ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

# Visually Meaningful Image Encryption.

**Arunkumar S*, Senthilselvan N, and Saikishor Jangiti.**

School of Computing, SASTRA University, Tamil Nadu, India.

**ABSTRACT**

Now-a-days, lots of images, which are very personal or confidential, are being transmitted over the internet either among individuals or companies. At the same time, attacks on those images are also increasing day-by-day. Hence to protect the contents of the image, many image encryption algorithms are evolving where most of them transform the original image to a noise- like or texture -like image. But this is an obvious visual sign indicating the presence of an encrypted image and thus results in a significantly large number of attacks. To overcome this problem, our algorithm generates a new image encryption concept to transform an original image into a visually meaningful encrypted one where a visually meaningful or good-looking encrypted image (VMEI) is produced that has a high possibility of being treated as an encrypted one. This would significantly reduce the risk of an encrypted image being attacked and modified. The algorithm also uses Lifting wavelet transform for further enhancement of the VMEI. At last the image sharpening is done to enhance the final image.

**Keywords**: Encryption, Lifting wavelet transform, meaningful image.

***Corresponding author***

ISSN: 0975-8585

## INTRODUCTION

### Image Encryption

In today's technological world, images are being transferred frequently among many organizations. The type of images may be of medical, architectural and also related to space which has valuable data inside them. So the images are very vulnerable to attacks by the intruders. Hence transmission of images must be done very securely. Encrypting the images is one of the ways to secure the content in the images. During this process, a sender selects the image that is to be sent called as original/raw image, converts into pixels, encrypts the image and sends it to the receiver. The receiver decrypts the image and views the original image.

### Encryption Algorithms

Encryption algorithms are divided into two types:

- **Symmetric**
- **Asymmetric**

In Symmetric Encryption algorithms, the same key is used to perform both encryption and decryption. Here, both sender and receiver know the key before performing the encryption and decryption respectively. Examples are: Substitution techniques, Transposition Techniques, AES (Advanced Encryption Standard) etc.

In asymmetric Encryption algorithms, different keys are used to perform encryption and decryption. The keys are known as Public and Private Keys. These type of techniques are used for confidentiality, authentication, or both.

### Substitution cipher Technique

Substitution cipher technique is one of the symmetric encryption techniques where the original content is modified by performing mathematical operations. On the decryption side, the original content is retrieved by performing the reverse of the above mathematical operation.

Example: Caesar cipher

In Caesar cipher technique, the plain text is replaced by performing the below mathematical operation
Cipher text= (plaintext) +k, 'k' must be a number.

If the above technique is used for alphabets, then the result should be in the range of 26. Hence, performing of modulo 26 operations is necessary. If the same technique is applied for numbers (as in the case of image pixels), then the result can be within any desired range.

### Wavelet Transforms

Wavelets, in the area of Image processing, are mainly used for representing images in various degrees of resolution. These divide the image into smaller regions and thus supports for image data compression. These smaller regions are called sub bands which can be reassembled to reconstruct the original image without error as shown in the below figure (Fig-1)

ISSN: 0975-8585

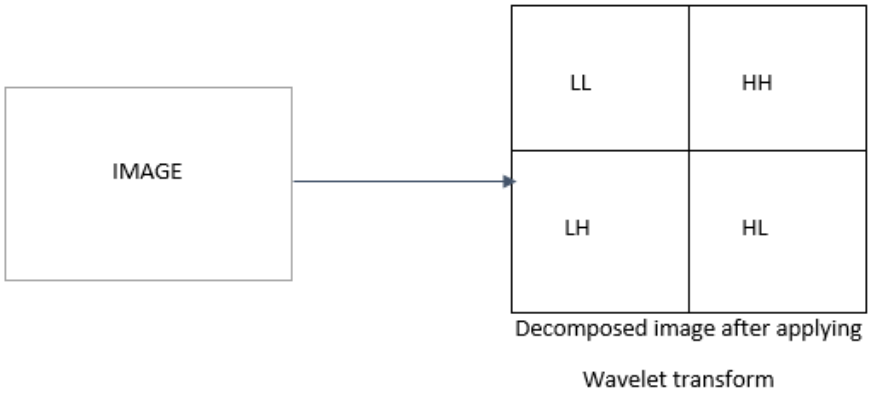


**Fig 1 Wavelet transform**

**Need for Wavelet transforms in image encryption**

The output format of the encrypted images which have undergone only encryption technique will be either in noise-like or texture like formats. This is an indication of certain content under the image which leads to the easy attacks by intruders. In order to hide the original image under the reference image, wavelets are also applied along with the encryption technique. This leads to the generation of Visually Meaningful Encrypted Images (VMEI).It is the best way to provide more security as there is no sign of encrypted form.

**Different Wavelet Transforms**

Now-a-days, wavelets are also being used along with the encryption technique. This technique of combining both the concepts of wavelets and encryption leads to higher security.

Different Wavelet Transforms used are:

- Fractional Fourier transform (FRFT)
- Fast wavelet transform (FWT)
- Discrete wavelet transform (DWT)
- Fractional wavelet transform (FRWT)
- Continuous wavelet transform (CWT)

**DWT and LWT**

Both DWT and LWT decompose the image into four sub bands. The main difference between DWT and LWT techniques lies in the PSNR (Peak Signal to Noise Ratio) and SNR (Signal to Noise Ratio) values which are high for LWT and low for DWT. Moreover the fourth sub band i.e. HH is more enhanced in LWT than in DWT.

SNR is defined as the ratio between the values of average of the pixels to the standard deviation of the pixels. If the resultant value is high, then the accuracy is more. This is proved to be greater for LWT compared with DWT. PSNR is defined as the ratio between the values of maximum value of the pixel and the power of the noise. It should be higher for any image. This value is also proved to be higher for LWT. Execution Time is defined as the time taken to perform a particular algorithm. The lesser the value, the higher the efficiency of that algorithm. It is proved that, LWT has less execution time when compared with DWT.

**LITERATURE REVIEW:**

According to Hai Yu, Zhiliang Zhu,in the paper “An Efficient Encryption Algorithm Based on Image Reconstruction”, the image decomposition and reconstruction was performed at the bit level. But , dealing

with integer coefficients of the image results in better outputs rather than double or bit values [1]. According to Mrs. Preet Kaur, Geetulalit,in the journal "Comparative Analysis of DCT, DWT &LWT for Image Compression", the comparison among DCT, DWT and LWT are explained with the metrics known as SNR, PSNR, and execution time values [2]. In the paper "Weighted Performance comparison of DWT and LWT with PCA", by Mrs.PreetKaur, Geetulalit, Principal Component Analysis using both DWT and LWT are compared for face retrieval. It is shown that DWT gives more elapsed time compared to LWT [3]. The generation of VMEI (Visually Meaningful Encrypted Images) is explained in the paper

"Image encryption: Generating visually meaningful encrypted images" by Long Bao and yicong [4]. The Lifting Wavelet transform using Haar wavelet is explained by Monika, PrachiChaudhary, GeetuLalit in the journal "The Lifting scheme using Haarand bio orthogonal wavelets for image compression". It states that Haar wavelet is simple and real where the results are obtained very fast. This wavelet is proved to be memory efficient. It is also flexible for manual calculations [5]. The different types of wavelets and their applications are explained by, RafelC. Gonzalez., RichardE. Woods in the book "Digital Image processing". It states that ,Wavelets, in the area of Image processing, are mainly used for representing images in various degrees of resolution. These divide the image into smaller regions and thus supports for image data compression. These smaller regions are called sub bands which can be reassembled to reconstruct the original image without error [6].

**CONCEPTUAL MODELING /PROPOSED ARCHITECTURE**

In the existing system, the DWT constructs the encrypted image without proper interaction between the sub bands. Moreover, DWT deals cannot deal with integer values. Thus, when the input data consists of integers, the outputs obtained do not consist of integers. Hence, the reconstructed image will not be accurate.

However, by using LWT that deals with integers, the output can be obtained completely in integer format. In the proposed system, LWT is used which will deal with integers in an efficient way.

**Proposed Architecture:**

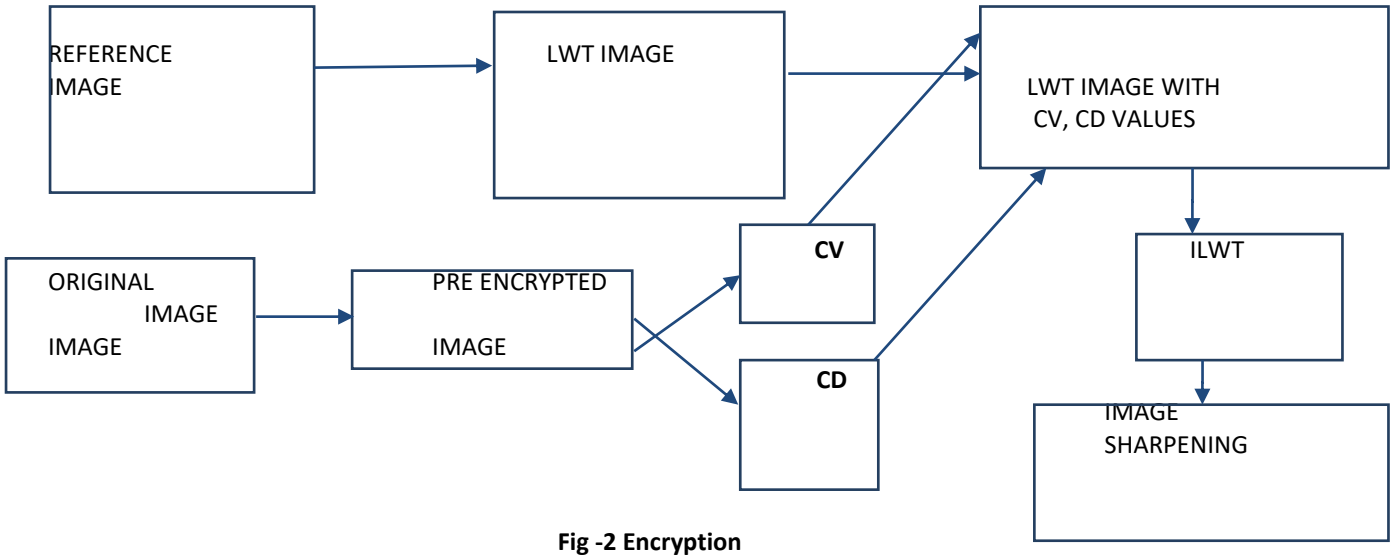


**Fig -2 Encryption**

The proposed system architecture for encryption is shown in the above figure (Fig-2)

In the encryption module, the input image and reference image are taken from the user. The encryption is performed on the input image to obtain the CV and CD values. Similarly, LWT is performed on the reference image to get the sub bands. Now the CV and CD are replaced in the place of LH and HH bands. Then the ILWT is performed to get the encrypted image.

ISSN: 0975-8585

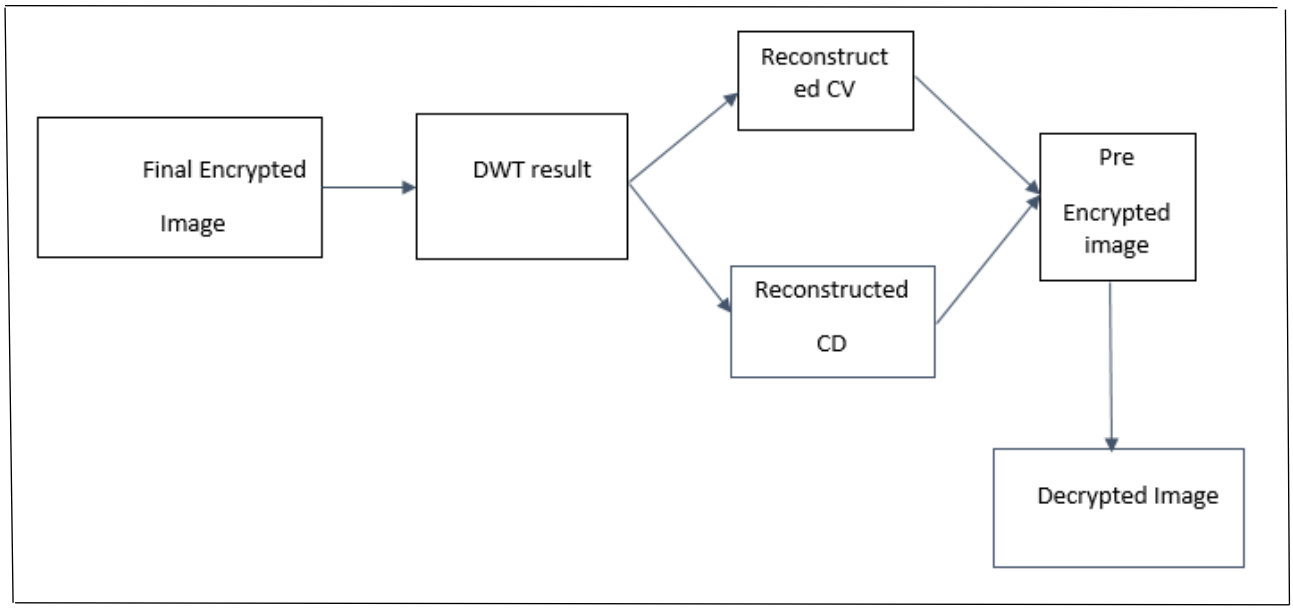


**Fig-3 Decryption**

The above figure (Fig-3) shows the decryption module of the proposed architecture. The LWT is applied on the encrypted image and CV, CD values are reconstructed to get the Pre encrypted image. The inverse substitution cipher is performed on the obtained image to get the final Decrypted image.

The mathematical calculation used for extracting CV and CD values is:
1. Retrieve the pixel values from the image.
2. CV is obtained by performing the following calculation on LH sub band
CV=floor (pixel value/10)
3. CD is obtained by performing the following calculation on HH sub band
CD=pixel value mod 10
The reconstruction of the CV and CD while performing decryption is done by using the below formula
Original pixel value = CV*10+CD

Then the inverse of substitution cipher is obtained to get the original image. Image sharpening can be done to the obtained image to enhance the image quality.

## METHODOLOGY AND APPROACH

### User Inputs

The user gives the input image i.e. 1.Original Image (fig-4)2.Reference Image(fig-5). The algorithm is developed such that the user can select images of any format and from anywhere in the system.

### Encryption of the Original Image

The reference image is converted into pixels and the substitution cipher technique is applied to each pixel so that the output will be a blurred image. Then, each pixel is made to undergo some changes by applying mod and ceil functions as shown below and the values of CV and CD are obtained.

$$CV(m,n)=floor(p(m,n)/10)$$
$$CD(m,n)=p(m,n) \bmod 10$$

Where p(m,n) is the pixel at m,n position

**Applying LWT for the reference image and performing encryption**

The LWT is applied for the input image such that the image is divided into four sub bands say LL, HL, LH, HH as shown in the figure (Fig-6). Now the CV and CD values obtained from the Encryption of the reference image are substituted in the place of LH and HH respectively and the image will be as shown in the figure (Fig-7). Then the ILWT (Inverse Lifting Wavelet Transform) is performed for the obtained image to get a Visually Meaningful Encrypted Image.

**View the encrypted image**

The user is provided with the facility to view the Encrypted image (Fig-8) obtained before sending it to the receiver

**DECRYPTION OF THE IMAGE**

**LWT of the encrypted image**

The receiver after receiving the encrypted image performs the LWT on that particular image to obtain the four sub bands as shown in the figure (Fig-9)

**Extracting CV and CD**

The values of CV and CD are obtained from the LH and HH values of the obtained image and calculations are performed in order to retrieve the original pixel values.

$$P(m,n)=CV(m,n)*10+CD$$

Now the obtained pixel values are made to undergo the technique which is of reverse to the substitution cipher algorithm such that the original pixels are regained.

**View the decrypted image**

The receiver can now view the decrypted image by converting the pixels obtained from above technique into image format as shown in the figure Fig-10

**Evaluation**

The evaluation for this proposed system is done using the wavelet transforms and their performance metrics. Here, the execution time, PSNR and SNR are considered. Different input images are analyzed with one reference image and the values of the above performance metrics are evaluated and tabulated as shown in the table (Table 1)

**RESULTS**

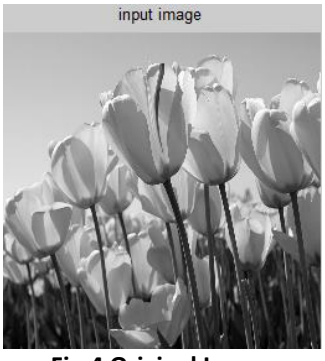


**Fig-4 Original Image**

ISSN: 0975-8585

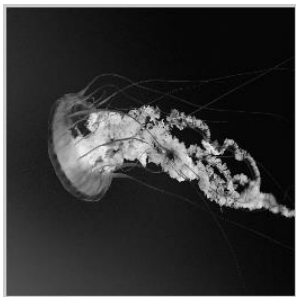

**Fig-5 Reference Image**

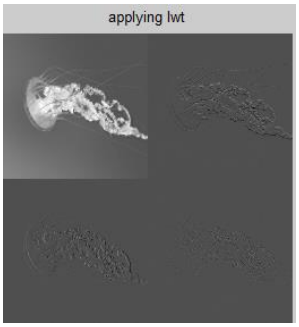


**Fig-6 Applying LWT for the reference image**


**Fig-7 Embedding CV and CD**

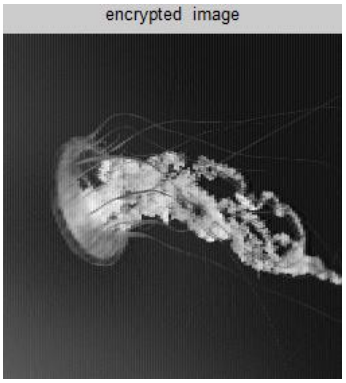


**Fig-8 View the encrypted image**

ISSN: 0975-8585

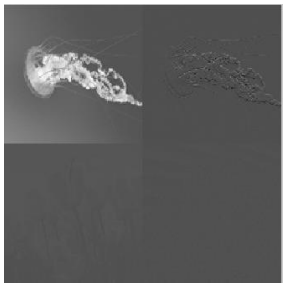

**Fig-9 LWT for the encrypted image**

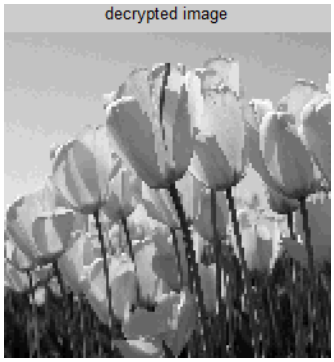


**Fig-10 Decrypted Image**

**Table 1: TABLE FOR COMPARING DWT AND LWT ELEMENTS**

| s.no | Images | | Execution time | | SNR | | PSNR | |
|---|---|---|---|---|---|---|---|---|
| | Original image | Reference Image | DWT | LWT | DWT | LWT | DWT | LWT |
| 1 | Unnamed.png | Images.jpg | 2.138 | 1.968 | 12.513 | 18.439 | 7.881 | 13.167 |
| 2 | Download.jpg | Images.jpg | 1.792 | 1.750 | 12.813 | 16.940 | 9.514 | 9.695 |
| 3 | images.jpg | Images.jpg | 2.1794 | 2.1312 | 12.3477 | 18.4650 | 8.3412 | 13.5335 |

**ACKNOWLEDGEMENT**

We acknowledge the support of Bollineni Bhavya, G Bhagya Lakshmi, M Lavanya Kumari in the implementation of visually meaningful image encryption to cross check our theoretical model.

## CONCLUSION

Visually Meaningful Encrypted Images are successfully generated by using both Encryption and LWT technique thus overcoming the defects of DWT. The values of SNR, PSNR, and execution times are enhanced more than the values obtained from DWT. The entire focus has been on single input image and single reference image. This may be extended to encrypt more than one input images using the same reference image and reducing data loss and preserving the clarity of the images.

## REFERENCES

[1] Yu H, Zhu Z, Chen G. IEEE.2009 Nov 6 (pp. 200-204).
[2] Katharotiya AK, Patel S, Goyani M. Journal of information engineering and applications. 2011;1(2):9-17.
[3] Madhavan J, Porkumaran K. IJAER 2015: (10) 3449-3466
[4] Bao L, Zhou Y. Information Sciences. 2015 Dec 10;324:197-207.
[5] Mishra V, Kumar A, Jaiswal AK. International Journal of Computer Applications. 2015 Jan 1;126(9).
[6] Rafael C Gonzalez, Richard E.woods Digital image processing Prentice hall publication 2002 pg 372 -379.