# DWT Based Watermarking For Lifting Based Compression And Symmetric Encryption Of JPEG Images

Ansu Anna Ponnachen[1], Lidiya Xavier[2]
[1](Department Of ECE,KMCT College Of Engg/Calicut University, India)
[2](Department Of ECE,KMCT College Of Engg/Calicut University, India )

***Abstract*— In the digital world the digital media is currently evolving at such rapidly;copyright protection is become increasingly important.Now a days these media is available with various image formats,due to which they are simple to copy and resell without any loss of quality.A wide range of digital media is often distributed by multiple levels of distributors in a compressed and encrypted format.It is sometimes necessary to watermark the compressed encrypted media items in the compressed encrypted domain itself for tamper detection or ownership declaration or copyright management purposes.The objective of image compression is to reduce irrelevance and redundancy of the image data inorder to be able to store or transmit data in an efficient form.This paper deals with the watermarking of compressed and encrypted JPEG 2000 images.The compression is achieved on JPEG 2000 images by lifting based architecture.The encryption algorithm used is stream cipher.The identification of watermark can be done in the decrypted domain.The watermarking technique used is spread spectrum.This can be implemented through matlab.**

***Key Words*—JPEG 2000,Lifting Scheme,Symmetric Encryption,DWT.**

## I. INTRODUCTION

In 1990's watermarking concept came into existence as the internet spreaded wholly.For hiding a secret image or data so many approaches are there like cryptography,steganography,watermarking,fingerprinting. As they are intentionally same,they differ from each other in their aims.Each of these techniques having different methods and they are also differ by their procedures. Cryptography focuses on keeping the message content.while steganography focuses on keeping the existence of secret message.

Digital watermarking provides copyright protection in the digital form.The various applications of watermarking involves ownership assertion,tamper detection,copyright protectionetc.There are various kinds of watermarking and they are fragile, semifragile and robust.Fragile watermarking may broke up or degraded under slight changes,while fragile is designed to break under all changes which exceed a specified threshold;where as robust will withstand to several changes including severe signal processing attacks.

This paper proposes a robust watermarking technique for the compressed and encrypted JPEG 2000 images.The JPEG 2000 compression achieved through lifting based DWT architecture[4].The encryption technique proposed is RC4 stresm cipher encryption.Some asymmetric schemes like RSA,Elgamal and paillier with homomorphism property can be used but there are mainly two drawbacks while using this[1].First one if we encrypt afew bit message size,the cipher text may expand and reaches loss in compression efficiency.Second one if we encrypt a large message size;the payload capacity decreases to compensate the compression loss;where payload capacity is the number of watermark signal bits embedded per encrypted message.Hence the secure symmetric RC4 stream cipher is preferred.

## II. PROPOSED SCHEME

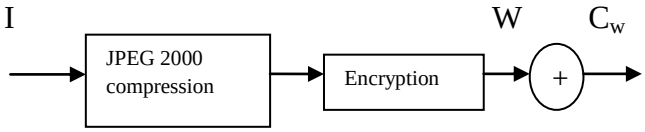
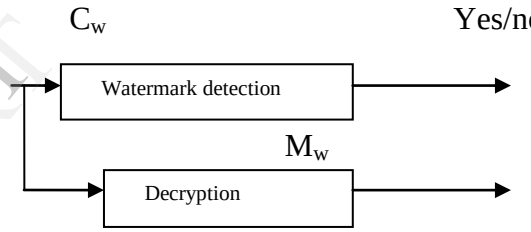



Fig.1 (a)Watermark Embedding




(b)Watermark Extraction

### A. JPEG 2000 Compression

The proposed algorithm works on JPEG2000[5] compressed code stream. JPEG2000 compression is divided into five different stages.In the first stage the input image is preprocessed by dividing it into non-overlapping rectangular tiles, the unsigned samples are then reduced by a constant to make it symmetric around zero and finally a multi-component transform is performed. In the second stage, the discrete wavelet transform (DWT) is applied followed by quantization in the third stage. Multiple levels of DWT gives a multi-resolution image. The lowest resolution contains the low-pass image while the higher resolutions contain the high-pass image. These resolutions are further divided into smaller blocks known a code-blocks where each code-block is encoded independently. Further, the quantized- DWT coefficients are divided into different bit planes and coded through multiple passes at embedded block coding with optimized truncation (EBCOT) to give compressed byte stream in the fourth stage. The compressed byte stream is arranged into different wavelet packets based on resolution, precincts, components and layers in the fifth and final stage.The DWT operation is performed based on lifting scheme.

Basic lifting scheme [6] is given through the block diagram given below.

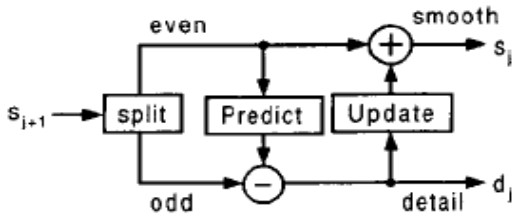



Fig (2) Lifting based DWT

The three stages in lifting are splitting,predicting and updating.

- Splitting : Splits the data into two smaller subsets.
- Predicting : Even samples are multiplied by the prediction operator to predict odd samples.
- Update : Even samples are updated with detail coefficient to get smooth coefficient.

The main algorithm for lifting can be available in original lifting papers[ 7-11].

In the case of digital image processing,images are the inputs and for DWT they are splitted into low and high frequency bands.Then the DWT consists of many levels.The 2 frequency bands are been divided in to 4 block levels.This is mainly for finding the low frequency variation of the image.A quantization is approach is for adopted for eliminating low colour variation of the object.This is mainly achieved by finding coefficients corresponding to the block levels and it is divided into various subbands by assigning to different matrices. And finally these are merged to a single plane.

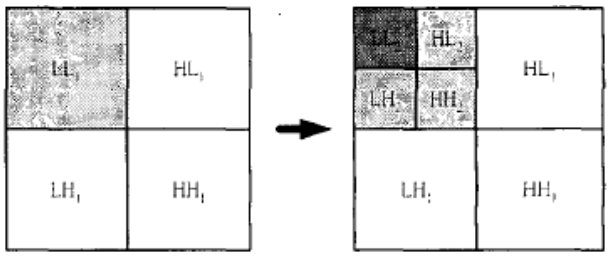



Fig (3) 2 level wavelet transform[11]

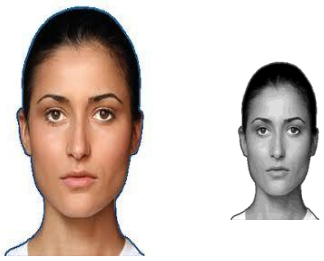


Fig (4)

(a)original image (b)compressed image

## *B. Encryption Algorithm[4]*

A secret key cryptosystem encrypt image pixel by pixel, with the stream cipher algorithm. RC4 stream cipher convert original image to encrypted image one bit at a time. In this structure a key is input to the keystream generator.A keystream generator (sometimes called a running-key generator) outputs a stream of bits: K1, K2, K3,……, Ki. This keystream is XORed with a stream of plaintext bits, P1, P2, P3,….,Pi to produce the stream of ciphertext bits C1, C2,……Ci.Key stream generator is also called pseudo random generator.

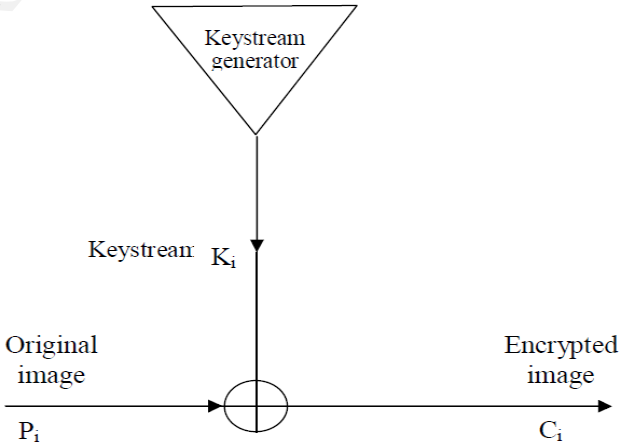
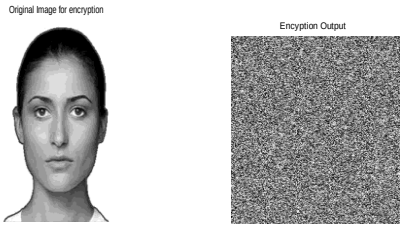



Fig (5) Encryption process

For eg: if the plain text is given as 11001100 with keystream 01101100 then the obtained cipher text is given as

11001100 xor
01101100
10100000:cipher text

In the case of decryption 10100000 xored with 01101100 gives 11001100.




(a) (b)

Fig (6)

In the above fig (a) shows the original image for encryption and (b) is the encrypted output.

### *C. Watermarking Algorithm*

A robust watermark is the one that withstand a wide variety of attacks that includes incidental and malicious.In digital image watermarking the secret data that we hide is called the watermark.The main image that the watermark is embedded is called cover image. It is the processing of embedding a bit,signature ,image etc that is kept as secret in to an input. The input also be an image, text etc. The purpose of this is providing extra security, authentication etc.There are many watermarking algorithms existing.The quality of watermarking is detrmined by the PSNR ratio by calculating MSE.Here we are proposing a watermarking algorithm based on DWT. The flowchart is given below.The main steps includes

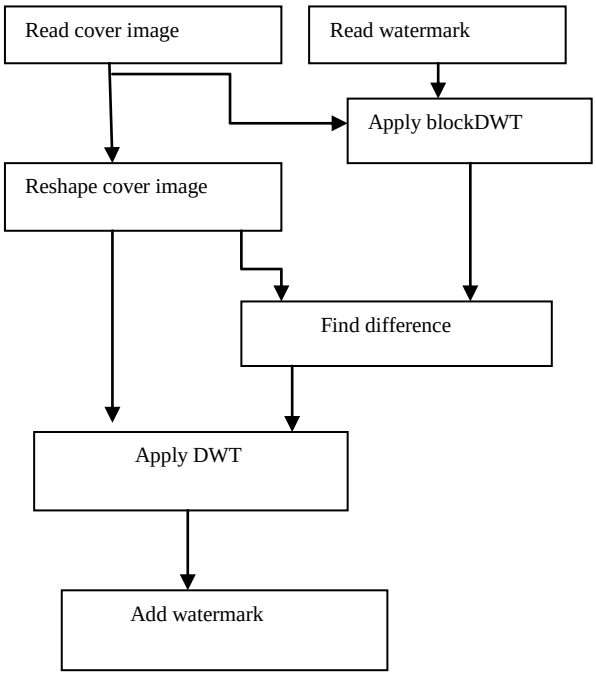



Fig (7) Flowchart for watermarking

- Read cover image and watermark
- Reshape cover image.
- Apply DWT on both images.
- DWT obtains both low and high frequency regions.
- Select high intensity region in the low frequency band which is having a specified threshold.
- The watermark is added in this high intensity portion of the low frequency region..

High intensity portion is having a threshold value above 255which is the white portion in the images.This is about watermark embedding process.The watermark extaction is the next stage includes detection and decryption.

### *D Watermark Detection*

The watermark is detected in the extraction stage.It can be achieved by thresholding process.

- Check the watermark scale value.
- If it is greater than a specified threshold value,then watermark is detected.
- The threshold is determined by the intensity value of the watermark.

If the scale value is higher than the specified value, then it is detected;otherwise not detected.The decryption process is also carried out in this stage.It is also performed by using RC4 decryption.They are always faster and use far less code compared with block ciphers.The key is user defined which is between 40 bits and 256 bits.The cipher text is xored with the key to produce the decrypted output. .For example when five character ASCII code given to a keystream generator is translated to 40 character binary equivalent or key stream which is used to encrypt the binary image.output of the key stream generator depend on the value of input key and the keystream generated will have the properties of true random number stream.ie,there should be an equal number of 0's and 1's.So RC4 is a well established stream cipher. RC4 was kept as a trade secret by RSA Security.

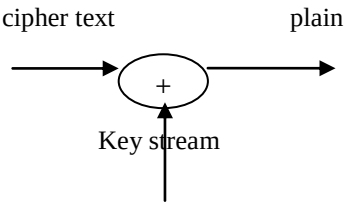



Fig (8) Decryption

*Peak Signal to noise Ratio:* It is an important parameter for determining the watermark image quality. We use Peak signal to noise ratio (PSNR) to evaluate quality of watermark image after embedding the secret message .This is basically a performance metric and use to determine perceptual transparency of the watermark image with respect to cover image.It is measured in terms of decibel(db).Higher the PSNR higher the quality of the image(which means there is a little difference between cover image and watermark image)..Quality of the image is more when it is greater than 40db and less when PSNR is 30db or low.ie PSNR is measured in terms of MSE(Mean Square Error).Thus performance can be measured. PSNR is defined by using the following equation.

$$PSNR=10log10\ \frac{255^2}{MSE} \qquad (1)$$

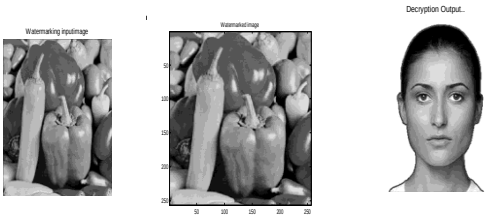
Where MSE is the mean square error and is calculated as

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\{I-W\}^2 \qquad (2)$$

Heare m and n are the rows and columns of the input images and is calculated by finding the difference between the input image and the watermark.As the MSE value decrease the PSNR value also decreases.

Another parameter that determines watermark image quality are various signal processing attacks like cropping,noises,filtering etc. The purpose of these attacks is to proof the robustness of the algorithm. We have tested three types of attacks which are reshaping ,adding noise and JPEG compression.But it is less affected since little loss in images will not results in much more loss.

## III. EXPECTING RESULTS




(a) (b) (c)

Fig (9)

As in the block diagram given in fig 1 the input image compressed,encrypted and then given for watermarking.The stage by stage output is shown above. Fig 9(a) is the watermarking input image,(b) is the watermarked output image ,then the encrypted output is decrypted and is obtained in (c) is the decrypted output.

## IV. CONCLUSION

The proposed scheme in this paper provides double security through encryption and watermarking.Encryption provides security by hiding the content of secret information;while watermarking hides the existence of secret information. The quality of the output is calculated by the PSNR calculation using MSE.

Future work is aimed by using some other compression schemes like JPEG-Ls or use some other watermarking techniques.



## REFERENCES

[1] A. V. Subramanyam, Sabu Emmanuel, "Robust watermarking of compressed encrypted JPEG 2000 images*," IEEE* transactions on multimedia, vol. 14, no. 3, june 2012

[2] R. Chandramouli, Nasir Memon, "Digital Watermarking," *(IJCSE)* International Journal on Computer Science and Engineering, vol. 2, 2010.

[3] Abdullah Bamatraf, Rosziati Ibrahim, "A new digital watermarking algorithm using combination of LSB and inverse bit," Journal of computing vol 3,issue 4,April 2011.

[4] William Stallings, "RC4 stream cipher encryption algorithm." vol 2, 2005.

[5] M. Rabbani and R. Joshi, "An overview of the JPEG 2000 still image compression standard," *Signal Process.: Image Commun.*, vol. 17, no. 1, pp. 3–48, 2002.

[6] Roger L. Claypoole, Jr. and Richard G. Baraniuk **"**Adaptive wavelet transforms via lifting."

[7] Mohan Vishwanath. Robert Michael Owens. and March JuneIrwin. "VLSI Architectures t'or the Discrete Wavelet transform." *IEEE Transaction of circuits and systems. -11:. Digitcil Sigizul Processing.* Vol. *52.* No. *5.* May, 1995.

[8] W. Sweldens,. "The lifting scheme: A construction of secondgeneration Wavelets.-' *7ech. Rep. / 993:6.* Industrial Mathematics Initiative. Department of Mathematics.Univcrsity of South Carolina. 1995.

[9] W. Sweldens. "The Lifting scheme: A custom-design construction of biorthogonal wavelets." *.+/d. Conipiit.*

[10] W**.** Sneldens. "The lifting scheme: A new philosophy in biorthogonal wavelet construction." In A.F.Lainc and M.U nser. editors. II

[11] Chin-Chi Liu. Yeu-Horng Shiau. and Jer-Min Jou. - 'Design and Implementation of a Progressive Image Coding Chip Based on the Lifted Wavelet Transform." *Proceeding of the VLSI Design'* August 2000. Taiwan; Chung-Jr Lian, Ktian-Ftr Chen, Hong-Hui *Chen, and Liang-Gee Chen* Lifting Based Discrete Wavelet Transform Architecture for JPEG2000, 2001 IEEE