International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

An Efficient Novel Approach for Compressed and Encrypted Domain Watermarking in JPEG2000 Images

L.S.Shibil Jeyanthi Prasad[1], C. Kanmani Pappa[2], M.Subbulakshmi[3], Dr.M.Vijayaraj[4]

[1]PG Scholar, Dept of ECE, National College of Engineering, Tirunelveli, Tamil Nadu, India.
[2]Assistant Professor, Dept of ECE, National College of Engineering, Tirunelveli, Tamil Nadu, India. *[3]Assistant Professor, Dept of ECE, National College of Engineering, Tirunelveli, Tamil Nadu, India.* *[4]Associate Professor, Dept of ECE, Government College of Engineering , Tirunelveli, Tamil Nadu, India.*

[1]shibiljeyanthiprasad13@gmail.com
[2]kans_262@rediffmail.com
[3]subbu_june23@yahoo.co.in
[4]m_vijayaraj@yahoo.com

***Abstract*— This paper proposes an efficient approach for compressed and encrypted domain watermarking in JPEG 2000 images. Digital media content is distributed in compressed and encrypted format and watermarking of these media for copyright violation detection, media authentication, proof of distributorship or ownership. Watermarking in compressed-encrypted content saves the computational complexity and also preserves the confidentiality of the content. The proposal method is to choose an encryption scheme that is secure and will allow watermarking in a predictable manner in the compressed encrypted domain. The encryption technique is to be used is RC5. The proposed technique embeds watermark in the compressed-encrypted domain, and the extraction of watermark in the decrypted domain. The robustness, embedding capacity, perceptual quality and security of the proposed encryption algorithm is to be investigated using the watermarking schemes like Spread Spectrum (SS),Scalar Costa Scheme Quantization Index Modulation (SCS-QIM) , and Rational Dither Modulation (RDM).**

***Keywords*— Compressed and encrypted domain watermarking, JPEG2000, RC5**

I. INTRODUCTION

In the past few decades, a phenomenal growth for digital media content capturing, processing and distribution have increased .This media content is distributed in compressed and encrypted format. Watermarking of these media for copyright violation detection, media authentication, proof of distributorship or ownership. In DRM systems [10] where the owner of multimedia content, distributed in a compressed and encrypted format to consumers through multilevel distributor network. For digital content delivery DRM system is used. They are distributors of content who distributes the encrypted content and requests the license server in the DRM system to distribute the associated license containing the decryption keys to open the encrypted content to the consumers. Each distributor needs to watermark the content for proving the distributorship, media authentication .Watermark in the compressed encrypted domain is to be done .

In this paper we focus on an efficient approach for compressed and encrypted domain watermarking in JPEG 2000 images. In [9] Deng et al. proposed an efficient buyer-seller watermarking protocol based on composite signal representation. Here the content is accessible only in encrypted form to watermark .In [6] Prins et al. proposed a robust quantization index modulation (QIM) based watermarking technique, in the encrypted domain where watermark is embedded.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Technique here is the addition or subtraction of a watermark bit to a sample is based on the value of quantized plaintext sample. In [5] Li et al. proposed a content-dependent watermarking technique, which embeds the watermark in an encrypted format, but the signal is in the plain text format.

To overcome the drawback of the existing system the proposed system is developed. The proposed system uses a novel technique to embed a watermark in the JPEG2000 compressed encrypted images. The algorithm is directly performed in the compressed-encrypted domain. It does not require decrypting or partial decompression of the content. To encrypt the image the RC5 encryption algorithm is used.

The rest of the paper is organized as follows: in Section II the main stages of the proposed method are described. Section III shows the experimental results, Finally, Section IV provides conclusions and some future work lines.

II. METHODOLOGY

The proposed method consist of the following three modules. They are encryption algorithm Embedding algorithm and Watermark detection.

First for JPEG2000 compression the input image of 512x512 pixel image are taken . Now the image is divided into non-overlapping rectangular tiles format, the unsigned samples are reduced by a constant to make it symmetric around zero. Finally a multi-component transform is performed. Then the discrete wavelet transform (DWT) is applied followed by quantization. Multiple levels of DWT give a multi-resolution image. The higher resolution contains the high-pass image while the lowest resolution contains the low-pass image .These resolutions are divided into smaller blocks known as code-blocks. Here each code-block is encoded independently. Then 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. Thus, it is possible to select bytes generated from different bit planes of different resolutions for encryption and watermarking. The proposed algorithm uses a block cipher. The Block diagram is shown in the below figure

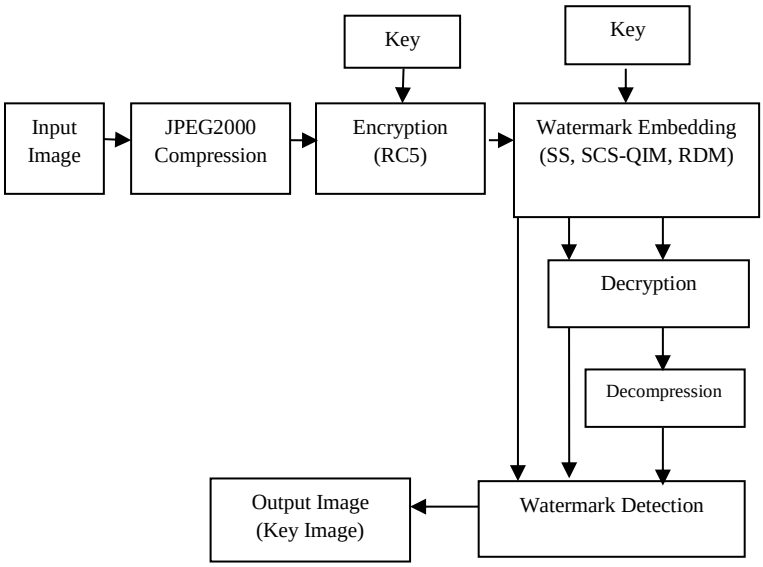
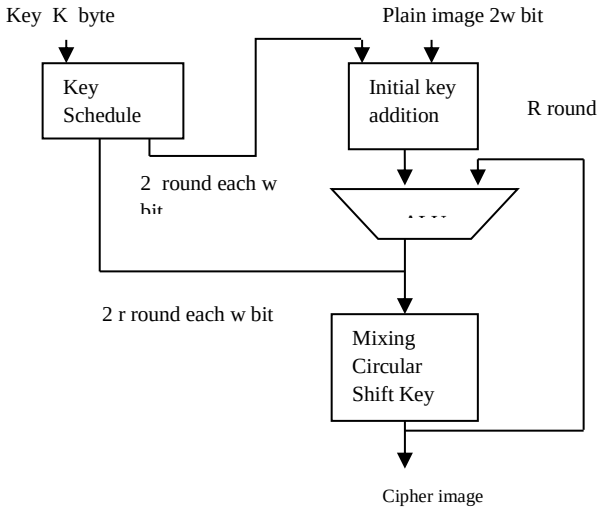


Fig 1. Watermark embedding and Extraction

A. *Encryption algorithm*

JPEG2000 gives out packetized byte stream as its output. In order to encrypt the message, we choose RC5 encryption algorithm. Then the encryption is done byte by byte to get the ciphered signal.



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Fig 2. RC5 encryption

In December 1994 Ronald Rivest designed RC5 encryption algorithm. RC5 is a fast block cipher. RC can be expressed as "Rivest Cipher", or "Ron's Code" (compare RC2 and RC4). Based on RC5 the Advanced Encryption Standard (AES) candidate RC6 . It consist of simple encryption routines which is easy to analyse and implement. RC5 has a variable block size (32, 64 or 128 bits), number of rounds (0 to 255) and key size (0 to 2040 bits) to provide flexibility in performance and security .Choices of parameters were a 128-bit key, a block size of 64 bits and 12 rounds.

RC5 has a key feature of data-dependent rotations which is good against different types of attacks. RC5 can be implemented both on hardware and software. RC5 consists of a number of modular additions and exclusive OR (XOR) s. The general structure of the RC5 algorithm is a Feistel-like network. Few lines of code can be specified by the encryption and decryption routines. However key schedule is more complex, the key can be expanded using one-way function with the binary expansions. The RC5 algorithm is basically denoted as RC5-w/r/b where r=number of rounds, w=word size in bits, b=number of 8-bit byte in the key.

B. Embedding algorithm

The RC5 encryption algorithm used is an additive privacy, using a additive watermarking technique the watermark embedding is performed . Since the embedding is done in the compressed ciphered byte stream, the watermarked image quality is decided by the embedding position. Hence, for watermarking, ciphered bytes from most significant bit planes degrades the image quality to a greater level so we choose inserting watermark in the ciphered bytes from the less significant bit planes of the middle resolutions.

Also, the higher resolutions are vulnerable to trans coding operations and lower resolution contains a lot of information and its modification leads to loss of quality. Study of impact on quality of watermarking in this compressed-encrypted domain is done using this experiment. Here how the watermark can be inserted in less significant bit planes of middle resolutions without affecting the image quality much is shown. Since the embedding and detection are done on integer domain, for SCS-QIM and RDM the watermark is added after rounding off to the nearest integer. The rounding off process decreases the watermark power or introduces noise and its effect on detection performance is given. Now we can explain the embedding process.

1. SS Watermarking

Many different watermarking methods for images have been proposed. Most of them are based on ideas known from spread spectrum radio communications, namely watermark recovery and additive embedding of a pseudo-noise watermark pattern by correlation.

Here the embedding process is performed using spread spectrum watermarking scheme. For embedding process the watermark signal W are generated by using watermarking information bits b ,chip rate r and PN sequence P .The watermark information bits b=$\{b_i\}$, where b_i=$\{1,-1\}$, are spread by r ,can be given as

$$a_j = b_i, \qquad ir \le j < (i+1) \tag{1}$$

The a_j sequence is multiplied by $\alpha > 0$ and P. Then the watermark signal $W = \{w_j\}$, where

$$w_j = \alpha a_j p_j \tag{2}$$

Now the watermark signal generated is added to the encrypted signal C, to give the watermarked signal C_w

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

$$C_w = C + W = c_{w_i} = c_i + w_i \quad \forall = 0,1 \dots L-1 \qquad (3)$$

2. SCS-QIM Watermarking

Here the watermark embedding process is performed with SCS-QIM scheme.We choose an ensemble of quantizers to embed the watermark. In the binary watermark $\in \{0,1\}$, the quantizer can be preferred as

$$U = \left(l + k_{qim_i}\right)\beta\Delta + w\beta\,\Delta/2 \quad \forall_i = 0,1 \dots . L-1 \quad (4)$$

The watermark sequence is then given by

$$W = \beta q \qquad (5)$$

And now the embedding is done as

$$C_w = C + W \qquad (6)$$

3. RDM Watermarking

RDM watermarking is based on quantization of the ratio of host signal to a function and the quantizes are given by

$$Q'_{\Delta} = 2\Delta + w\,\Delta/2 \qquad (7)$$

The embedding rule can be written as

$$c_{w_i} = g\; c_{w_{i-1}} Q'_{\Delta}\left(\frac{c_i}{g\left(c_{w_{i-1}}\right)}\right) \quad \forall = 0,1 \dots L-1 \quad (8)$$

Where c_{w_i} - current watermarked samples

$c_{w_{i-1}}$ - previous watermarked samples

$$w_i = c_{w_i} - c_i \qquad (9)$$

Thus the watermark is embedded in the compressed encrypted domain.

C. Detection of Watermark

Final stage of our project is the detection of watermark. Either in encrypted or decrypted compressed domain the watermark can be detected. Now we can explain the detection in encrypted domain followed by decrypted domain.

a) Encrypted Detection Domain

In the encrypted domain C_w is directly given to the extraction module for watermark detection.

SS Watermarking

The encrypted watermarked signal which is received from the previous section $C_w = C + W$ is applied to the correlator detector .Then it is multiplied by PN sequence which is used for embedding, summation over chip-rate window , yielding the correlation sum .

$$S_i = \sum_r (c_{w_j} p_j) = \sum_r (c_j + w_j) p_j = b_i \sigma_p^2 \alpha \qquad (10)$$

Here $c_j p_j$ is zero if C and P are uncorrelated. This cannot be applied always for real compressed data. We can subtract away C from $C_w$to remove the correlation effect completely to get a better watermark detection rate. The watermark information bit is given by sign S_i

$$sign\,(S_i) = sign\left(b_i \sigma_p^2 \alpha r\right) = sign(b_i) = b_i \qquad (11)$$

SCS-QIM Watermarking

SCS-QIM Watermarking can be estimated by quantizing the received signal

$$\widehat{w} = Q_{\Delta}\left(c_{w_i}\right) - c_{w_i} \qquad \forall = 0,1 \dots L-1 \qquad (12)$$

If $\widehat{w}$ is close to zero, then watermark bit is extracted and if close to, then bit is retrieved.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

RDM Watermarking

In RDM watermarking the detection of watermark is performed by the minimum distance criteria. The equation can be given as

$$\hat{w}=\text{argmin}_1 -1 \left(\frac{c_i}{g\left(c_{w_{i-1}}\right)} - \quad Q'_{\Delta} \quad \left(\frac{c_i}{g\left(c_{w_{i-1}}\right)}\right)\right) \quad \forall= 1 \dots L-1 \qquad (13)$$

Here gives two quantizers belonging to bits 1 and -1. The distance is computed to both the quantizers and the one which gives minimum distance gives the watermark bit.

b) Decrypted Detection Domain

Now the received compressed encrypted watermarked image is passed through the decryption module and the key stream can be generated.

$$M_w = D\ (C_w, k) = \left(\ c_{w_i} - k_i\right) mod 255 \quad \forall= 0,1 \dots L-1 \qquad (14)$$

c) Decompressed Detection Domain

In the decompressed detection domain I_{DW} is the decompressed-watermarked image, I_{DU} is the decompressed original image, and I_{DWA} is the decompressed-watermarked-attacked image. The watermark signal in decompressed domain can be computed as $\widehat{W} = I_{DU} - I_{DW}$ and in case of attack, $\widehat{W} = I_{DU} - I_{DWA}$. For decompressed detection, a

$$= (c_i + w_i - k_i) mod 255$$

$$= m_i + w_i$$

$$= m_{w_i}$$

The embedded watermark information W can be estimated from M_w using correlation detector without the knowledge of originals M or C in SS detection. In order to obtain better detection results, we can encrypt $M_w$with K which gives C_w and removing C.

Similarly for RDM and SCS-QIM, the decrypted message M_w along with cipher key k is fed to the watermark extraction module. Then the signal M_w is encrypted with the key k with the methods as described. Thus, we get the ciphered watermarked signal C_w and the watermark is detected.

correlation measure between embedded and attacked watermark signal is computed as

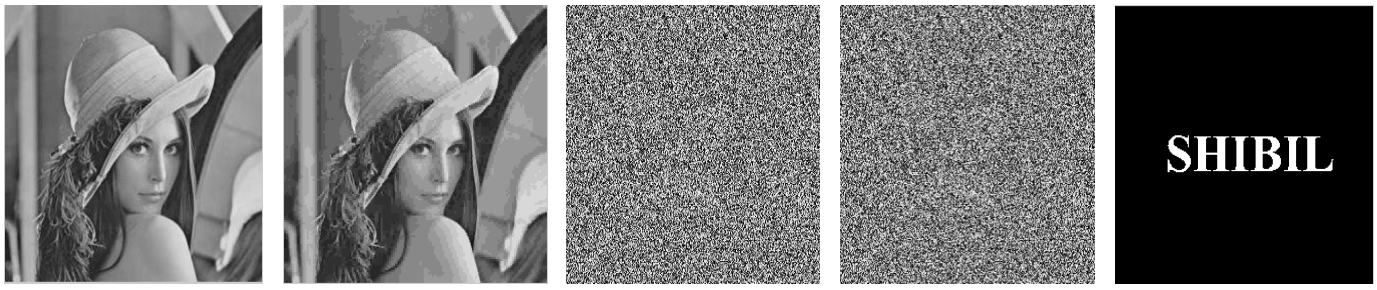
$$corr\left(\widehat{W}_i, \widetilde{W}\right) = \frac{E\left[\left(\widehat{W}_i - \mu_{\widehat{W}_i}\right)\left(\widetilde{W} - \mu_{\widetilde{W}}\right)\right]}{\sigma_{\widehat{W}_i}\sigma_{\widetilde{W}}} \quad \forall_i = 1,2 \dots N_w \qquad (15)$$

Where E [.]- correlation measure which denotes the expectation operator

μ - mean

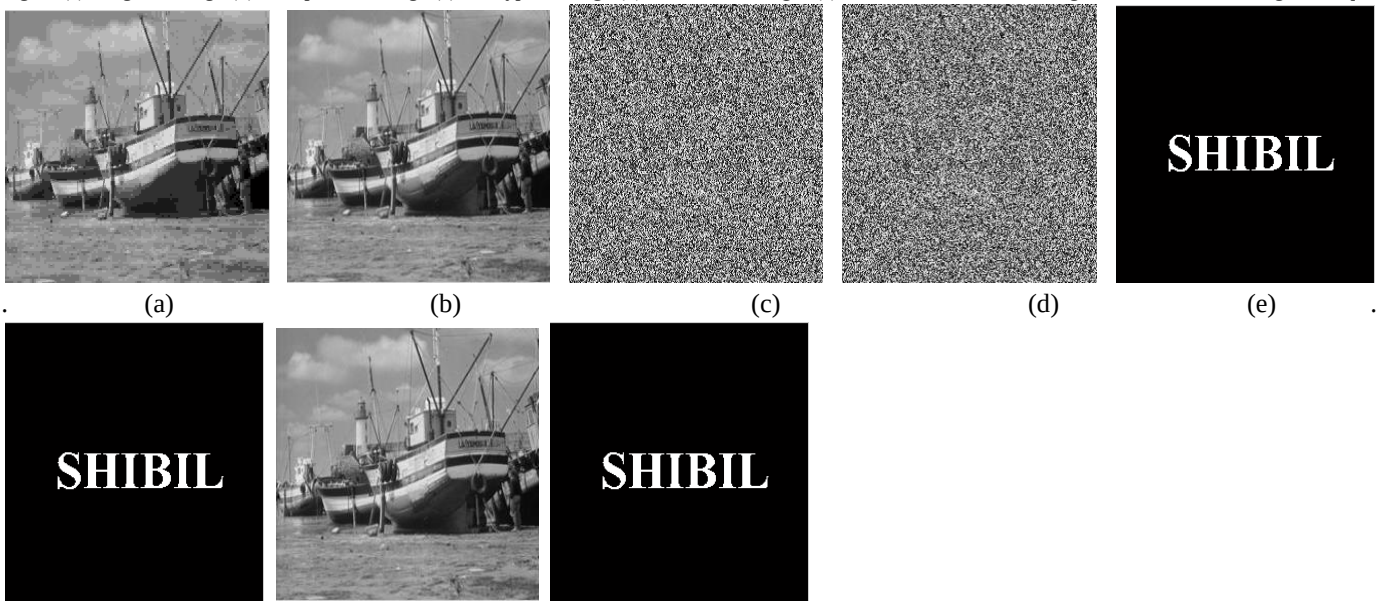
σ^2- variance.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)



(a) (b) (c) (d) (e)

Fig 3. (a) Original image.(b) Compressed image.(c) Encrypted image.(d) Embedded image. (e) Watermark detected image ,for SS watermarking technique

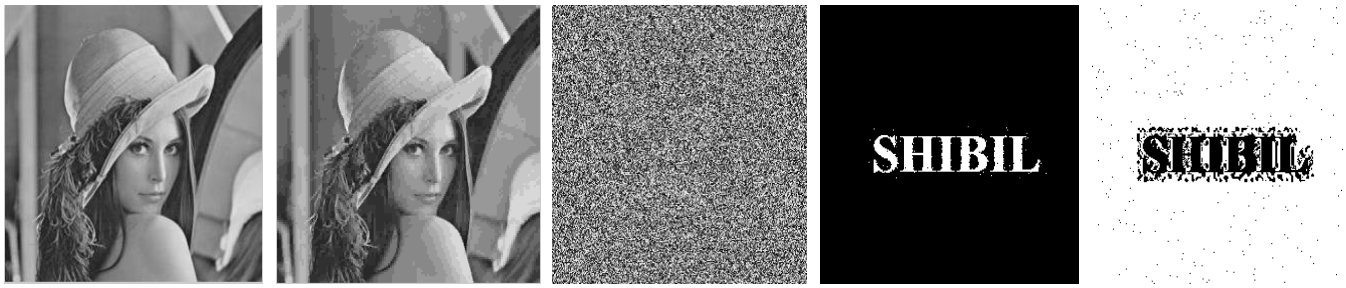


. (a) (b) (c) (d) (e) .

(f) (g) (h)

Fig 4. (a) Original image.(b) Compressed image.(c) Encrypted image.(d) Embedded image. (e) Watermark detected image
(f) watermark detected image after decryption (g) recovered image (h) Watermark detected image ,for SCS-QIM watermarking technique

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)



. (a) (b) (c) (d) (e)

(f) (g) (h)

Fig 5. (a) Original image.(b) Compressed image.(c) Encrypted image.(d) Embedded image. (e) Watermark detected image
(f) watermark detected image after decryption (g) recovered image (h) Watermark detected image ,for RDM watermarking technique

III. Experimental Results

To evaluate the performance of the binarization techniques several performance metrics are available. We use the Payload and PSNR to analyses the performance

1) Pay Load

The payload capacity for the number of watermarked bit planes means the bit planes are watermarked. The average payload capacity versus number of bit planes watermarked under different resolutions using SCS-QIM scheme. The payload capacity does not vary too much for SS,SCS-QIM and RDM, only the average payload for all the resolutions are plotted for SS and RDM schemes.

Average payload capacity is given here as the ratio of the average embedded number of bits to the average compressed stream size (in bytes), where average is computed as a simple mean.

2) Peak Signal-to-Noise-Ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between the attacked image and the original image. The PSNR formula is written as

$$PSNR = 10\ X\ log_{10} \frac{255\ X\ 255}{\frac{1}{HXW}\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}[f(x,y)-g(x,y)]^2}\ dB \quad (16)$$

Where W -width of the image and H - height of the image

f(x, y) - the grey levels located at coordinate (x, y) of the original image

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

g(x, y)- the grey levels located at coordinate (x, y) of the attacked image

Table I. Pay Load Value

L	All Resolutions Payload(Bits)
6	9807
7	19489
8	30412
9	38663
10	42534
11	44887

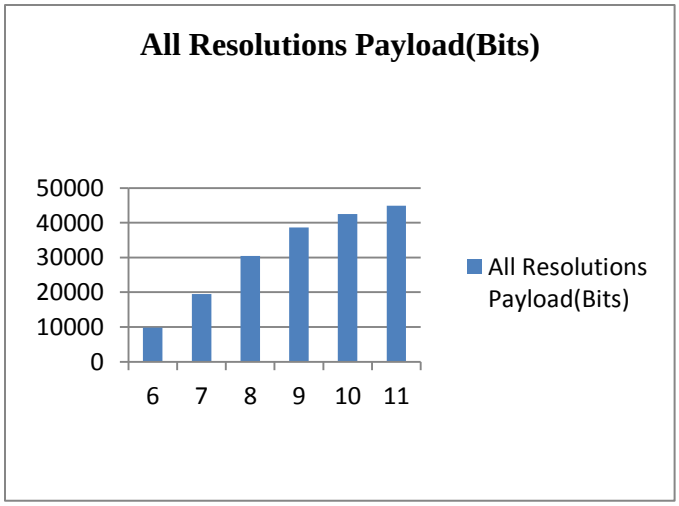


Fig 6.Chart for payload value

Table II. PSNR Value

L	All Resolutions PSNR(dB)
6	33.6
7	27.45
8	21.06
9	16.81
10	11.4
11	7.7

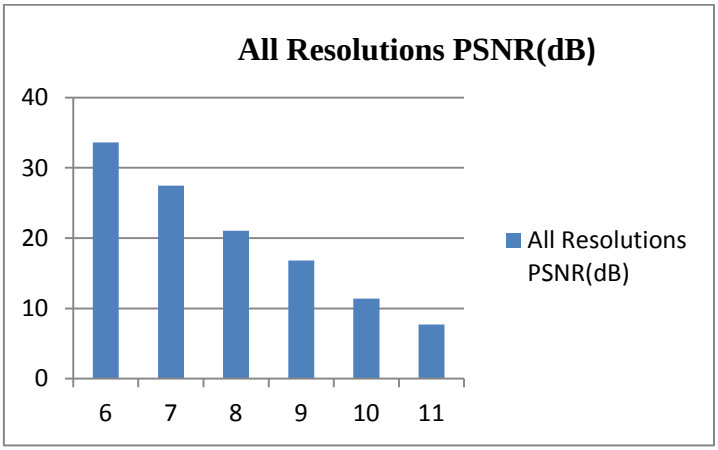


Fig 7.Chart for PSNR value

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

IV. Conclusion

In this project we proposed an efficient approach for compressed and encrypted domain watermarking in JPEG 2000 images using three different existing watermarking schemes. The RC5 algorithm is easy to analyse and for implementation. This algorithm is directly performed in the compressed-encrypted domain. There is no partial decompression or decrypting of the content are required. Our schemes preserves the confidentiality of content as the embedding is done on encrypted data. It helps to detect the watermark after decryption and control the image quality. In compressed or decompressed domain the detection is carried out . Using experimental results we analysed the relations between payload capacity and PSNR for different resolutions.

Future work aims at extending the proposed method of RC6 encryption algorithm can be used for encryption. Comparison will be performed using RC4, RC5 and RC6.

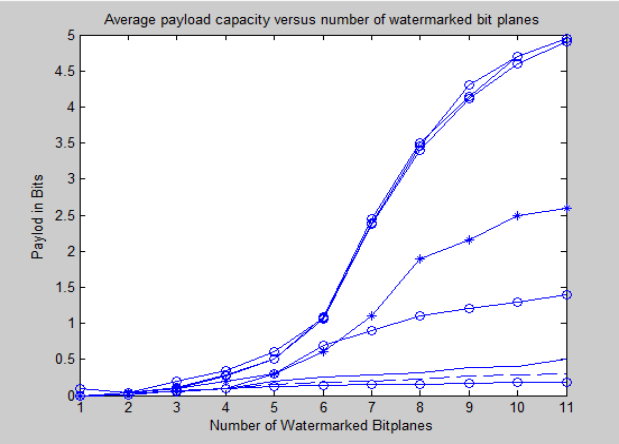


Fig 8. Average payload capacity versus number of watermarked bit planes

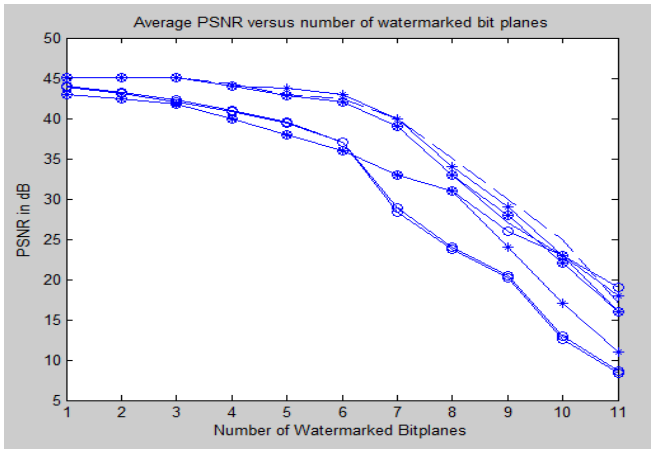


Fig 9. Average payload versus PSNR under different resolutions

V. References

[1] S.P.Mohanty, K.R. Ramakrishnan,M.S. Kanakanhalli, "A dual watermarking technique for images, Proceedings of the 7th ACM International Multimedia Conference" (ACMMM), Florida, USA, vol. 2, 1999, pp. 49–51.

[2] H. Wu and D.Ma, "Efficient and secure encryption schemes for JPEG2000," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, 2004, vol. 5, pp. 869–872.

[3] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proc. 2nd Annu. Int. Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005)*, 2005, pp. 109–117.

[4] Abrardo, M. Barni, F. Pérez-González, and C. Mosquera, "Improving the performance of RDM watermarking by means of trellis coded quantisation," *IEEE Proc. Inf. Security*, vol. 153, no. 3, pp. 107–114, 2006.

[5] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," *Opt. Eng.*, vol. 45, pp. 1–3, 2006.

[6] J. Prins, Z. Erkin, and R. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," EURASIP J. Inf. Security, vol. 2007.

[7] G. Schaefer and M. Stich, "UCID—An uncompressed colour image database," *Multimedia Syst.*, vol. 15, no. 4, pp. 243–270, 2009.

[8] Langelaar, Emir Ganic Ahmet M. Eskicioglu, "Reversible Watermarking approach for JPEG and MPEG Stream", Proceedings of the 7th ACM International Multimedia Conference (ACMMM), Florida, USA, vol. 2, 2009, pp. 49–51.

[9] M. Deng, T. Bianchi,A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[10] Subramanyam, S. Emmanuel, and M. Kankanhalli, "Compressed encrypted domain JPEG2000 image watermarking," in *Proc. IEEE Int. Conf. Multimedia and Expo*, 2010, pp. 1315–1320.

[11] Emir Ganic Ahmet M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", IEEE Signal Process Lett. 17 (6) (2010) 567–570.

[12] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans. Inf. Forensics* Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[13] Gaurav Bhatnagar, Balasubramanian Raman, "A new robust reference watermarking scheme based on DWT-SVD", IEEE Trans. Inf. Technol. Biomed. 13 (2) (2011) 158–165.

[14] Kwon,Ruizhen Liu, Sheetal Sharma,"A Novel Approach for reversible watermarking technique using Block based DCT", IEEE Trans. Circuits Syst. Video Technol. 16 (1) (2011) 129–133.

[15] Ruizhen Liu, Tieniu Tan, "A SVD-Based Watermarking Scheme For Protecting Rightful Ownership", IEEE Multimedia 13 (2) (2012) 60–66.