*2011 International Conference on Information and Network Technology*
*IPCSIT vol.4 (2011) © (2011) IACSIT Press, Singapore*

# Comparison of Encryption Levels for Image Security Using Various Transforms

K.Sumathy [1], R.Tamilselvi [2]

[1] RMK Engineering college,Chennai,muthusuma@gmail.com

[2] RMK Engineering college,Chennai,tamil_ct@rediffmail.com

**Abstract**. In recent trends, information security is becoming more important in data storage and transmission. Therefore, the protection of information from unauthorized access is important. Image encryption plays a significant role in the field of information security. Several security Algorithms are existing for safer transmission of data. In this paper a new encryption method is developed and a comparison is done by transforming images using DCT, DWT and DCT with DWT. Various parameters are analyzed for comparison of encrypting levels.

**Keywords:** Key Generation, DCT, DWT, Encryption, correlation coefficient

## 1. Introduction

With the increasing growth of electronic media, security is an important issue in communication and storage of images. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, and military communication. In these applications, it is relevant to hide the content of a message when it enters an insecure channel. The original image to be send by the sender is converted into encrypted format prior to transmission. The process of recovering original image at the receiver is called decryption. The encryption process requires an encryption algorithm and a key. The decryption can be done only with the unique key. Thus confidentiality of the medical images is maintained with the particular key.

Aloka Sinha and Kehar Singh proposed an algorithm using digital signature and Bose-Chaudhuri Hochquenghem (BCH) code in 2003. Also an algorithm based on SCAN patterns and compression for encryption is explained by S.S. Maniccam and N.G. Bourbakis, 2001. Vector quantiztion methods used for encryption is explained by Chin-Chen Chang and et al, 2001.Based on chaos and mirror like method Jiun-In Guo and Jui-Cheng Yen proposed image encryption algorithm.

Feasible and simple image encryption algorithm based on DNA sequence has been developed by Shihua Zhou and et al , 2010. Image encryption is analyzed through various parameters like mean, root ,mean square ,correlation coefficient etc.2010 In the paper explained by Qiang Zhang and et al 2009, encryption is analyzed based on chaos and DNA sequences.

Ismet Ozturk and Abrahim Soukpınar compared various encryption algorithms and proposed new schemes which add compression capability to the mirror-like image encryption and visual cryptography algorithms.[2005].

In this paper,a specific key is generated for security using DNA sequences. The original image is encrypted by decomposing the image by DCT,DWT and a combination of DCT and DWT. In the next section, various parameters like mean, standard deviation, correlation coefficient and Root mean square value are measured between the original image and the encrypted image.

## 2. Encryption Techniques

Security Algorithms play a significant role in ensuring the integrity of data. Many encryption algorithms are available for secured transmission of data. Asymmetric algorithms are more commonly known as Public-key cryptography, first introduced in 1978 with RSA encryption. These types of encryption algorithms involve a pair of keys that encode and decode messages. One key is used to encrypt data into ciphertext while the other key decrypts it back into plaintext. Asymmetric algorithms tend to be slower than their symmetric counterparts. Because of this, they aren't recommended for encrypting large amounts of data. The biggest advantage to such a scheme lies in the utilization of two keys. Hence the name, the public key can be made publicly available, enabling anyone to encrypt private messages. However, the message can only be decrypted by the party that owns the relative private key. This type of encryption algorithm also provides proof of origin to ensure to overall integrity of communications.

## 3. Methods

### 3.1. Key Generation Using DNA Sequence

In this paper, we use DNA base pairs for key generation. A DNA sequence basically contains four nucleic acid bases :Adenine(abbreviated A), Cytosine(C), Guanine (G) and Thymine(T), with A bonding only to T, and C bonding only to G. The following bit patterns are assigned to AGCT:

| | |
|---|---|
| A | 1010 |
| G | 1011 |
| C | 1100 |
| T | 1111 |

The principle of specific key (K) generation is given by:

Step 1: Bits are represented in matrix format(X)
Step 2: Multiply the matrix with its complement(XX')
Step 3: XOR the product with original matrix.
Step 4: Complement the resultant matrix
Step 5: Bit manipulations are done for advanced security.
Step 6: Size of the image is added with the new address table to get a new vector table.

### 3.2. Block Transformation

The original image to be sent is divided into distinct blocks .These blocks are transformed using DWT transform, DCT transform and a combination of DCT with DWT.

In Discrete Cosine Transform (DCT), the blocks are transformed from the spatial domain to the frequency domain .In Discrete wavelet Transform(DWT), a block is decomposed into a set of basis functions called as wavelets. The wavelet transform is computed separately for different segments of the time-domain signal at different frequencies

### 3.3. Key Addition

The generated key is taken as a private key and it is added with the transformed image to get the encrypted image.

### 3.4. Comparison of Encryption Levels

The encrypted image got by using DWT ,DCT and DCT with DWT are compared and the various parameters are analyzed. The end user can select particular transform depending on their image security. This is the main advantage of the proposed algorithm.

## 4. Simulation Results

In this algorithm, a specific key is generated with the AGCT pairs. The generated key is reshaped into transformed image size to get proper addition of transformed image with the key. The final encrypted image is obtained for all the transformations.

## 4.1. Original Image

The original image to be sent to the receiver with encryption is given in the following figure

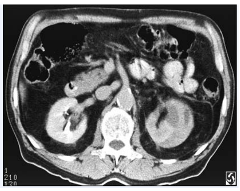


Fig 1 Original Image

## 4.2. Transformed image

The transformed images are depicted in the following figures 2,3 and 4.

Fig2 DCT Transformed Image

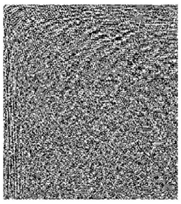


Fig3 DCT with DWT Transformed Image

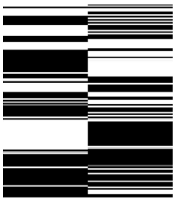
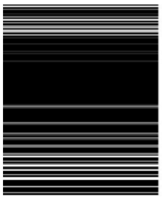


Fig4 DWT Transformed Image



## 4.3. Encrypted Image

After the key addition, transformed image is converted into encrypted image. The final encrypted image is shown in the figure 4 and 5

Fig 5 DCT Encrypted Image

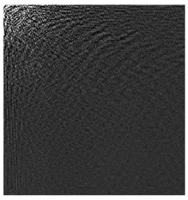


Fig 6 DCT with DWT Encrypted Image

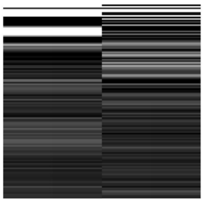


Fig7 DWT Encrypted Image

## 4.4. Statistical Analysis of Encrypted Image with Different Transforms

a. Mean:

Mean or Average is defined as the sum of all the given elements divided by the total number of elements.

Mean = sum of elements / number of elements
=a1+a2+a3+.....+an/n

b. Standard deviation:

It shows how much variation or dispersion there is from the average

$$\sigma = \sqrt{\mathrm{E}[(X - \mu)^2]}.$$

c. RMS:

The **root mean square** (abbreviated **RMS)**, also known as the **quadratic mean**, is a statistical measure of the magnitude of a varying quantity.

$$x_{\mathrm{rms}} = \sqrt{\frac{{x_1}^2 + {x_2}^2 + \cdots + {x_n}^2}{n}}.$$

d. Correlation coefficient:

Correlation coefficient gives the statistical relationships between two or more random variables or observed data values

Table 1 Various parameters of the original image

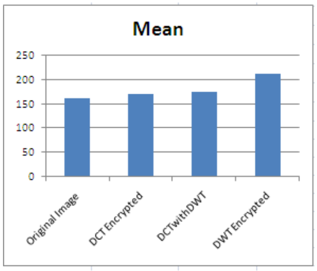
| Mean | Standard Deviation | RMS |
|---|---|---|
| 161.11 | 78.37 | 179.71 |

Table 2 Various parameters of the Encrypted image

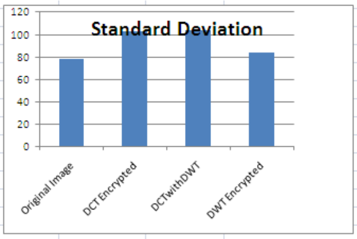
| Transform Used | Mean | Standard Deviatio n | RMS | Correlation Coefficient |
|---|---|---|---|---|
| DCT | *169.23* | 102.64 | 197.92 | 0.023 |
| DCT with DWT | *174.13* | 103.89 | 202.77 | 0.025 |
| DWT | 211.50 | 84.27 | 227.67 | 0.016 |

## 5. Comparison Charts

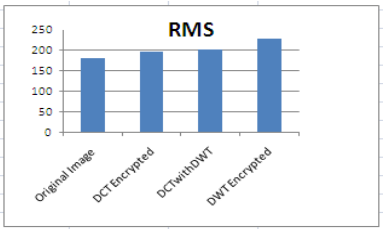
### 5.1. Comparison of Mean



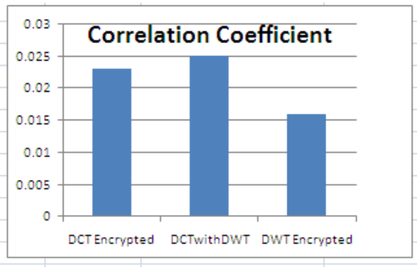
### 5.2. Comparison of Standard Deviation



### 5.3. Comparison of RMS



### 5.4. Comparison of Correlation Coefficient



## 6. Results and Discussions

The proposed work analyses the encryption of the original image with various transforms. The difference between the original and encrypted image is found by the analyzed parameters. The randomness in the encrypted image is studied by mean, RMS and standard deviation. By finding the correlation coefficient, we see that the correlation between the original and the encrypted image is very less.

## 7. Conclusion

In this algorithm, encrypted image is highly uncorrelated with the original image. Thus the security of the image is ensured. The user can select the transform depending on the nature of the security of the image.

## 8. References

[1] Shihua Zhou, Qiang Zhang, Xiaopeng Wei ,“ Image Encryption Algorithm Based on DNA Sequences for the Big Image”, International Conference on Multimedia Information Networking and Security,2010.

[2] Qiang Zhang , Ling Guo, Xianglian Xue, Xiaopeng Wei ,” An Image Encryption Algorithm Based on DNA Sequence Addition Operation”,IEEE,2009

[3] Mohammad Ali Bani Younes and Aman Jantan,“Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, 35:1, 2008.

[4] Christy M. Gearheart, Benjamin Arazi,, Eric C. Rouchka,,”DNA-based random number generation in security circuitry”, BioSystems 100,2010.

[5] H S Manjunatha Redd y, K B Raja “High capacity and security steganography using Discrete wavelet transform”, International Journal of Computer Science and Security (IJCSS), 3:6

[6] Ismet Ozturk and Abrahim Sogukpinar, “Analysis and Comparison of Image Encryption Algorithms”, World Academy of Science, Engineering and Technology 3 2005