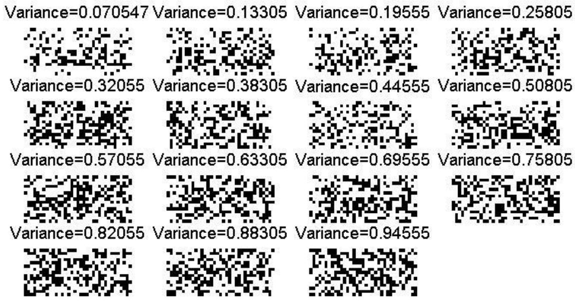
(c)

Fig. 23. The watermarked image after variance attack (a) DCT (b) DST(c) DWT.



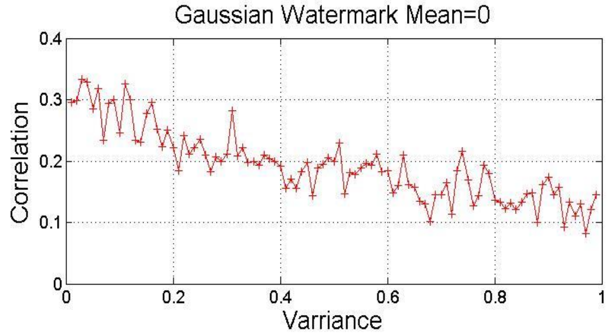
(a)

(b)

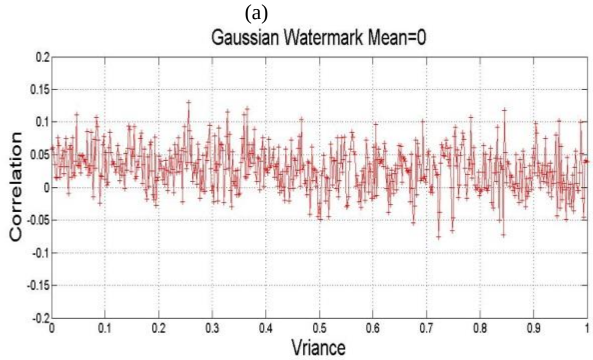


(c)

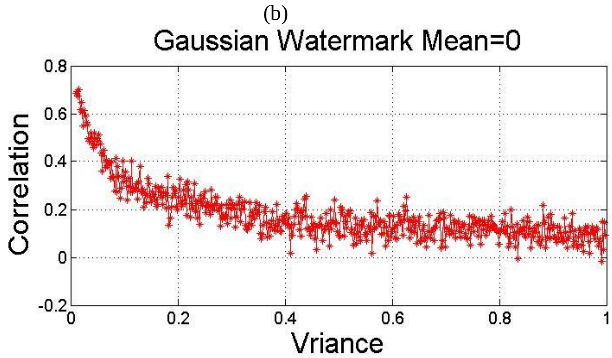
Fig. 24. The extracted watermark image after variance attack (a) DCT, (b) DST and (c) DWT.



(a)

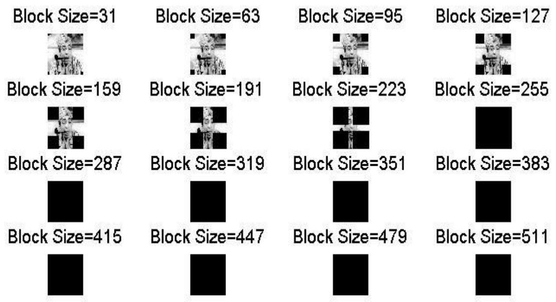


(b)

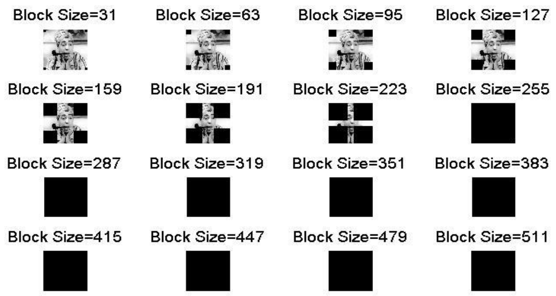


(c)

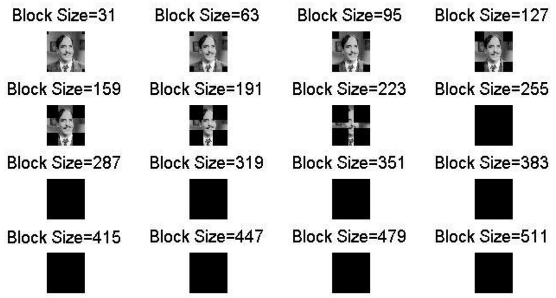
Fig. 25. The correlation coefficient versus variance in case of (a) DCT, (b) DST and (c) DWT.



(a)

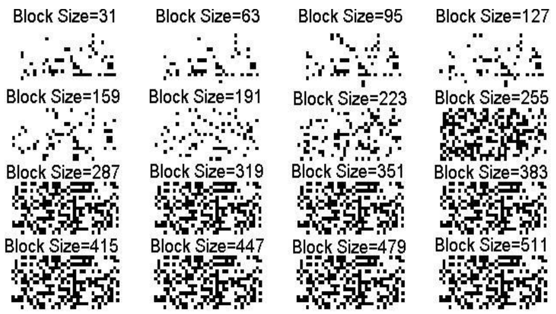


(b)

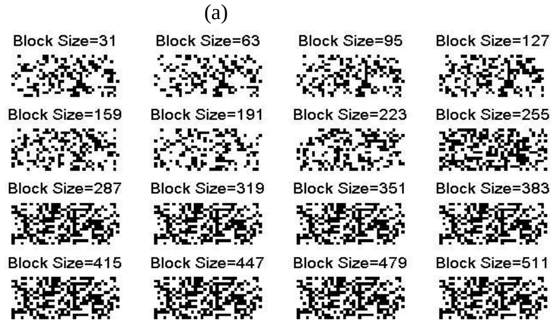


(c)

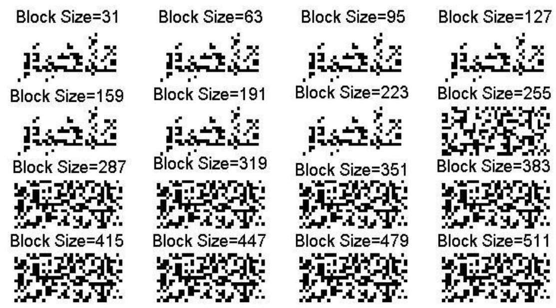
Fig. 26. The watermarked image after cropping attack (a) DCT, (b) DST and (c) DWT.



(a)

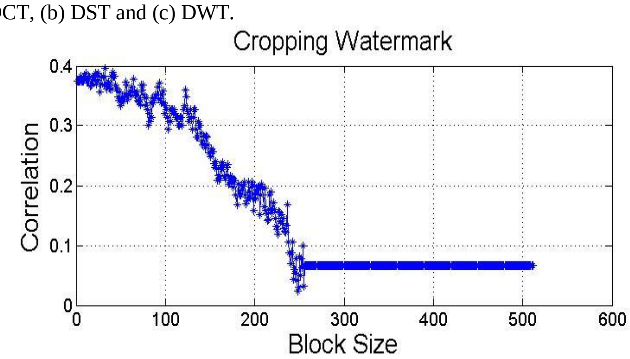


(b)

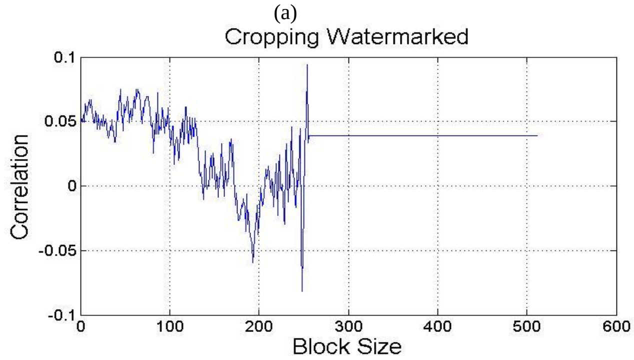


(c)

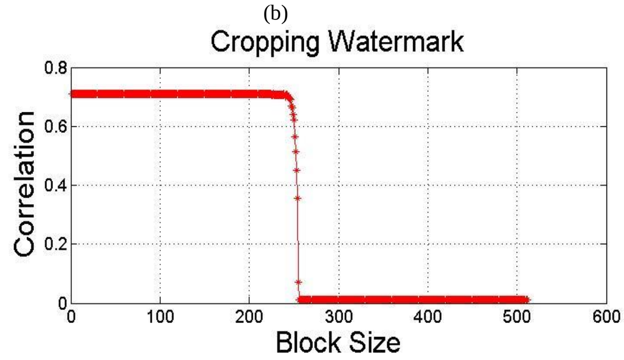
Fig. 27. The extracted watermark image after cropping attack (a) DCT, (b) DST and (c) DWT.



(a)

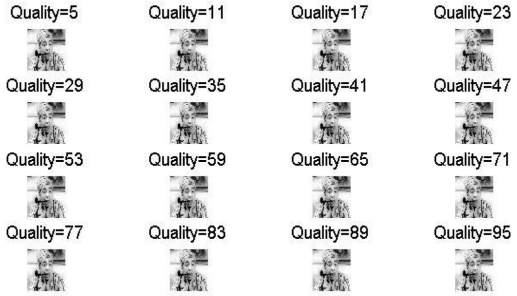


(b)

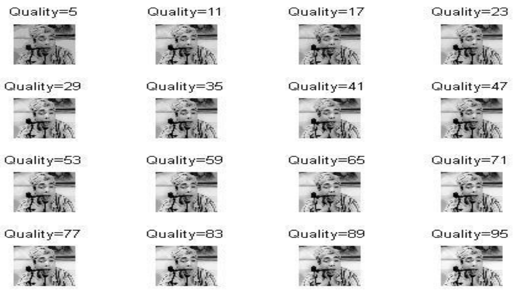


(c)

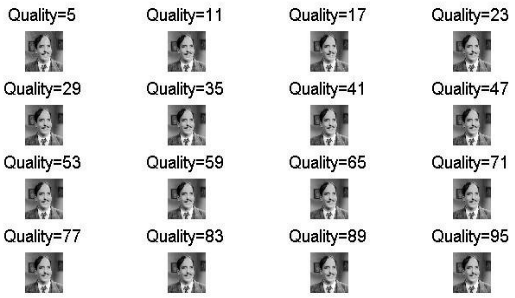
Fig. 28. The correlation coefficient versus block size cropping in case of (a) DCT, (b) DST and (c) DWT



(a)

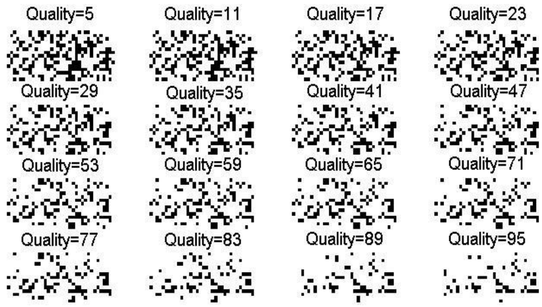


(b)

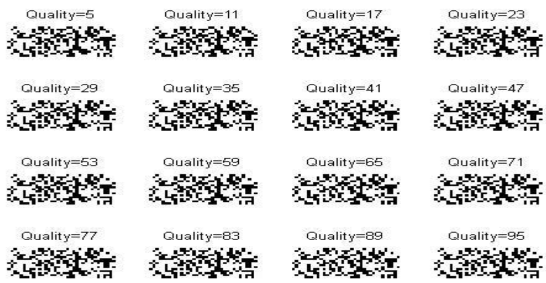


(c)

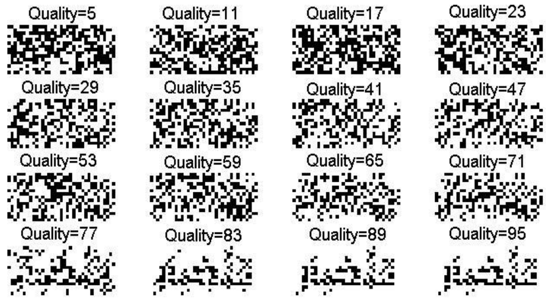
Fig. 29. The watermarked image after compression attack (a) DCT, (b) DST and (c) DWT.



(a)

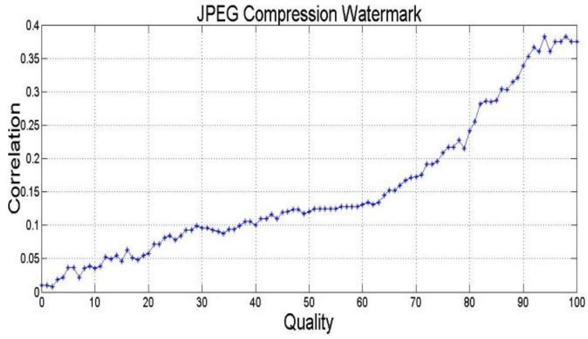


(b)

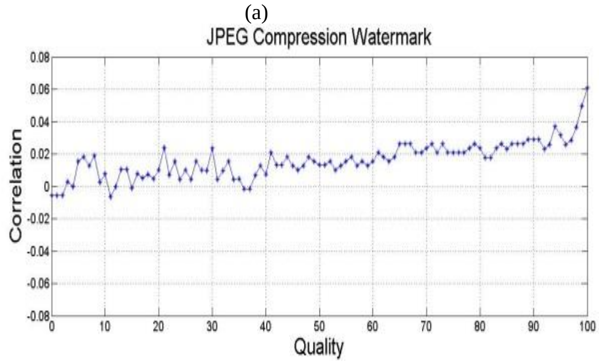


(c)

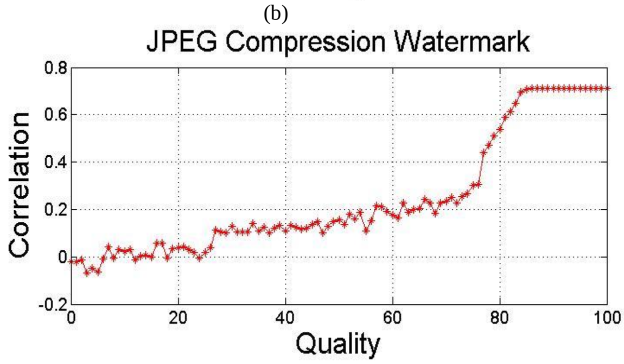
Fig. 30. The extracted watermark image after compression attack (a) DCT, (b) DST and (c) DWT.



(a)

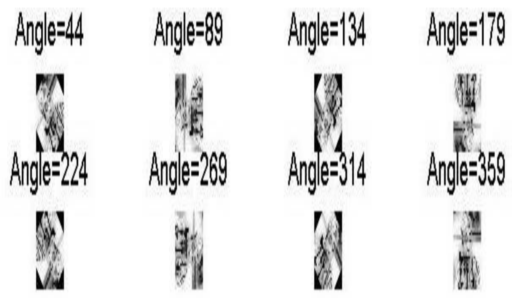


(b)

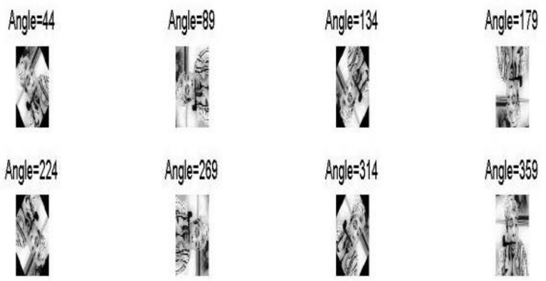


(c)

Fig. 31. The correlation coefficient versus compression quality in case of (a) DCT, (b) DST and (c) DWT.



(a)

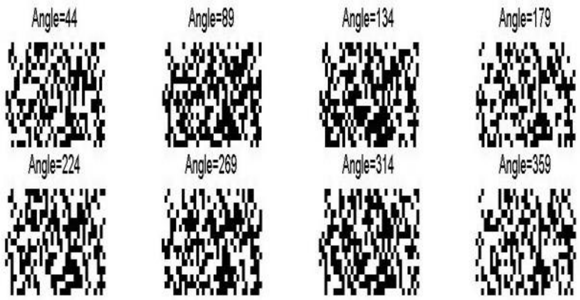


(b)

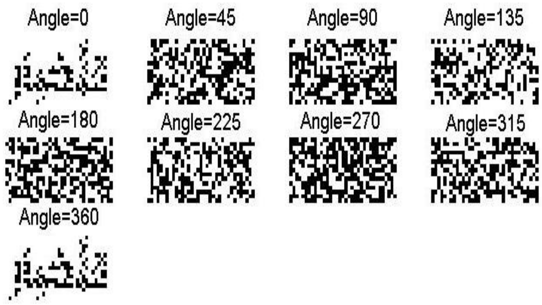
(c)

Fig. 32. The watermarked image after rotation attack (a) DCT, (b) DST and (c) DWT.

(a)

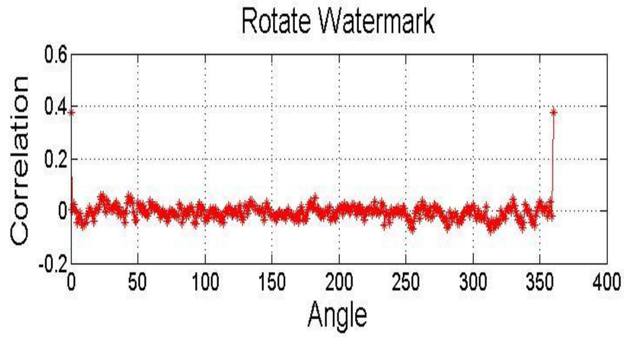


(b)

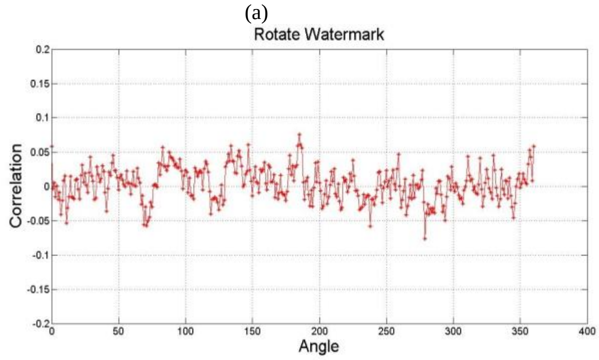


(c)

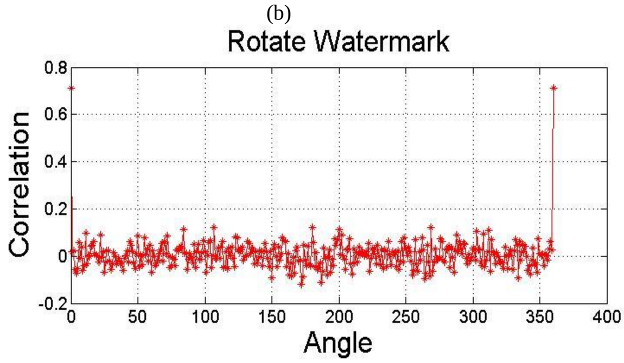
Fig. 33. The extracted watermark image after rotation attack (a) DCT, (b) DST and (c) DWT.



(a)



(b)



(c)

Fig. 34. The correlation coefficient versus rotation angle in case of (a) DCT, (b) DST and (c) DWT.

4.8 Sharpening Attack

In this attack, the watermarked image is attacked by sharpening the image. Sharpening spatial filters are used to highlight fine detail in an image or to enhance detail that has been blurred, either in error or as a natural effect of a particular method of image acquisition. In Fig. 39, it shows the extracted image after attack by Sharpening. In Fig. 40, the extracted watermark image is displayed. From the above, it can be realized that DWT has great robustness than DCT and DST is the lowest. For DWT, it can be recognized the watermark image clearly but in DCT it little difficult to recognized and in DST it is undistinguishable.

(a)

(b)

(c)

Fig. 35. The extracted image after GLPF attack (a) DCT, (b) DST and (c) DWT.

(a)

(b)

(c)

Fig. 36. The extracted watermark image after GLPF attack (a) DCT, (b) DST and (c) DWT.

(a)

(b)

(c)

Fig. 37. The extracted image after Blurring attack (a) DCT, (b) DST and (c) DWT.

(a)

(b)

(c)

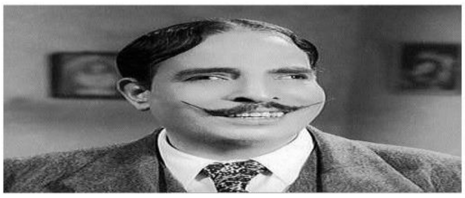
Fig. 38. The extracted watermark image after Blurring attack (a) DCT, (b) DST and (c) DWT.

4.9 Median Filtering Attack:

It is the reduction noise in image by blending the brightness pixel within a selection. The filter searches the radius of a pixel that a lifer tool much from adjacent pixel and replace the enter pixel with medium brightness value of searched pixel. In this attack, Median Filtering the image attacks the watermarked image. It is well known that in a set of ordered values, the median is the central value. Median filtering reduces blurring of edges. The idea is to replace the current point in the image by the median of the brightness in its neighborhood. In Fig. 41, it shows the extracted image after attack by Gaussian smoothing. In Fig. 42, the extracted watermark image is displayed. From the above, it can be realized that all transforms have bad response to median filter attack where it cannot be recognized the extracted watermark image.

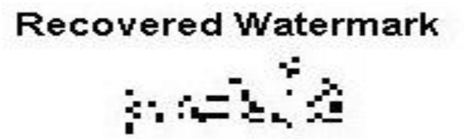
(a)

(b)



(c)

Fig. 39. The extracted image after Sharpening attack (a) DCT, (b) DST and (c) DWT.



(a)

(b)

(c)

Fig. 40. The extracted watermark image after Sharpening attack (a) DCT, (b) DST and (c) DWT.

(a)

(b)

(c)

Fig. 41. The extracted image after Median Filtering attack (a) DCT, (b) DST and (c) DWT.

(a)

(b)

(c)

Fig. 42. The extracted watermark image after Median Filtering attack (a) DCT, (b) DST and (c) DWT.

IV. CONCLUSION

As seen from the results, DWT has a good response for most of attacks and high performance than other transform. It is more convenient for this cloud application. The DST has bad response and low imperceptibility and for most of attacks, it fails to pass these attacks and stand against. DCT has a good imperceptibility but in some attack it fails and in other it pass. The best value for embedding factor is K=1. The correlation and PSNR for these value is counted and high performance of is distinguishable. All these transform based on FracFT are used to provide services to all AuthGs and insure the security of the content belongs to ERTU. The several tests are used to evaluate the performance of each transform and which one can handle various situations of AuthGs whatever the location. these tests are deployed for different situation of attacks from human or transmitters cannel condition as well. This is done using web-based application to provide the security for the AuthGs and then the contents of ERTU within the cloud.

REFERENCES

[1] Ammar Odeh, Aladdin Alzubi, Qassim Bani Hani and Khaled Elleithy, ' Steganography by Multipoint Arabic Letters', Systems, Applications and Technology Conference (LISAT), 2012 IEEE Long Island, 2012 , pp(1 – 7).

[2] Frank Hartung and Friedhelm Ramme, "Digital Management and Watermarking of Multimedia content for M-Commerce Applications", Vol. 38, No. 11, November 2000, pp(87-84).

[3] Li Zhang and Bing Tang, 'A Combination of Feature-Points-Based and SVD-Based Image Watermarking Algorithm', 2012 International Conference on Industrial Control and Electronics Engineering, pp. (1092-1095).

[4] Md. Iqbal H. Sarker and M. I. Khan, 'An Improved Blind Watermarking Method in Frequency Domain for Image Authentication', International Conference on Informatics, Electronics & Vision (ICIEV), 17-18 May 2013, pp. 1 – 5.

[5] Jordi Nin and Sergio Ricciardi,'Digital Watermarking Techniques and Security Issues in the Information and Communication Society', 27th International Conference on Advanced Information Networking and Applications Workshops, 25-28 March 2013, pp. 1553 – 1558.

[6] Reza Mehdi Hadi and Peyman Ayubi, 'Blind Digital Image Watermarking Based on CT-SVD and Chaotic Cellular Automata', IEEE 2012, pp. (301-306).

[7] Soo-Chang Pei and Min-Hung Yeh, 'Two Dimensional Discrete Fractional Fourier Transform' Signal Processing 67 (1998), pp(99-108).

[8] Hameed Al-Qaheri, Abhijit Mustafi and Soumya Banerjee, 'Digital Watermarking using Ant Colony Optimization in Fractional Fourier Domain' Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 3, July 2010 pp(179 – 189).

[9] Ensherah A. Naeem1, Mustafa M. Abd Elnaby, and Mohiy M. Hadhoud. ' Chaotic Image Encryption in Transform Domains', IEEE 2009, pp(71-76).

[10] M. Sharkas, B. Youssef and N. Hamdy, 'AN ADAPTIVE IMAGE-WATERMARKING ALGORITHIM EMPLOYING THE DWT', The 23rd National Radio Science Conference, March 2006.

[11] Chi-Kwong Chan and L.M. Cheng, 'Hiding data in images by simple LSB substitution', Pattern Recognition Society, 2004, pp(469-474).

[12] RAYMOND B. WOLFGANG, CHRISTINE I. PODILCHUK and EDWARD J. DELP, ' Perceptual Watermarks for Digital Images and Video', PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999, pp. (1108-1126).

Salwa M. Serag Eldin, Electronics and Electrical Communication Engineering Dept., Tanta University, Dr, IEEE member sserag@gmail.com.

Salah A. Khamis, Electronics and Electrical Communication Engineering Dept., Tanta University, Assistant Professor, IEEE member, s.khamis@f-eng.tanta.edu.eg.

Prof. Abdel-Aziz Ibrahim Mahmoud HASSANIN, Electronics and Electrical Communication Engineering Dept., Faculty of Electronic Engineering, Menufia University, IEEE member, abdel_aziz_hassanin@hotmail.com.

Mohammed A. Alsharqawy, Egyptian Radio and Television Union (ERTU), IEEE member, mnm_1946@hotmail.com.