DIGITAL IMAGE WATERMARKING OF COMPRESSED IMAGE USING JPEG2000 AND ENCRYPTION TECHNIQUES

Bhagyashri D. Shende
Department of M.E. Electronics,
Walchand Institute of Technology, Solapur University,
Solapur, Maharashtra, India

Prof. Mrs. R. J. Shelke
Department of M.E. Electronics,
Walchand Institute of Technology, Solapur University,
Solapur, Maharashtra, India

ABSTRACT

The necessity for copyright protection, ownership verification, and other issues for digital data are getting more and more value these days. For the rapid revolution in digital multimedia and the ease of creating similar and unauthorized data, the digital data can be copied or manipulated or distributed. So it is necessary to watermark the media content for tamper proofing or quality assessment or copy control. In this paper we propose a JPEG2000 compression. The compression standard is chosen such that it provides higher compression ratio and the compressed byte stream are randomized by the encryption algorithm. In our paper watermarking was done in the compressed – encrypted domain. We use different watermarking techniques for this. Attempting to watermark such a randomized bit stream can cause a dramatic degradation of the media quality. Thus it is necessary to choose an encryption scheme that is both secure and will allow watermarking in a predictable manner in the compressed encrypted domain. The projected method is a robust watermarking algorithm to watermark JPEG2000 compressed and encrypted images (grayscale) of size 512×512. The encryption algorithm in this paper uses stream cipher. While the estimated technique embeds watermark in the compressed-encrypted domain, and the extraction of watermark can be done in the encrypted domain. The proposed algorithm also conserves the confidentiality of data as the embedding process can be done on encrypted data. The planned method can examine the PSNR and the security of the proposed algorithm, using the watermarking scheme: Spread Spectrum (SS) and Scalar Costa Scheme Quantization Index Modulation

KEYWORDS: *JPEG2000 Compression standard, Stream Cipher algorithm, Watermarking Technique such as SS (Spread Spectrum), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM).*

INTRODUCTION

Digital watermarking is the process of embedding data into digital multimedia content such that the data which we call the watermark can later be extracted or detected for a variety of purposes including copy prevention and control. Fundamentally, Digital Asset Management System (DAMS) include various assets like image, audio, video, logo etc. Mainly, DAMS means the combination of hardware, software, professional services that provides central location for storing, managing, retrieving the digital assets [3]. These assets contain some additional information hence it is open to only intended users. The owner of multimedia content distributes these assets to consumer through multiple levels of distributers. As distributors are not consumers hence they can't access the original message. Hence it is necessary to compress and encrypt digital assets before its distribution. Sometimes there is risk of losing the data for this reason watermarking should be done for copyright protection. [2] So the projected method introduces a robust watermarking technique for JPEG2000 images (grayscale) of size 512×512 in which watermark can be embedded in predictable manner in compressed an encrypted byte stream. This technique uses JPEG2000 compression standard which provides lot of benefits over JPEG such as ROI capacity, transmission in noisy environment, high compression efficiency, etc. As the compression provides less transmission time and less it reduces storage space requirement hence compression can be done before encryption. The grouping of encryption and watermarking gives robust security of image. This watermarking algorithm can be evaluated by investigating the watermarked image quality using the watermarking scheme: Spread Spectrum (SS) and Scalar Costa Scheme Quantization Index Modulation [1], [3]. The section II describes the methodology of proposed system; section III describes the different performance metrics which are used for analyzing the whole system, section IV gives the experimental results and section V describes performance analysis in the form of conclusion.

PROPOSED SCHEME

In the proposed algorithm, the image is compressed using JPEG2000 standard and encrypted, the watermark is embedded on the compressed and encrypted domain and extraction of watermark is done from encrypted domain.[1] Consider the following block diagram which gives overall idea about the proposed scheme.

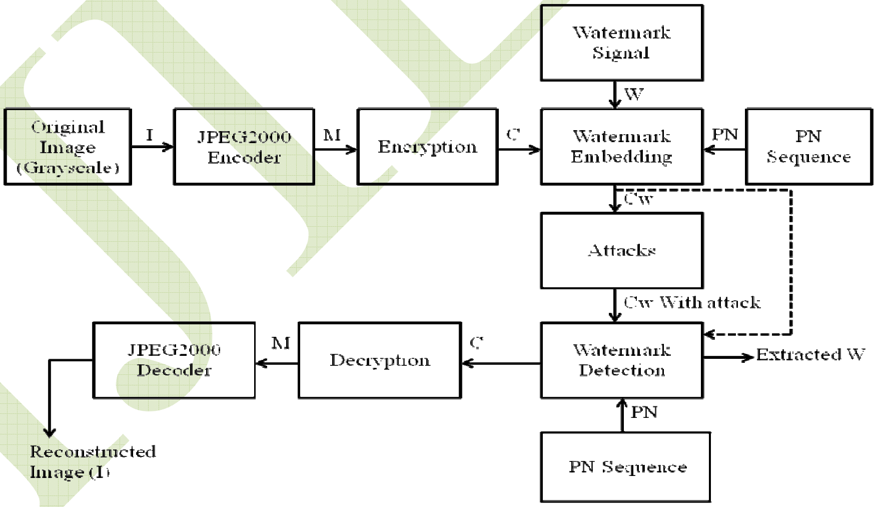


Fig: 1: Block Diagram of Proposed Scheme

Considering the above situation of proposed technique, first image can be taken and it is compressed using JPEG2000 compression standard. After that, the output of JPEG2000 encoder is code stream and is encrypted using stream cipher algorithm. The encrypted data is given to the block embedding watermark as an input. The watermark is embedded in the encrypted data using the two different watermarking techniques: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM). After embedding a watermark in an encrypted data, the watermark can be detected from the encrypted watermarked data then it can be decrypted & decompressed to get the original image.

A. JPEG2000 Compression

JPEG 2000 is a new image compression standard and coding system. It was produced by the Joint Photographic Experts Group committee in 2000 with the intention of superseding their original discrete cosine transform-based JPEG standard with a newly planned, wavelet-based technique [1], [13]. The standardized filename extension is .jp2. The following figure shows the functional diagram of JPEG2000 encoder and decoder.

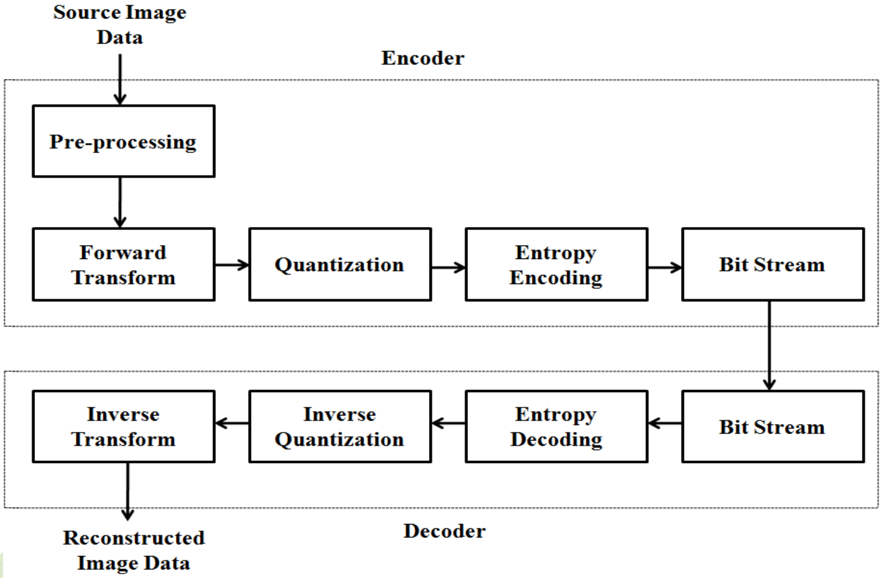


Fig: 2: JPEG2000 Encoder and Decoder

In JPEG 2000 encoder stage, the input source image data is given to the pre-processing stage. In pre-processing, DC level shifting is done. After that DC level shifting operation is performed. The purpose of DC level shifting is to make sure that the input image samples have a dynamic range that is approximately centered on the zero. The next footstep is Quantization. After transformation, all coefficients are quantized. Quantization is the process by which the coefficients are reduced in precision. This operation is lossy, unless the quantization step is 1 and the coefficients are segments in the compressed bit stream. The output of pre-processing unit is given to the forward transform. In JPEG 2000 Discrete Wavelet Transform (DWT) is used to decompose each tile component into different sub bands. Multiple levels of DWT give a multi-resolution image. After that encoding process occurred. In JPEG 2000 Huffman Encoding is used for encoding the quantized coefficients. Huffman coding is based on the frequency of occurrence of pixel in images. Finally we get the compressed bit stream [18]. If we increase the DWT decomposition level then compression ratio increases means it requires less space for storage. Consider the example of lena.png image which is of size 512x512 means 262kb and size of compressed data is 4kb. Hence compression ratio is 67.993 for DWT decomposition level 4.

B. Encryption and Decryption

A secure symmetric stream cipher with homomorphic property is used for encryption here. It is essentially used due to the following reasons. Symmetric ciphers with homomorphism can be applied on a smaller message size, like a byte. So there is a tradeoff between security-compression efficiency-payload capacities, which poses a challenge for deciding which cipher scheme to apply. [4], [5]. So it uses the RC4 stream cipher with homomorphism property. It uses a variable sized key that can range between 8 and 2048 bits in multiples of 8 bits. The RC4 algorithm generates a pseudo-random key stream that is then used to generate the cipher text. It is called pseudorandom because it generates a sequence of numbers that only approximates the properties of random numbers. The key stream is generated from a variable length key using an internal state composed of the following elements:

a. A 256 bytes array (denoted S) containing a permutation of these 256 bytes
b. Two indexes i and j, used to point elements in the S array (only 8 bits are necessary for each index since the array only have 256 elements). Once the S array has been initialized and shuffled with the key-scheduling algorithm (KSA), it is used and modified in the pseudo-random generation algorithm (PRGA) to generate the key stream [10] [14].

a) Key scheduling algorithm

The key-scheduling algorithm is used to generate the permutation array. The first step of this algorithm consist in initializing the S table with the identity permutation: the values in the array are equal to their index.

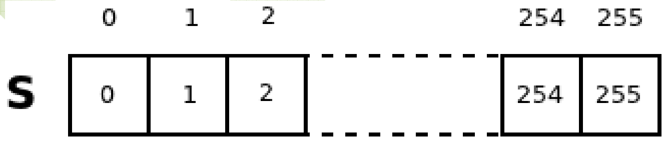


Fig.6: S Table

Once the S array is initialized, the next step consists is shuffling the array using the key to make it a permutation array. To do so, we simply iterate 256 times the following actions after initializing i and j to 0:

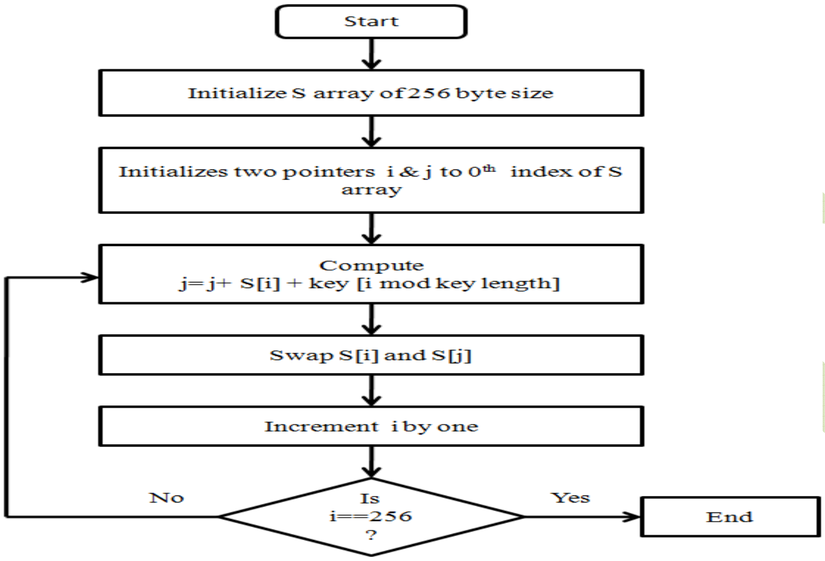

Start
Initialize S array of 256 byte size
Initializes two pointers i & j to 0th index of S array
Compute
j=j+ S[i] + key [i mod key length]
Swap S[i] and S[j]
Increment i by one
Is i==256 ?
No
Yes
End

Fig.7: Key Scheduling Algorithm

Once i have reached 256, the S array has been properly initialized. Now that the S array is generated, it is used in the next step of the RC4 algorithm to generate the key stream.

b) The pseudo-random generation algorithm

This step of the algorithm consists in generating a key stream of the size of the message to encrypt. This algorithm enables us to generate a key stream of any size. To do so, we first initialize the two indexes to 0 and we then start the generation of the key stream one byte at a time until we reached the size of the message to encrypt. For each new byte to compute we do the following actions:

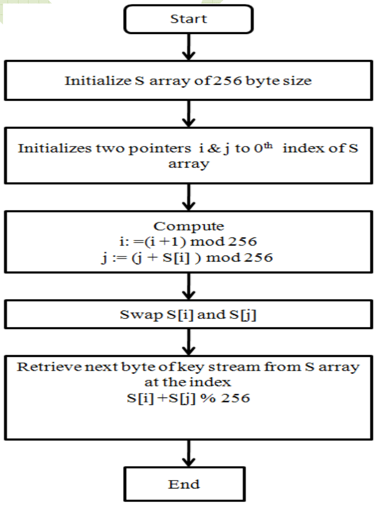

Start
Initialize S array of 256 byte size
Initializes two pointers i & j to 0th index of S array
Compute
i: =(i +1) mod 256
j := (j + S[i]) mod 256
Swap S[i] and S[j]
Retrieve next byte of key stream from S array at the index
S[i] +S[j] % 256
End

Fig.8: pseudo-random generation algorithm

C. Watermarking Scheme

After compressing and encrypting an image the watermarking process is applied on it. In this paper, we are using the Spread Spectrum Watermarking Scheme and Scalar Costa Scheme Quantization Index Modulation (SCS-QIM). [1], [4], [7].

a) Spread Spectrum (SS)

The watermark signal is generated by using watermark information bits (b); scaling factor α and PN sequence (P). [1]. the watermark information bits $b_i = \{b_i\}$. The watermark signal $W = \{W_i\} = \{-1, 1\}$

$$W_i = \alpha * b_i * P_i \qquad (1)$$

Where Pi= {-1, 1}

And Watermarked Signal (C_W) is given by

$$C_w = C + W \qquad (2)$$

Where i = 0, 1… L – 1.

The received encrypted-watermarked (C_W) signal is applied to the detector. It is multiplied by PN (P) sequence used for embedding, followed by summation, yielding the correlation sum (S_i)

$$S_i = \sum Cw_i * P_i \qquad (3)$$

The first term in the above equation is zero if C and P are uncorrelated. However, this is not always the case for real compressed data. Thus, we can apply the non-blind detection technique, i.e., subtract away C from Cw to remove the correlation effect completely. Thus get a better watermark detection rate. The sign of it gives the watermark information bit:

$$\text{Sign}(S_i) = \text{Sign}(b_i) = b_i \qquad (4)$$

b) Scalar Costa Scheme Quantization Index Modulation (SCS-QIM)

For SCS-QIM watermarking, the watermark message is encoded into a sequence of watermark information bits, where W[n] ∈ {0, 1}. Each of the watermark bit is embedded into the corresponding host elements x[n]. For making the codebook secure a random sequence PN can be chosen such that PN[n] ϵ {0, 1}. The embedding rule is given by

$$q_n = Q_\Delta(x[n] - \Delta(W[n]/2 + PN)) - (x[n] - \Delta(W[n]/2 + PN)) \qquad (5)$$

Here Q_Δ denotes a scalar uniform quantization with step size Δ. This embedding scheme depends on two parameters: the quantizer step size Δ and the scale factor β. The watermark sequence is then given by

$$W = \beta * q_n \qquad (6)$$

Finally the watermarked signal is obtained as

$$C_w = C + W \qquad (7)$$

In detection method, by quantizing the received signal to the nearest data in the codebook, the watermark data is detected. For this purpose we use the equation

$$W = Q_\Delta(C_{wi}) - C_{wi} \qquad (8)$$

If W = 0, then watermark bit zero is extracted and if close to $\pm\Delta/2$, then bit one is retrieved.

DISCUSSION

A. Performance Metrics

The following section describes the different performance metrics which are used for analysing the performance of whole system.

a) PSNR:

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible power of a signal and the power of distorting noise that affects the quality of its representation. The PSNR is utilized to evaluate image quality. PSNR is calculated by using the following mathematical Expression:

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \qquad (9)$$

Where MSE is the root mean square error and 255 is the maximum value of luminance level.

b) Correlation:

The correlation factor measures the similarity between the original watermark and the watermark extracted from the attacked watermarked image (robustness) [12].

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}}$$

where $\bar{A}$ = mean2 (A), and $\bar{B}$ = mean2 (B). (10)

c) Compression Rate

The proposed method introduces JPEG2000 compression standard. The mathematical expression for compression rate is given by:

$$\text{Compression Rate} = \frac{\text{Uncompressed Size}}{\text{Compressed Size}} * 100 \qquad (11)$$

B. Security Analysis of Encryption Algorithm

The RC4 cryptosystem that we have used is a very well known technique and is believed to be secure after first few hundred bytes are discarded. Hence forth, we will assume that first few hundred bytes are discarded. Now we establish the security of the applied encryption scheme based on Shannon's theory of security [15]. We assume that M ~ U [0,255] and let P_M and P_K denote the probabilities of occurrence of random variables M and K respectively, so the amount of information contained in is given by

$$H_M = - \sum P_M \log (P_M) \qquad (12)$$

Similarly, compute for a truly random key K ϵ [0,255].

$$H_K = - \sum P_K \log (P_K) \qquad (13)$$

For perfect secret systems the amount of information H_M can be hidden completely if $H_K >= H_M$ [27], which is correct if the key is truly random, where H_M & H_K are the entropies of M and K respectively.

EXPERIMENTAL RESULTS

The proposed framework is implemented in MATLAB software. Several experiments have been conducted to test performance of the proposed strategy. In this section some selected results are reported. The experiment is carried out for a set of 5 images of size 512*512. The value of alpha is in the range of 0 to 3. JPEG2000 gives good image quality after compression. As decomposition level increases, compression rate also increases and payload capacity decreases. The experiment is carried out for DWT decomposition level 4. The performance analysis using attacks is also studied. For SS and SCS-QIM methods, Gaussian noise and circular shift attacks are used. Without any attack, the proposed method shows good experimental results such as correlation between embedded & extracted watermark is 1. In the compressed domain SS technique uses the non blind detection method while other method uses the blind detection method for estimating the watermarked data. Robustness of the proposed scheme against normal signal processing operation such as compression, noise and circular shift has been evaluated on all the watermarked image data. With circular shift attack, correlation between embedded & extracted watermark decreases. The SS and SCS-QIM methods of watermarking are robust against noise attack such as AWGN noise. In case of attack of AWGN noise, SS method gives better watermark detection results as compared to SCS-QIM method. In case of circular shifting (Circularly shifting the array elements) attack, SCS-QIM is robust. For Gaussian noise snr is taken as 10db. For circular shift we shift the array elements by position 6. By decreasing compression rate, it is possible to get good PSNR between original & final image. The following experimental graphs are used for performance analysis. The fig.9 shows the graph of compression rate verses payload capacity which indicates that as compression rate increases, payload capacity decreases. It is clear that as we move from higher to lower DWT decomposition level, the payload capacity increases, and the quality of the image is good. The increase in payload capacity is due to increase in size of dimensions of higher resolutions, generating more number of compressed bytes, which provides more space for embedding. Also, from the fig. there is an inverse relation between compression rate and PSNR between original & compressed image. If there is an increase in compression rate then there is a decrease in PSNR between original & compressed image and vice versa. It is clear from experimental results that the entropy condition for RC4 security is independent of DWT decomposition level. For any level it satisfies the condition for RC4 security i.e. truly random key which is used for encryption and decryption.

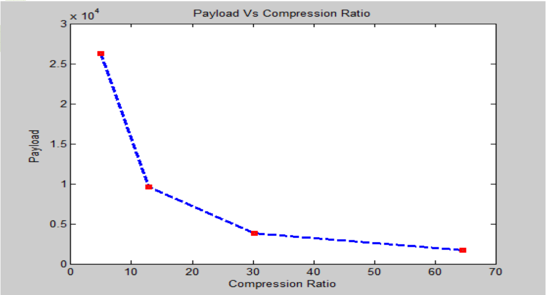


Fig. 9: Graph of payload capacity Vs Compression Rate

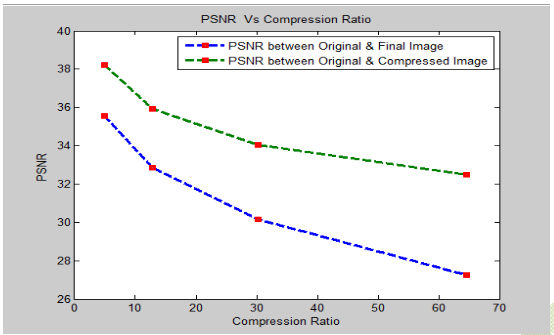
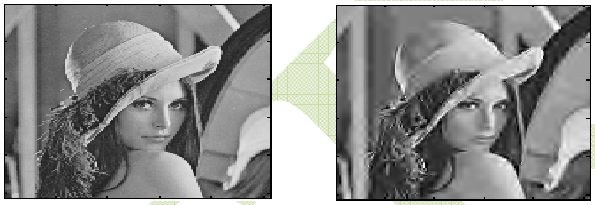


Fig.10: Graph of PSNR Vs Compression Rate

Consider the following experimental results of lena.png image.



Original Image **Final decompressed Image**

Fig. 11: Experimental Results

The following table shows performance analysis of Spread Spectrum method (With and Without Attack) and Scalar Costa Scheme Quantization Index Modulation method (With and Without Attack), Effect of DWT level of decomposition on different parameters, RC4 security analysis. The W is watermark signal, WF is extracted watermark for SCS-QIM method, S is extracted watermark signal for SS method

Image	**PSNR(M & Cw)**		**Correlation (W & S)**		**Correlation (M & Cw)**	
	Without Attack	With Attack	Without Attack	With Attack	Without Attack	With Attack
Lena.png	55.0552	55.0509	1.00	0.84570	0.999981	0.99998
Elaine.tif	55.0126	55.0117	1.00	0.84891	0.999981	0.999981
Pepper.png	54.8345	54.8342	1.00	0.84749	0.999981	0.99998
Girl.tif	54.7288	54.3598	1.00	0.8510	0.99998	0.99998
Rice.tif	54.759	54.751	1.00	0.85005	0.999981	0.999981

Table I: SS method Analysis with & without Attack (Attack: circular shift)

Image	**PSNR(M & Cw)**		**Correlation (W & S)**		**Correlation (M & Cw)**	
	Without Attack	With Attack	Without Attack	With Attack	Without Attack	With Attack
Lena.png	55.0552	55.05	1.00	0.842169	0.999981	0.99998
Elaine.tif	55.0126	55.0122	1.00	0.848915	0.999981	0.99998
Pepper.png	54.8345	54.84	1.00	0.841837	0.999981	0.999981
Boat.png	54.7288	54.7258	1.00	0.84860	0.99998	0.99998
Rice.tif	54.75	54.7488	1.00	0.840796	0.999981	0.999981

Table II: SS method Analysis with & without Attack (Attack: Gaussian Noise)

Image	**PSNR(M & Cw)**		**Correlation (W & WF)**		**Correlation (M & Cw)**	
	Without Attack	With Attack	Without Attack	With Attack	Without Attack	With Attack
Lena.png	55.0602	55.05	1.00	1.00	0.99998	0.99998
Elaine.tif	55.0134	55.0134	1.00	1.00	0.99998	0.99998
Pepper.png	54.8366	54.8364	1.00	1.00	0.99998	0.99998
Girl.tif	54.3677	54.3650	1.00	1.00	0.99998	0.99998
Rice.tif	54.7492	54.7473	1.00	1.00	0.99997	0.9999

Table III: SCS-QIM method Analysis with & without Attack (Attack: Circular Shift)

Image	**PSNR(M & Cw)**		**Correlation (W & WF)**		**Correlation (M & Cw)**	
	Without Attack	With Attack	Without Attack	With Attack	Without Attack	With Attack
Lena.png	55.0602	54.613	1.00	0.677935	0.999981	0.99998
Elaine.tif	55.0134	54.4865	1.00	0.729532	0.999982	0.99998
Pepper.png	54.8366	54.6434	1.00	0.744463	0.99998	0.99998
Girl.tif	54.3677	54.2698	1.00	0.73573	0.999983	0.999983
Rice.tif	54.7492	54.70	1.00	0.720906	0.999979	0.999979

Table IV: SCS-QIM method Analysis with & without Attack (Attack: Gaussian Noise)

DWT Decomposition Level	PSNR(I & reconstructed I)	Compression Ratio	Payload	PSNR(Original & Compressed Image)
1	35.5558	4.87383	26240	38.2017
2	32.8762	12.8477	9593	35.9429
3	30.143	30.2009	3848	34.0492
4	27.2346	64.5993	1669	32.4763

Table V: Effect of DWT Decomposition level on different parameters

DWT Decomposition Level	Entropy (M)	Entropy (K)
1	7.7175	7.9922
2	7.7242	7.9922
3	7.7132	7.9922
4	7.5690	7.9922

Table VI: RC4 security Analysis

CONCLUSION

The projected technique introduces a robust watermarking scheme. The algorithm is simple to implement as it is directly performed in the compressed-encrypted domain, i.e., it does not require decrypting or partial decompression of the content. Our scheme also preserves the confidentiality of content as the embedding is done on encrypted data. The detection is carried out in compressed domain. We analyze the relation between payload capacity and quality of the image (in terms of PSNR). In our paper mainly three goals are achieved such as compression which is used for reducing the storage space requirement, Encryption for Robust image security and watermarking of compressed and encrypted images for copyright protection control or ownership declaration. Here two watermarking techniques used are SS and SCS-QIM. SS uses non-blind detection technique while SCS-QIM uses blind detection technique for estimating the watermarked data. The proposed system works robustly in both with attack and without attack operations. In our paper, we encrypt JPEG2000 compressed bit stream. Hence rest of the operation is performed in frequency domain and at decompression step we convert it into spatial domain. Hence the performance parameters are PSNR and correlation shows optimum values as compared to other methods. Future work aims at extending the proposed scheme to other image compression schemes such as JPEG, JPEG-LS. The major challenges with this compression schemes would be the lack of error resilience of the variable length codes used for encoding, and maintaining the compressed file size after encryption and watermarking so that the impact on compression gain is minimal.

REFERENCES

[1] A. V. Subramanyam, Sabu Emmanuel, Member, IEEE, and Mohan S. Kankanhalli, Senior Member, IEEE," *Robust Watermarking of Compressed and Encrypted JPEG2000 Images" IEEE Trans. on multimedia, vol. 14, no. 3, june 2012, pp.703 - 716*

[2] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli, "*Privacy preserving multiparty multilevel DRM architecture," in Proc. 6th IEEE Consumer Communications and Networking Conf., Workshop Digital Rights Management, 2009, pp. 1–5.*

[3] T. Thomas, S. Emmanuel, A. Subramanyam, and M. Kankanhalli, "*Joint watermarking scheme for multiparty multilevel DRM architecture," IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 758–767, Dec. 2009.*

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

[5] H. Wu and D.Ma, *"Efficient and secure encryption schemes for JPEG 2000," in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, 2004, vol. 5, pp. 869–872.*

[6] 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.*

[7] 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.*

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

[9] Deepa L , Meerakrishna G ,Vinitha ,Febeena," *Compressed Image Watermarking using Visual Cryptography", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.*

[10] F. Battisti, M. Cancellaro, G. Boato, M. Carli, and A. Neri, *"Joint watermarking and encryption of color images in the Fibonacci-Haar domain," EURASIP J. Adv. Signal Process., vol. 2009.*

[11] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. De Natale, and A. Neri, *"A joint digital watermarking and encryption method," in Proc. SPIE Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008, vol. 6819, pp. 68 191C–68 191C.*

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

[13] Z. Li, X. Zhu, Y. Lian, and Q. Sun, "*Constructing secure content dependent watermarking scheme using homomorphic encryption," in Proc. IEEE Int. Conf. Multimedia and Expo, 2007, pp. 627–630.*

[14] Q. Sun, S. Chang, M. Kurato, and M. Suto, *"A quantitive semi-fragile JPEG2000 image authentication system," in Proc. Int. Conf. Image Processing, 2002, vol. 2, pp. 921–924.*

[15] R. Rivest, A. Shamir, and L. Adleman, *"A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.*

[16] C. Shannon, "Communication theory of secrecy systems*," MD Comput., vol. 15, no. 1, pp. 57–64, 1998.*

[17] T. ElGamal, "*A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.*

[18] P. Paillier, "*Public-key cryptosystems based on composite degree residuosity classes," Lecture Notes in Computer Science, pp. 223–238, 1999.*

[19] 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.*

[20] J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "*Scalar costa scheme for information embedding," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 1003–1019, Apr. 2003.*

[21] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, "*Rational dither modulation: A high-rate data-hiding method invariant to gain attacks," IEEE Trans. Signal Process., vol. 53, no. 10, pt. 2, pp. 3960–3975, Oct. 200*