Image Encryption using the Dual Transformation Technique with Random Phase Encoding

Prakash Chandra Bharti
P. G. Student
JUET Guna, (MP), INDIA

Ashutosh
P. G. Student
JUET Guna, (M.P.), INDIA

ABSTRACT
In this paper, a new method has been presented by which an image can be effectively encrypted. Image encryption is a method of encoding a message so that eavesdroppers cannot read the information, only the authorized person can be able to decode the message. In this paper dual transformation is being used one is discrete wavelet transform (DWT) and another is the discrete Fourier transform (DFT). Instead of using Discrete Fourier transform twice different transform is used so that is can be more secure. Before the application of transform, a random phase encoding is done on the image signal by generating a random phase matrix between some range. It is very useful in secure multimedia communication.

General Terms
Image Encryption, Cryptography, Encoding.

Keywords
Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Random Phase Encoding.

1. INTRODUCTION
Image encryption is necessary nowadays everyone wants security. In defense sector and in research sector security is a prime concern. For the multimedia data it is very important that the information data is retained means that the decrypted image should be as same as the original image. Discrete wavelet transform has very interesting property that it separates the different frequency component. For the separation of different frequency component filter banks [1-2] are used. The filter bank structure is shown below:

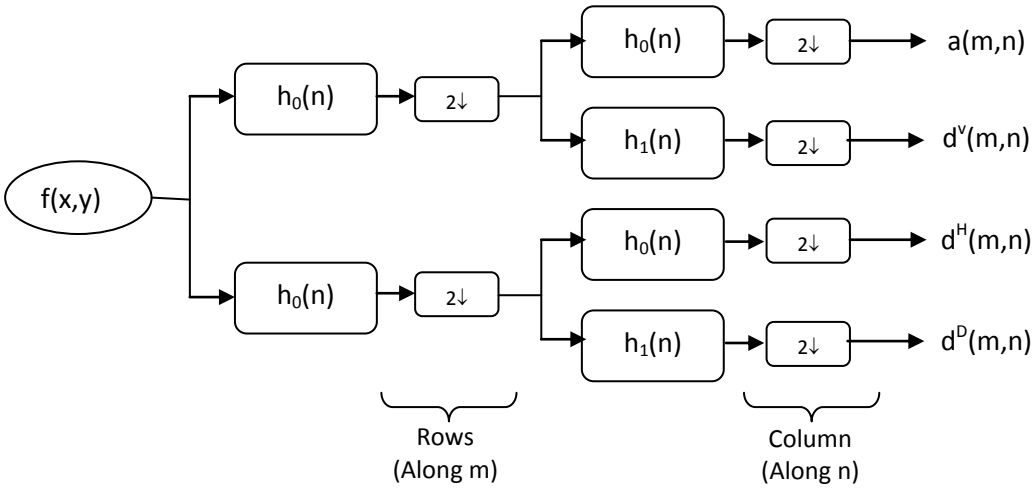


Figure 1: Filter bank for wavelet decomposition.

In DWT of an image first apply the transform [1-3] row wise then the image is separated into low and high frequency respectively the function for wavelet decomposition of the image is shown below for one dimensional signal:

$$f \rightarrow (a^L | d^L)$$

$$a^L = (a_1, a_2, a_3, \dots \dots a_{N/2})$$

$$d^L = (d_1, d_2, d_3, \dots \dots d_{N/2})$$

Where L is the decomposition level, **a** is the approximation sub-band and **d** is the detail sub-band.

$$a_m = \frac{f_{2m} + f_{2m-1}}{\sqrt{2}} \qquad for\ m = 1,2,3, \dots \dots, N/2$$

$$d_m = \frac{f_{2m} - f_{2m-1}}{\sqrt{2}} \qquad for\ m = 1,2,3, \dots \dots, N/2$$

For example, if f={f_1,f_2,f_4,f_5,f_6,f_7,f_8} is a time – signal of length 8, then the HWT decomposes f into an approximation sub-band containing the low frequencies and the detail sub-band containing the high frequencies:

$$Low = a = \{f_2 + f_1, f_4 + f_3, f_6 + f_5, f_8 + f_7\}/\sqrt{2}$$

$$High = d = \{f_2 - f_1, f_4 - f_3, f_6 - f_5, f_8 - f_7\}/\sqrt{2}$$

To apply HWT on images, we first apply a one level Haar wavelet to each row and secondly to each column of the resulting "image" of the first operation. The resulted image is decomposed into four sub-bands: LL, HL, LH and HH sub-bands. (L = low and H = high). The LL sub-band contains an approximation of the original image

while the other sub-band contain the missing details. The LL sub-band output at any stage can be decomposed further.
The Inverse Haar Wavelet is computed in the reverse order as follows:

$$f = (\frac{a_1 - d_1}{\sqrt{2}}, \frac{a_2 + d_2}{\sqrt{2}}, \dots \dots \frac{a_{N/2} - d_{N/2}}{\sqrt{2}}, \frac{a_{N/2} + d_{N/2}}{\sqrt{2}})$$

To apply IHWT on images, we first apply a one level inverse haar wavelet to each column and secondly to each row of the resulting "Image" of the first operation.

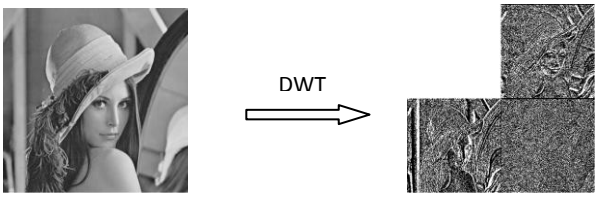


Figure 2: Wavelet transform of a grayscale image.

The discrete Fourier transform [4-6] of a sequence {u (n), n=0,……..,N-1} is defined as follows:

$$v(k) = \sum_{n=0}^{N-1} u(n) W_N^{kn}, \qquad where\ k = 0,1, \dots \dots \dots N-1$$

Where,

$$W_N \triangleq exp\left\{\frac{-j2\pi}{N}\right\}$$

The inverse transformation is given by:

$$u(n) = \frac{1}{N} \sum_{k=0}^{N-1} v(k) W_N^{-kn}, \qquad n = 0,1, \dots \dots N-1$$

The above pair of equations is not scaled properly to be unitary transformation. Which is defined as follows:

$$v(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} u(n) W_N^{kn}, \qquad k = 0,1, \dots \dots N-1$$

$$u(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} v(k) W_N^{-kn}, \qquad n = 0,1, \dots \dots N-1$$

The unitary DFT matrix F is given below:

$$F = \left\{\frac{1}{\sqrt{N}} W_N^{kn}\right\}, \quad 0 \le k, n \le N-1$$

For image 2D Discrete Fourier transform [1-2] can be applied the formula for the 2D transformation is given below:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) exp^{-j2\pi(ux/M + vy/N)}$$

Where, f(x,y) is image signal, M, N are the dimensions of the image.

The inverse 2D Discrete Fourier Transform is given below:

$$f(x,y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) exp^{j2\pi(ux/M + vy/N)}$$

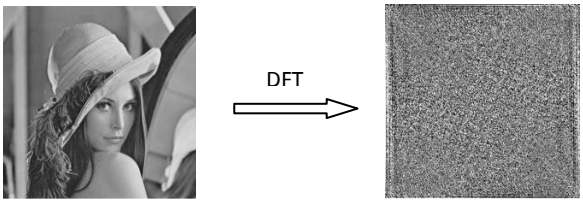


Figure 3: Wavelet transform of grayscale image.

2. PROPOSED ENCRYPTION TECHNIQUE

The proposed encryption technique is a dual transformation with random phase encryption technique. In this two different transform has been used. The whole encryption process is divided into two steps. In first step one transformation is applied i.e. first wavelet transform is applied, after that second transform i.e. Discrete Fourier Transform is applied. The block diagram of the encoding process is given below:

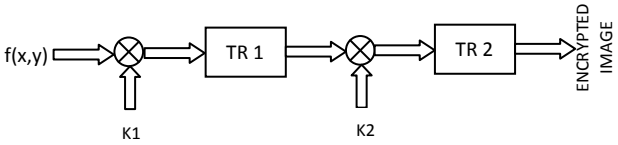


Figure 4: Dual Transform Encryption Process

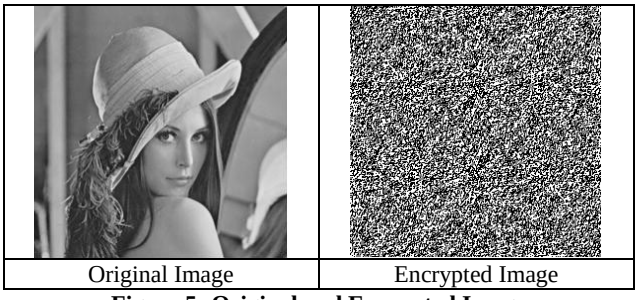
In both the stages before the application of transform, the random phase [5] is multiplied with the image. The random phase matrix is generated as given, let [exp(jα(n,m))] and [exp(jβ(n,m))] are two random phase matrix of same dimension as that of the image matrix dimension i.e. N * M where α(n,m) and β(n,m) are uniformly distributed between [0-4π] and [0-2π] and n,m ranging 1<=n<=N, 1<=m<=M. α(n,m) and β(n,m) are not dependent on each other.

$$K_1=[exp(j\alpha(n,m))] \ , \ K_2=[exp(j\beta(n,m))]$$

Mathematical formulation for encryption are as follows:

$$E = FFT\ [[DWT\ [I * K_{1]}] * K_{2]}$$

Where, E is encrypted image, I is the original image and K_1, K_2 are random phase matrix.



Original Image	Encrypted Image

Figure 5: Original and Encrypted Image

3. PROPOSED DECRYPTION TECHNIQUE

The proposed decryption technique is just reverse of that of the encryption process. First apply the inverse transform which was applied in second step in the encryption process.

After that random phase decoding. Then apply inverse transformation of the first transform applied which was applied in the encryption process. Then random phase decoding has been done on the image, after that the image recovered is the decrypted image. The block Diagram of the decryption process is shown below:

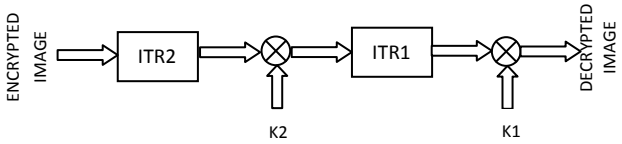
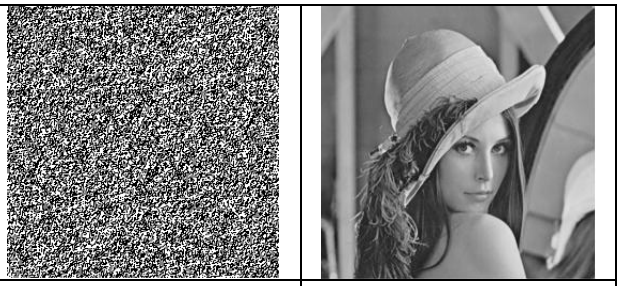


Figure 6: Dual Transform Decryption Process

The random phase decoding is done with the help of same random phase matrix which was used at the time of encoding the image. The mathematical formulation of decryption process is shown below:

$$D = [IDWT\ [IFFT\ [E]/\ K_{1}]]\ /\ K_2]$$

Where, D is decrypted image, E is received encrypted image, K_1 and K_2 are the random phase matrix.



Encrypted Image	Decrypted Image

Figure 7: Encrypted Image and Decrypted Image

4. ERROR METRIC/QUALITY COMPARISION METRIC

In this section error metric has been presented by which the quality of image can be compared. It is basically finding the similarity between the original image and the recovered image. There are various calculation involved in the quality comparison like calculation of [7-8] mean squared error (MSE), signal to noise ratio (SNR), peak signal to noise ratio (PSNR).

i) Mean Squared Error (MSE): It is the measure of similarity by calculating the error signal by taking the difference of original and recovered image and taking squared average of it.

$$MSE = \frac{1}{MN}\sum_{i=i}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))^2$$

ii) Signal to Noise Ratio (SNR): Signal to noise ratio [8] can be calculated by the given formula below.

$$SNR = 10log\left\{\frac{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}x(i,j)^2}{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[x(i,j) - y(i,j)]}\right\}$$

Where, x (i,j) is original image and y(i,j) is recovered image.

iii) Peak Signal to Noise Ratio (PSNR): Peak signal to noise ratio can be calculated by the given formula below:

$$PSNR = 20log\left(\frac{255}{RMSE}\right)$$

Where, RMSE can be calculated by the MSE.

$$RMSE = \sqrt{MSE}$$

5. RESULTS

The above algorithm for the image encryption and decryption using the dual transformation technique is tested on several images, and the mean square error, signal to noise ratio and peak signal to noise ratio has been calculated. The calculated result is shown below.

Table 1: Results for natural images.

Sr. No	Image	MSE	SNR	PSNR
1	Lena	$6.8617*10^{-30}$	360.3402	782.3412
2	Pepers	$6.1675*10^{-30}$	363.3321	783.4078
3	Splash	$4.0238*10^{-30}$	338.0268	787.6785
4	Mandrill	$5.7934*10^{-30}$	340.3263	784.0336
5	Couple	$9.1755*10^{-31}$	356.2846	802.4613
6	Caster_stand	$4.4867*10^{-30}$	339.3776	786.5895
7	Airplane	$1.2341*10^{-29}$	339.9576	776.4716
8	Sailboat	$8.0771*10^{-30}$	344.8308	780.7105
9	House	$1.0587*10^{-29}$	349.3891	778.0048
10	Strawberries_coffee	$1.1570*10^{-29}$	342.3227	777.1170

Table 2: Results for synthetic images.

Sr.No.	Image	MSE	SNR	PSNR
1	CHECK BOX	$5.7679*10^{-30}$	338.6153	784.0728
2	TEXT	$2.3881*10^{-29}$	347.9187	789.8701
3	OIL	$3.3142*10^{-30}$	347.9326	789.6188
4	NVIDIA	$6.0705*10^{-30}$	362.9036	783.5664
5	GRAPHIC	$1.2193*10^{-30}$	330.9969	799.6180
6	BOX	$5.0163*10^{-30}$	333.2873	785.4739

The below gives the calculation of time required to compute the encoding and decoding algorithm given above.

Table 3: Time computation for the encoding and decoding process for Natural Images.

Sr. No.	Images	Encoding Time	Decoding Time
1	Lena	0.251336	0.050070
2	Pepers	0.268949	0.049378
3	Splash	0.264723	0.055648
4	Mandrill	0.251023	0.057384
5	Couple	0.243052	0.051681
6	Caster_Stand	0.278351	0.051154
7	Airplane	0.268358	0.051266
8	Sail Boat	0.301892	0.058388
9	House	0.269759	0.050069
10	Strawberries_coffee	0.263549	0.058427

Table 4: Time computation for the encoding and decoding process for Synthetic Images.

Sr. No.	Images	Encoder	Decoder
1	CHECKBOX	0.241341	0.059461
2	OIL	0.306702	0.049382
3	TEXT	0.300463	0.057724
4	NVIDIA	0.312236	0.052425
5	GRAPHIC	0.295547	0.057609
6	BOX	0.293496	0.063490

Some Image Results of encryption and decryption is shown in visual form below.

6. CONCLUSION

In this paper the proposed algorithm has been tested on several test images and the result is found good as in the above process the mean square error of image is very very less, this shows that error is negligible, and the psnr is very good. This image encryption technique provides more security as in this encryption technique uses two different transform. With random phase encoding.

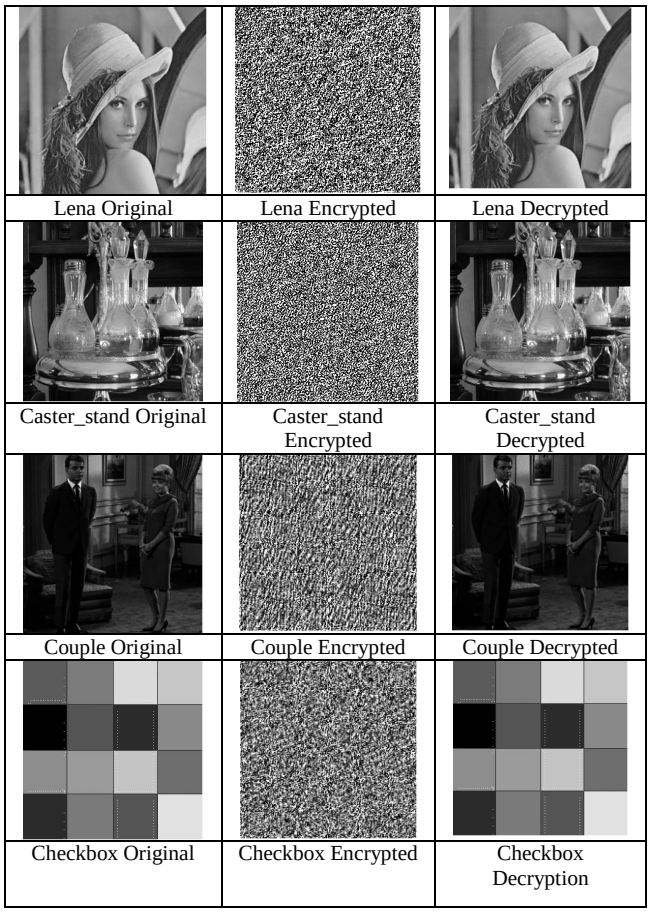


Figure 8: Orignal Image, Encrypted Image and Recovered Image

7. ACKNOWLEDGMENTS

The author would like to thanks Asst. Prof Satish Kumar Singh for their guidance. The author would like to thank to their family members and close friends for many fruitful Discussions.

8. REFERENCES

[1] Gonzalez Rafel C. and Woods Richards E., "*Digital Image Processing*", Third Ed., Textbook 2011, Published by Pearson Education Inc., ISBN: 978-81-317-2695-2.

[2] Gonzalez Rafel C., Woods Richards E. and Eddins Steven L., "*Digital Image Processing Using MATLAB*", Second Edition, Published by Tata Mc. Graw Hill Companies, ISBN-13: 978-0-07-070262-2, ISBN-10: 0-07-070262-4

[3] Wasseem Nahy Ibrahem, "*Wavelet and Multi Resolution Processing Tutorial*", Available at: uotechnology.edu.iq/sweit/Lectures/Image-Processing-4th/Dip-lecture8.pdf.

[4] Anil K. Jain, "*Fundamentals of Digital Image Processing*", Published by PHI Learning Private Limited, ISBN-978-81-203-0929-6.

[5] Soo-Chang Pei, and Wen-Liang Hsue, "*The Multiple Parameter Discrete Fractional Fourier Transform*", IEEE Signal Pprocessing Letters, VOL. 13, NO. 6, JUNE 2006.

[6] Solomon David, "*Data Compression: The Complete Reference*", Fourth Edition, Published by Springer Publication, ISBN-13: 978-1-84628-602-5, ISBN-10: 1-84628-602-6.

[7] C. Sasi Varnan, A. Jagan, Jaspreet Kaur, Divya Joyti and D. S. Rao, "*Image Quality Assessment Technique on Spatial Domain*", IJCST Vol. 2, Issue 3 September 2011, pp 177-184.

[8] G. Gupta and H. Aggrawal, "*Digital Image Watermarking Using two Dimensional Discrete Wavelet Transform, Discrete Cosine Transform and Fast Fourier Transform*", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[9] Test Images, Available at : www.sipi.usc.edu/database/

[10] Test Images, Avaliable at: http://www.imageprocessingplace.com/root_files_V3/image_databases.htm