An Optimization Technique for Image Watermarking Scheme

S.Veeramani [#1], *Y.Rakesh* [*2]

[#] Dept. of ECE, Srk Institute of Technology, AP, India

[*] Assistant Professor

Dept. of ECE, Srk Institute of Technology, AP, India

***Abstract*— In this paper, a robust watermarking scheme using optimization watermarking technique is proposed. In the proposed scheme, the watermark image is to embed in the SCS transform domain. The advantage is that they are able to detect malicious tampering while being robust against content-preserving processes such as compression, filtering and Salt and pepper noise, and we plotted graphs for average payload versus bitplanes to show the image quality for higher resolutions and studied PSNR, MSE for images.**

***Keywords*—** *Digital watermarking, RC4, DWT*

I. INTRODUCTION

Due to the increasing popularity and accessibility of digital manipulation and copying hardware and software, malicious tampering and illegal reproduction of multimedia in-formation has become difficult to detect. Digital rights management (DRM) has been an active area of research for the past decade, aiming to stop theft and tampering of digital media content. DRM was chosen as one of the top ten emerging technologies that would “change the world” by the MIT Technology Review [2]. The goal of DRM is to detect, track and possibly prevent unauthorized manipulations and distribution of intellectual property. Digital watermarking is one of the components of DRM that can be used to provide evidence of ownership and tampering. Digital watermarking has already been implemented in various products; however, its success is limited due to limited effectiveness and lack of legal support [3]. This thesis examines digital watermarking from application-oriented perspectives. Our aim is to advance the technology and propose cost efficient schemes to advance its use in protecting intellectual property and privacy.

Digital content has several advantages over analog content. It usually has higher quality and the quality does not degrade over time. Digital files are easy to edit: one can insert or delete information at exact locations. Also, unlike analog audio tape, film and VHS video, digital copies of original data have no loss in fidelity in general. Furthermore, digital content can be easily transmitted over a network such as the Internet. However, these advantages give rise to increasing concerns in copyright management and privacy protection. Traditional connection-based security systems such as encryption are not able to provide adequate protection because they do not prevent redistribution and modification once the original information is decrypted. One method to solve this problem is digital watermarking, in which an imperceptible mark is embedded into the protected file. The watermark can contain copyright information for authentication, a description of the file for tamper detection, or secret information for controlled access. Studies have been concentrated on watermarking for still images, digital audio and digital video. Typical block diagrams for digital watermark embedding and detection algorithms are shown in Fig. 1 and Fig. 2 respectively.

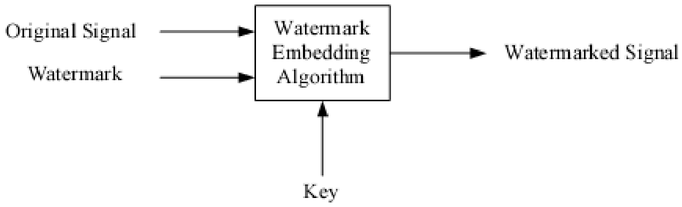


Fig. 1. A block diagram of a general watermark embedding system.

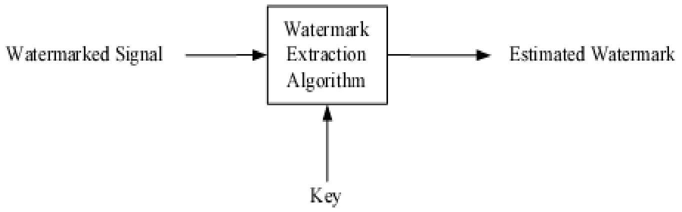


Fig. 2: A block diagram of a general watermark detection system.

In the watermark embedding system, a watermark, which is typically a binary bit sequence, is strategically inserted into the original signal so that the watermarked signal does not have any perceivable differences from the original. The use of a private key prevents unauthorized users from generating legitimate watermarked signals. The challenge for a watermarking system is to embed a perceptually insignificant mark that can survive losses and distortions in the transmission channel and still be able to be detected at the receiver.

II. RELATED WORK

A. *Encryption background*

Ciphering of digital images play a vital role since image data acquires more space than text data and also time is the important factor to be considered in case of encryption. The time is a factor very important for the image encryption [4]. There are two levels of time to be considered, the first is the time to encrypt, and the other is the time required to transfer images.

To mitigate above, the foremost step is to choose a robust, rapid and easiest method to implement cryptosystem. In pervious study, we have found some articles on image encryption: In 2000, Tarish [5] proposed image cryptographic system based on stream cipher as a tool for image encryption. In 2003, Pommer [6] two approaches of selective encryption where wavelet-based methods are used for compression. The first attempt was to hide the choice of filters, while the second approach of selective encryption was based on wavelet packets and the decomposition tree are keep secret. In the present work, the RC4 algorithm is developed to encrypt image with wavelet subband images (LL, HL, LH or HH).

III. PROPOSED SYSTEM

A. *DWT COMPRESSION*

The proposed technique first decomposes an image into coefficients called sub-bands and then the resulting coefficients are compared with a threshold.

Discrete wavelet transform is one of the main steps in JPEG2000 standard. By applying DWT to each tile image are decomposed into high and low subbands as illustrated in Figure 3

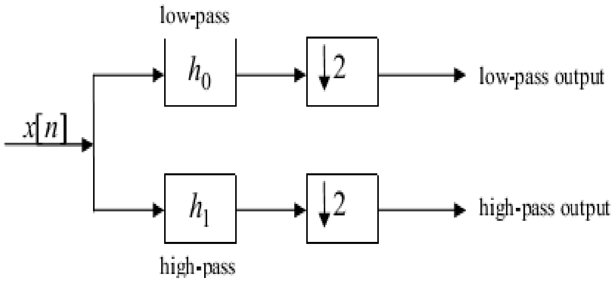


Fig. 3. The DWT principle scheme.

The DWT is performed by filtering each column and row of the preprocessed image tile with a high- and low-pass filters. Because this process is double the number of samples, the output from each filter is down sampled by 2, so that the sample rate remains a constant. At first are processed all columns and then all rows from the source image.

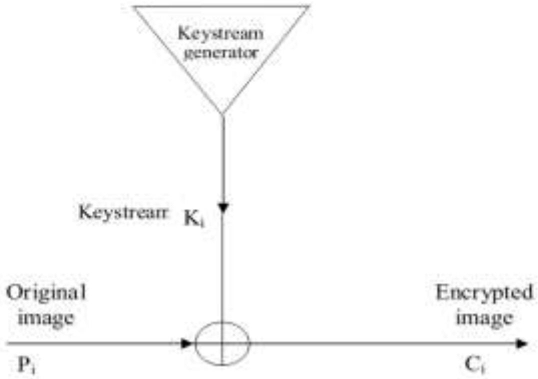
B. . *ENCRYPTION ALGORITHM*

RC4 Algorithm:

A secret key cryptosystem encrypt image pixel by pixel, with the RC4 algorithm. RC4 algorithm converts original image to encrypted image in bit by bit manner which is shown in Figure (4) [7].

RC4 system consists of two main parts:

1- Algorithm to generate key stream.
2- XOR gate.



.

Fig. 4. RC4 system

A key stream so called run key-generator which yields stream of bits in sequence as

K1, K2, K3… Ki

. $C_i = P_i \oplus K_i$ ………….. 1

This above generated key stream is further applied XORed operation with a stream of plaintext bits, P1, P2, P3… Pi to produce the stream of cipher text bits C1, C2 …Ci

C. EMBEDDING ALGORITHM

The encryption algorithm used is an additive privacy homomorphic one, so the watermark embedding is performed by using a robust additive watermarking technique. Since the embedding is done in the compressed ciphered byte stream, the embedding position plays a crucial role in deciding the watermarked image quality.

Hence, for watermarking, we consider the ciphered bytes from the less significant bit planes of the middle resolutions, because inserting watermark in ciphered bytes from most significant bit planes degrades the image quality to a greater extent. Also, the higher resolutions are vulnerable to transcoding operations and lower resolution contains a lot of information, whose modification leads to loss of quality.

We show how the watermark can be inserted in less significant bit planes of middle resolutions without affecting the image quality much. Since the embedding and detection are done on integer domain, the watermark is added after rounding off to the nearest integer for SCS-QIM.

SCS-QIM: In [8], Eggers et al.proposed SCS scheme for watermark embedding. In this scheme, given watermark strength, we choose a quantizer from an ensemble of quantizers to embed the watermark.

D. IMAGE QUALITY MEASURES

Peak signal-to-noise ratio (PSNR) is the quality metric method that is used for comparing a reconstructed image with that of original image. For an 8-bit grayscale image, the peak signal value is 255. Hence the PSNR of an M×N 8-bit grayscale image x and its reconstruction x is calculated as:

$$\mathbf{PSNR=10log_{10}\ 255^{2}\backslash MSE}$$ **……………1**

Where the mean square error (MSE) of any image is designated as:

$$MSE=\frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[x(m,n)-\hat{x}(m,n)]^2$$

……..2

Mean square error (MSE) is the sum of squares of difference between I and Iw.

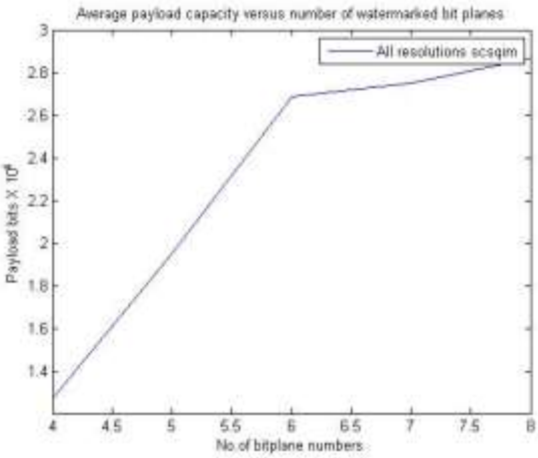


Fig.5 Average payload capacity versus number of watermarked bit planes

In Fig. 5 it is clear that as we move from lower bitplanes towards higher payload capacity increases, and the quality of the image is clear enough as increase in capacity payload which is due to increasing factor in dimensions size for higher resolutions that in turn generates large no.of compressed bytes that yields more space for embed purpose.

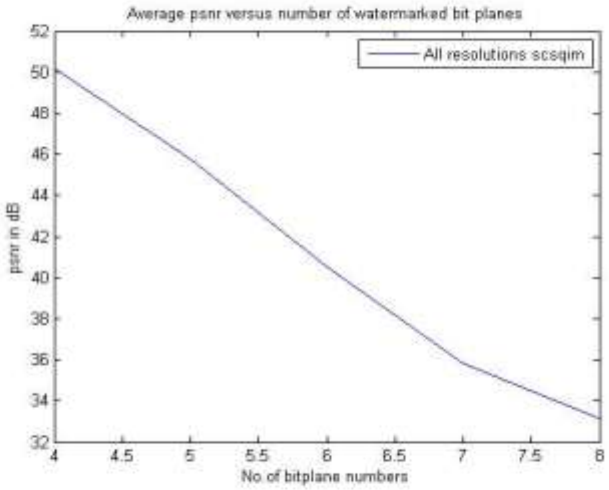


Fig.6 .Average PSNR versus number of watermarked bit planes

In Fig.6, as we move from lower bitplanes to higher PSNR decreases. However, the resolution 5 (HL1, LH1, HH1) has a higher PSNR in spite of high embedding capacity because the degradation caused due to watermarking higher resolution is lesser

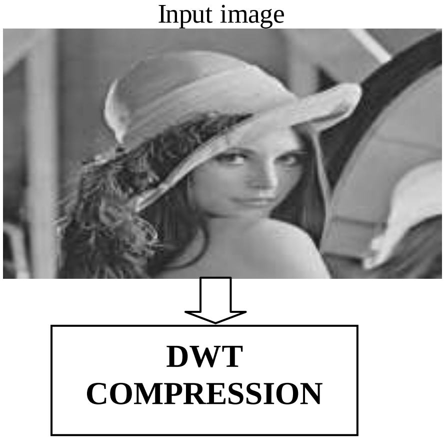
SALT AND PEPPER NOISE ATTACKS

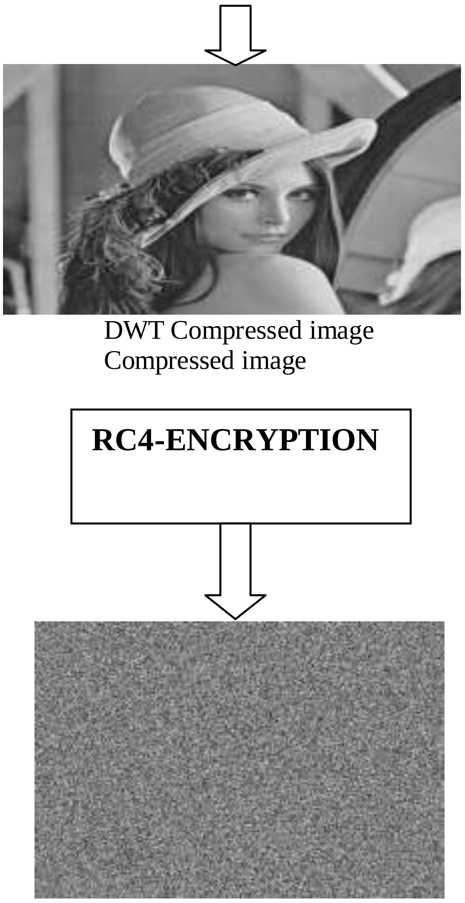
Noise is unwanted information which will contaminate the any digital image. Digital images that are corrupted by some sort of salt and pepper noise due to several reasons in which some are like faulty memory locations in hardware, damages in channel decoder and also during transmission through noisy channel etc.

When the digital images are corrupted or attacked by salt and pepper noise that will change pixel value to either minimal (0) or maximal (255) for any 8-bit gray scale images which will finally changes pixel intensity randomly to 0 or 255.

RESULTS AND DISCUSSION

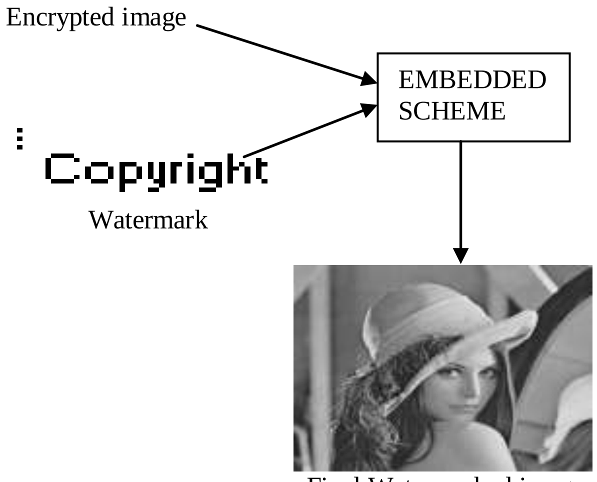
As we see applied this grayscale images to compression technique to get compressed image so that it consumes less space during transmission of image through channel and it is also encrypted to provide security and embedded watermark to show authentication and ownership.





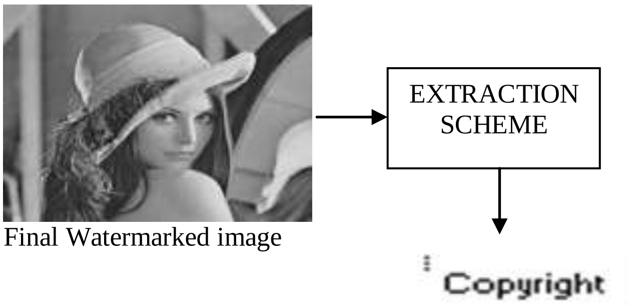
Encrypted image

Fig 7 Compressed & Encryption process



Final Watermarked image

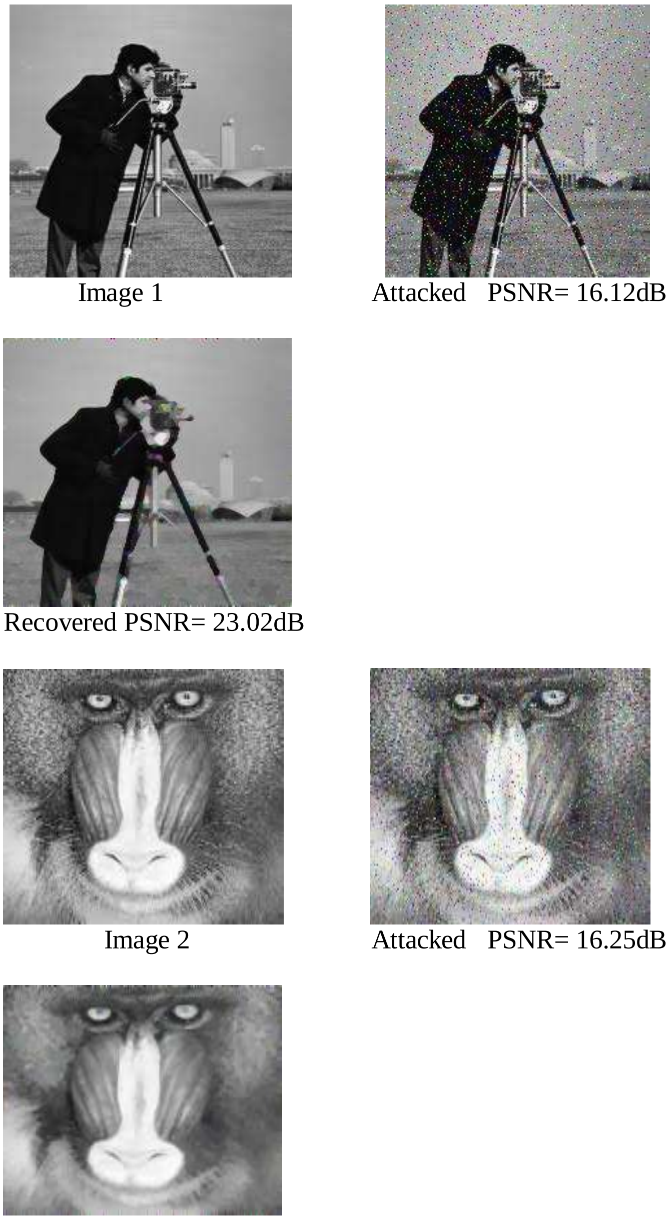
Fig 8 Embedding Scheme



Extracted watermark

Fig 8 Extraction Scheme

NOISE ATTACK ANALYSIS



Recovered PSNR= 21.17dB

Fig 9 Noise attack process

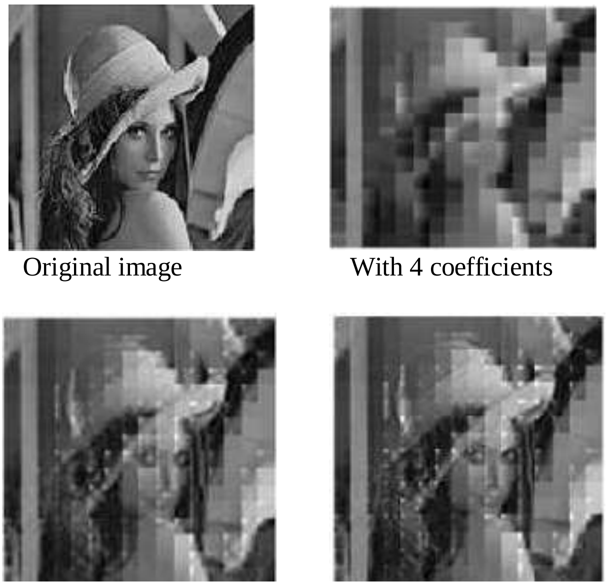
From fig 9 results shows PSNR of an attacked images is less than the recovred images indicates effectiveness of the scheme.

TABLE.1: Performance Comparison of DCT and DWT

IMAGES	COMPRESSION USED	PSNR	MSE
BABOON1	DCT	24.29	242.04
BABOON1	DWT	30.78	54.2
INDEX1	DCT	10.24	61.42
INDEX1	DWT	32.04	40.08
INDEX2	DCT	24.31	242.07
INDEX2	DWT	31.70	43.88

We have studied both DCT as well as DWT for both image compression and also decompression. By taking several images as inputs to the method, which is observed that MSE is low whereas PSNR is high in DWT than that of DCT based compression in all the 3 cases of different images.

JPEG Compression

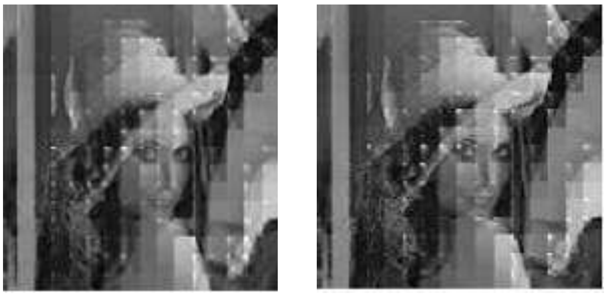


Original image

With 4 coefficients

With 16 coefficients

With 25 coefficients



With 40 coefficients

with 50 coefficients

Fig 10(a) to 10(f) JPEG compression Scheme

Fig 10(a) to Fig 10(f) show compressed images for the original Lena image after taking various numbers of coefficients for quantization.As the number of coefficients increases quality of the image increases whereas compression ratio continues to decreases. Fig 11 shows that SNR value increases with number of coefficients**.**

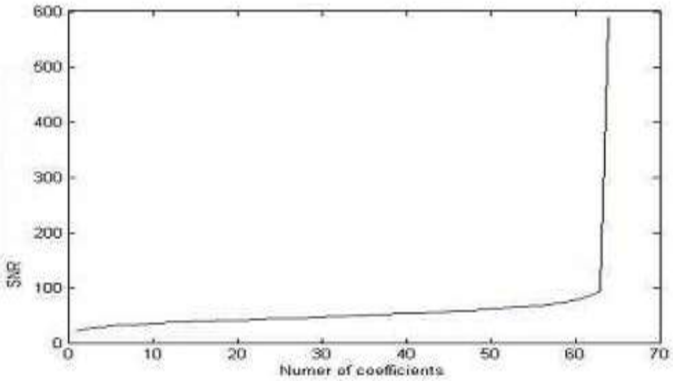


Fig 11 SNR vs. No.of coefficients

CONCLUSION

The proposed scheme shows robust watermark technique against compressed, salt and pepper noises attacks and requires less time to process images and provides security to images. Our analysis shows that the proposed method is more secure.

A comparative study of DCT & DWT shows that basic image compression can be achieved DCT that can be done by 8X8 image blocks for example JPEG compression. Similarly for achieving higher decoded image qualities can be accomplished with DWT for example JPEG2000 compression. Also our study proved that DWT compression superior than DCT technique.

REFERENCES

1. CI Podilchuk, EJ Delp, Digital watermarking: algorithms and applications. IEEE Signal Process. Mag. 18(4), 33–46 (2001)

[2] R. Singh. (2001, Jan.) Emerging technologies that will c hange the world: Digital rights management. MIT Technology

Review.[Online].Available:http://www.technology review.com/InfoTech/12264/

[3] Y.-L. Chang, "Who should own access rights? a game-theoretical approach to striking the optimal balance in the debate over digital rights management," Artificial Intelligence and Law, vol. 15, no. 4, pp. 323–357, Dec. 2007.

[4]. IJ Cox, J Kilian, FT Leighton, T Shamoon, Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process.6 (12), 1673–1687 (1997)

[5] Tarish A.H., "Designing and implementation a stream cipher cryptography system", MSc. Thesis, Computer Science Department, University of Technology, 2000.

[6] Pommer A.,"Selective Encryption of Wavelet-compressed Visual Data", PhD. Thesis, Department of Scientific Computing, Salzburg University, Austria, June 2003

[7]. V Solachidis, I Pitas, Circularly symmetric watermark embedding in 2-D DFT domain. IEEE Trans. Image Process.10, 1741–1753 (2001)

[8]. IJ Cox, J Kilian, FT Leighton, T Shamoon, Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process.6 (12), 1673–1687 (1997)

BIODATA.

Veeramani Surapaneni completed her B.Tech in Nova College of Engineering and Technology for women, jupudi in the year 2010 and presently she is Pursuing M.Tech Srk Institute of Technology, Eenikepadu in the 2013.

Rakesh.Y working as Assistant prof at SRKIT in the Dept. of ECE completed his M Tech at Vignan Engineering College and pursuing his PHD at Nagarjuna University. His areas of interest are signal processing and image processing