International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 3, Issue 4, July-August 2014 **ISSN 2278-6856**

A commutative Encryption and Watermarking (CEW) scheme for JPEG2000 compression standard

A. M. Riad[1], Reham R. Mostafa[2] and Rasha elhadry[3]

[1]Mansoura University, Faculty of computer and information science,Egypt

[2,3]Mansoura University, Faculty of computer and information science, Egypt

Abstract

Commutative Encryption and Watermarking (CEW) combines encryption and watermarking to provide a comprehensive security protection for multimedia data. On the other hand, the storage and transmission is an important dilemma due to enormous size of multimedia data, therefore an effective solution to both bandwidth and storage problem is the use of data compression. In this paper, we propose a commutative watermarking and encryption (CEW) scheme for jpeg2000 compression standard.The commutative property of the proposed scheme allow to encrypt a watermarked image without interfering with the embedded watermark, or to watermark encrypted image and still allowing a perfect decrypting. The encryption and watermarking are carried out after the quantization step in jpeg2000 compression standard. It is based on decomposed data after quantization into two parts. One part is encrypted and the other is watermarked. The security of the scheme is assured since the encryption and watermarking is implemented in compressed domain. Experimental Results show the effectiveness of the proposed scheme.

Keywords: JPEG2000, Encryption, Watermarking, Commutative Encryption and watermarking scheme (CEW)

1. INTRODUCTION

The rapid growth in the multimedia and communication technologies, recently, resulted in the transmission of large amount of multimedia data over internet. Internet can be considered as insecure channel which ease the illegal distributing of multimedia data and tampering of visual data that is sensitive in nature. For this reason, multimedia data require confidentiality and integrity. As stated in ITU-T,Rec.X.800[1] and IETF RFC 2828 [2], the data security is achieved by ensuring the following services: authentication, to verify the identity claimed by or for any system entity; data confidentiality, to protect data against unauthorized disclosure; data integrity, to verify that data have not been changed, destroyed, or lost in an authorized or accidental manner. Watermarking and cryptography are used to satisfy these constraints. Media encryption prevents media content from leakage by encoding multimedia data into unintelligible form, which protect media data's confidentiality during the process of transmission, storage, etc. The limitation of multimedia encryption is that once the multimedia data is decrypted, there is no way for content owner to prevent illegal replication, reproduction, or delivery of multimedia content. Media watermarking is the technique that embeds some information into multimedia content perceptually or imperceptibly, that protects media data's identification or ownership. In the invisible watermarking, imperceptibility and robustness are required. The imperceptibility means that the watermarked media is perceptually similar to the original media, and robustness means that the embedded watermark survives such operation as recompression, adding noise, filtering, scaling, etc. Because multimedia encryption and watermarking realize different functionalities, the can be combined together to protect both confidentiality and the ownership. Based on whathas been accomplishedin scientific researchforthe integrationbetween Encryption and watermarking, there are main two categories of joint watermarking and encryption method:

- Joint decryption/watermarking, where watermark embedding is conducted during the decryption process [3–5]. These methods called Joint Fingerprint and decryption (JFD) method.
- Joint encryption/watermarking: where watermarking and encryption step processes are merged. In this case, the watermark can be extracted: (a) in the spatial domain, i.e. after the decryption process, or; (b) in the encrypted domain, or; (c) in both domains [6]. These approaches called Commutative watermarking and encryption (CEW) techniques

Commutative Encryption and Watermarking (CEW) [7] is the most significant subject in this field. In some application, if encryption and watermark are commutative, some computational cost will be saved. The commutative property allows to encrypt a watermarked image without interfering with the embedded signal or to watermark an encrypted image and still allowing a perfect decrypting.

The system that combine watermarking and encryption is defined as CEW system as shown in figure 1, if the following condition is satisfied:

$$S = W(E(X, K_E), w, K_w) = E(W(X, w, K_w), K_E) \quad (1)$$

Thus, the watermark can be detected according to

$$w = V(D(S, K_D), K_w) = V(W(X, w, K_w), K_w) \quad (2)$$

where X is the original image, S is the watermarked-encrypted image, $E(\ )$ is the encryption function, $D(\ )$ is the decryption key, $W(\ )$ is the watermarking embedding function, $V(\ )$ is the watermarking extraction function, K_E is the encryption key, K_D is the decryption key, K_W is watermarking key, and w is the watermark. In [7, Sec.2.2], four properties are formulated to describe watermarking in the encrypted domain:

- Property 1. The watermarking function W can be performed on an encrypted image.
- Property 2. The extraction function V is able to reconstruct a watermark in the encrypted domain when it has been embedded in the encrypted domain.
- Property 3. The extraction function V is able to reconstruct a mark in the encrypted domain when it has been embedded in the clear domain.
- Property 4. The decryption function does not affect the integrity of the watermark.

In spite of the difficulties to realize effective algorithms that combine partial encryption and watermarking, some solutions have been proposed. In [8, 9] Lian et al. proposed two schemes of CEW based on partial encryption. In these schemes, multimedia data was partitioned into two parts, one part of the media data was encrypted and the other part was watermarked. Because encryption part is independent on the watermarked part, the encryption algorithm's property and watermarking algorithm's property are both kept unchanged. On the other hand, multimedia data requires considerable storage capacity and transmission bandwidth. Image coding refers to the coding of digital images to create a new representation to serve certain application requirements. Commonly, image coding is used for compression which produces a representation code that is shorter (in bits) than the original image. The discrete cosine transform (DCT) has been the most common transform utilized in transform based image coding schemes. The DCT is used in the JPEG standard [10]. However, more recently, the discrete wavelet transform (DWT) has gained interest, as it has been shown to offer greater decorrelation and energy compaction when applied to image. Wavelet-based image coding systems showing greater performance compared to DCT-based systems. The DWT is utilized in the newer JPEG2000 standard [11]. Wavelet-Based Image Coding, as shown in figure 2, use transforms to provide decorrelation and energy compaction in the spatial domain, before quantization is applied. This reduces spatial redundancy as well as providing a representation that closely relates to HVS models. After quantization, the transform coefficients will be coded using approaches such as run length encoding and/or entropy coding, to produce the final binary output.

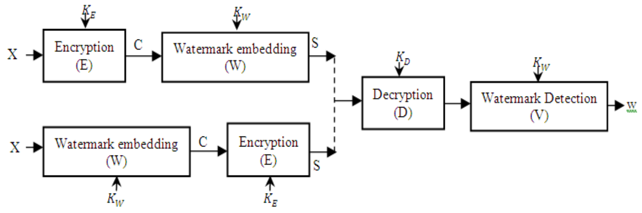
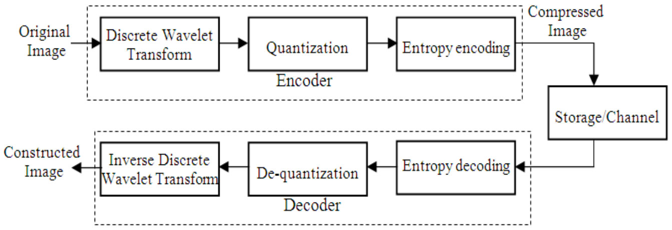


Figure 1 Architecture of commutative watermarking and encryption



A variety of powerful and sophisticated wavelet based image coders have been developed. For example, the embedded zerotree wavelet (EZW) coding proposed by Shapiro in [12] is a very effective and computationally simple technique for image compression. It is not only effectively removes the spatial redundancy across multiresolution scales but also provides fine scalability. Said and Pearlman in [13] present a set partitioning in hierarchical tree (SPIHT) coding that is one of the simplest and most efficient improvement of the EZW coding. The performance of SPIHT algorithm is not only better than EZW but its coding procedures are also extremely fast. Because the SPIHT has the high quality reconstruction and low bit rate property, it is very suitable for the secret image compression. Recently, a novel still image compression standard jpeg2000 was announced and widely used. It is based on a scheme originally proposed by Taubman and known as EBCOT ("Embedded Block Coding with Optimized Truncation" [14]). The major difference between previously proposed wavelet-based image compression algorithms such as EZW or SPIHT is that, after performing a global wavelet transform, EBCOT as well as JPEG2000 operate on independent, non-overlapping blocks of transform coefficients which are coded in several bit layers to create an embedded, scalable bitstream. In this paper, a commutative encryption and watermark (CEW) scheme that is based on jpeg2000 compression standard was proposed. In this scheme, the encryption and watermarking was carried out after the quantization step in jpeg2000 compression standard, in which the quantized coefficients are partitioned into two parts. One part, which contains the most significant information of an image, was encrypted, and the other part was watermarked. The rest of paper organized as follow: the jpeg2000 codec is described in Section 2. Then in section 3 our proposed CEW scheme is presented and the obtained results are discussed in detail in section 4. The conclusions are presented and future work is discussed in section 5.

JPEG2000 Compression Standard

JPEG2000 is the new international standard for image compression developed jointly by the Joint Photographic Experts Group committee in 2000 with the intention of superseding their original discrete cosine transform-based JPEG standard (created in 1992) with a newly designed, wavelet-based method. The goal of the JPEG2000 is to develop "a new image compression system for all kinds of still images (bi-level, grayscale, color, multi-component) with different characteristics (continuous-tone, text, cartoon, medical, etc), for different imaging models (client/server, realtime transmission, image library archival, limited buffer and bandwidth resources, etc.) and preferably within a unified system" [15]. Generally speaking, JPEG2000 is designed to supplement and enhance the existing JPEG standard for still image coding. It provides advanced features such as low bitrate compression, lossless and lossy coding, multiple resolution representation, progressive transmission, region of interest (ROI) coding, error-resilience, random codestream access and processing, and a more flexible file format.

2.1 JPEG2000 coding structure

The general codec structure of the JPEG2000 is illustrated in Figure 3.The JPEG2000 encoder is illustrated in Figure 3a. The discrete transform is first applied on the source image data. The transform coefficients are then quantized and entropy coded, before forming the output codestream (bitstream). The decoder is the reverse of the encoder (Figure 3b). To reconstruct the original image, the codestream is first entropy decoded, dequantized and inverse discrete transformed. To recapitulate, the encoding procedure is as follows [16, 17]:

- The source image is partitioned into components.
- Tiling is applied to the original image and its components by partitioning it into rectangular non-overlapping blocks (tiles). These tiles can be processed and manipulated independently.
- The discrete wavelet transform (DWT) is applied on each tile. The tile is decomposed in different resolution levels.
- These decomposition levels are made up of subbands of coefficients that represent the horizontal and vertical spatial frequencies of the tile component.
- After DWT, all the coefficients in subbands are quantized and collected into rectangular arrays of "code-blocks".
- The bit-planes of the coefficients in a "code-block" are entropy coded.
- The encoding can be done in such a way, so that certain ROI's can be coded in a higher quality than the background.
- Markers are added in the bitstream to allow error resilience.
- The codestream has a main header at the beginning that describes the original image and the various decomposition and coding styles that are used to locate, extract, decode and reconstruct the image with the desired resolution, fidelity, region of interest and other characteristics.
- The optional file format describes the meaning of the image and its components in the context of the application.

3.The Proposed Commutative Encryption and Watermarking (CEW) Scheme

The block diagram of the proposed CEW scheme is shown in figure 4. The scheme is integrated with jpeg2000 compression standard framework. The main idea is to partition the data obtained in DWT domain after quantization into two parts. One part is encrypted and the other is watermarked.

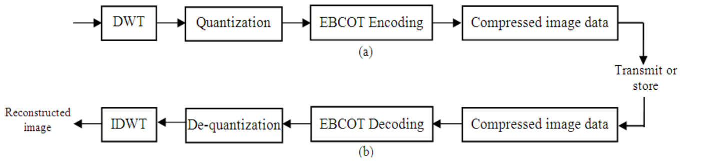


Figure 3 Codec structure. The structure of the (a) encoder, (b) decoder

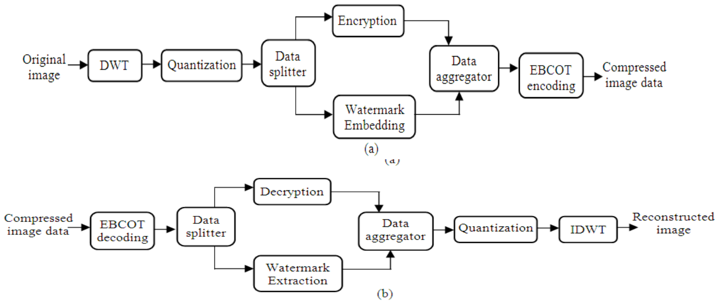


Figure 4: Proposed CEW scheme based on jpeg2000 codec, (a)encryption and watermarking embedding procedure, (b) decryption and watermarking extraction procedure

In the proposed CEW scheme, the human visual system (HVS) is used to determine which part of the quantized coefficients are suitable for encryption to achieve a high perceptual security, and which part of the quantized coefficients is suitable to embed the watermark imperceptibly. Discrete wavelet transform (DWT) is the multiresolution description of an image. It decomposes an image into four subbands as shown in figure 5. LL is the low frequency coefficients, LH is the high frequency coefficients horizontally, HL is the high frequency coefficient vertically, and HH is the high frequency coefficient diagonally.

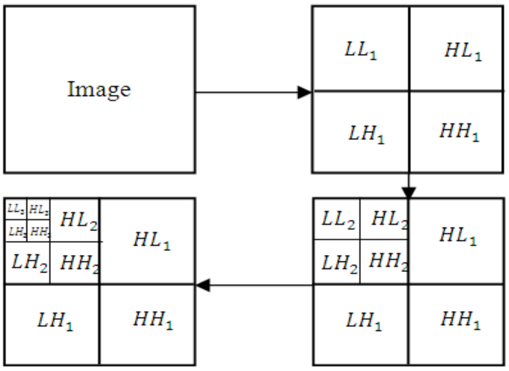


Figure 5 Flow of DWT process (3-level decomposition)

The human visual system (HVS) [18] is more sensitive to the low frequency coefficients, and less sensitive to the high frequency coefficients. From this fact, we propose the CEW scheme in which encrypts the low frequency coefficients and embeds the watermark in the high frequency coefficients. Encrypting the low frequency coefficients achieve a high perceptual security because most of the image energy is concentrated at the lower frequency coefficients. On the other hand, the high frequency coefficients include the edges and textures of the image and human eye is not sensitive to changes in these coefficients. This allows the watermark to be embedded without being perceived by the human eye.

3.1 Encryption and watermark embedding

Encryption and watermarking was carried out after the quantization step in jpeg2000 compression standard. For encryption, the proposed CEW scheme encrypts the sign bits of the wavelet coefficients in the four subbands in low frequency with RC4 stream cipher. Thus, the sign bits can be extracted from the coefficient, encrypted by RC4 stream cipher, and returned to the corresponding coefficients. In jpeg2000 codec, the sign bits are encoded independently and thus the sign encryption does not change the compression ratio. For watermarking, the algorithm proposed in [19], is adopted to embed the watermark in the proposed CEW scheme. This algorithm embeds the watermark by modifying the wavelet coefficients in pairs after quantization of the original image. The process of embedding the watermark into quantized wavelet coefficients is as follow: suppose A and B are two adjacent wavelet coefficients, A includes two parts which are integer part A_int and decimal part A_dec. The last eight bits of A_int are denoted as:

A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8

Similarly, The last eight bits B_int of are denoted as:

B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8

The method of embedding one bit watermark in (A_int, B_int) is as following:

If $w = 0$, and $A_m \neq B_m$, let

$$(A\_\text{int})' = \begin{cases} ((A\_\text{int} >> m) << m) \mid (2^{m-1}-1) & if\ \ A_m = 1 \\ ((A\_\text{int} >> m) << m) \mid (2^{m-1}) & \text{else} \end{cases} \tag{3}$$

If $w = 1$, and $A_m = B_m$, let

$$(A\_\text{int})' = \begin{cases} ((A\_\text{int} >> m) << m) \mid (2^{m-1}-1) & if\ \ A_m = 1 \\ ((A\_\text{int} >> m) << m) \mid (2^{m-1}) & \text{else} \end{cases} \tag{4}$$

Where m is chosen from the set {1, 2, …, 8}

3.2 Decryption and watermark extraction

At the decoder side, the quantized coefficients in the four subbands in the low frequency are separated from the data obtained from the EBCOT decoder. The sign bits of these encrypted coefficients are extracted and decrypted using the same key as used in encryption process. The watermark is extracted in a simple and fast way without the assistance from either the original image or reference watermark. The watermark extraction is done as follow: find two quantized adjacent wavelet coefficients A', B' in the high frequency subband, where, the integer part of A' is $(A\_\text{int})'$, and the integer part of B' is $(B\_\text{int})'$.

The method of extracting one bit watermark w' from $(A\_\text{int})'$ and $(B\_\text{int})'$ is

$$w' = \begin{cases} 1 & if\ \ A'_m = B'_m; \\ 0 & else. \end{cases} \tag{5}$$

4. Experimental Results

For a comprehensive assessment of the proposed CEW scheme, the experiments are conducted to evaluate the security of encryption and the imperceptibly and robustness of watermark.

4.1 Security of encryption

For image encryption, it is important to keep the encrypted image unintelligible. It is called perceptual security. In order to evaluate perceptual security, three measures are adopted:

- Peak signal to noise ratio (PSNR)
  The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and an encrypted image. The lower the PSNR mean that the lower the intelligibility of the encrypted image and the higher the perceptual security.The result of the proposed scheme are shown in Table 1, in which it can be seen that the corresponding PSNR are all smaller than 15 and the encrypted image are unintelligible, preserving the perceptual security of the proposed scheme.
- Information Entropy Analysis
  The information entropy ideally should be 8 bits for gray level images. If an encryption scheme generates an output encrypted image whose entropy is less than 8 bits, then there would be a possibility of predictability, which may threaten its security [20].Information entropy is calculated by the following equation.

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)}, \tag{6}$$

where represent the probability of occurrence of the symbol . Simulation results for entropy analysis are shown in Table 6. Entropy analysis shows that the proposed encryption algorithm has entropy that close to ideal entropy (8), so the algorithm is secure from leakage of information.

Table 1: Some result of encrypted images

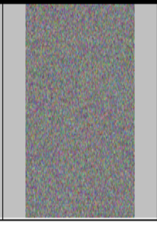
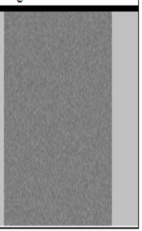
Lena encoded by jpeg2000	Encrypted Lena image PSNR = 13.33	Airplane encoded by jpeg2000	Encrypted airplane image PSNR = 12.09
			

Table 2 Image Entropy

Image	size	Entropy Value	
		Encrypted image	Original image
Airplane	256 × 256	7.9453	7.7854
House	512 × 512	7.9994	7.8225
Sailboat	512 × 512	7.9874	7.8945

4.2 Imperceptibility and robustness of the watermark

In the experiment, the cover image used is an 512×512 gray level image and the watermark logo is an 32×45 binary logo. Table 3 shows the 512×512 bit gray level cover image (Airplane, and House), the 32×45 binary watermark, the watermarked imageand the extracted watermark. The Peak signal to noise ratio (PSNR) is used to measure the quality of watermarked image. The Normalized Correlation (NC) is used to measure similarities of extracted watermarks. A higher PSNR value reflects the facts that the watermarked image is more similar to the original image. Moreover, a higher NC value reflects the fact that the extracted watermark is of higher quality. Various attacks are used to test the robustness of the watermark. Table 4 shows watermarking logo extracted from Sailboat 512×512 watermarked images, after exposing the watermarked image to different attacks. The Normalized Correlation (NC) is used to express quality of the reconstructed logo for each of the attacks.

Table 3 : shows the two standard gray level cover image with watermark logo, watermarked image, and extracted

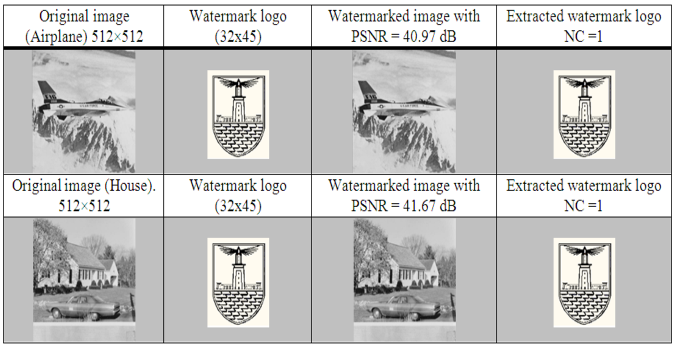
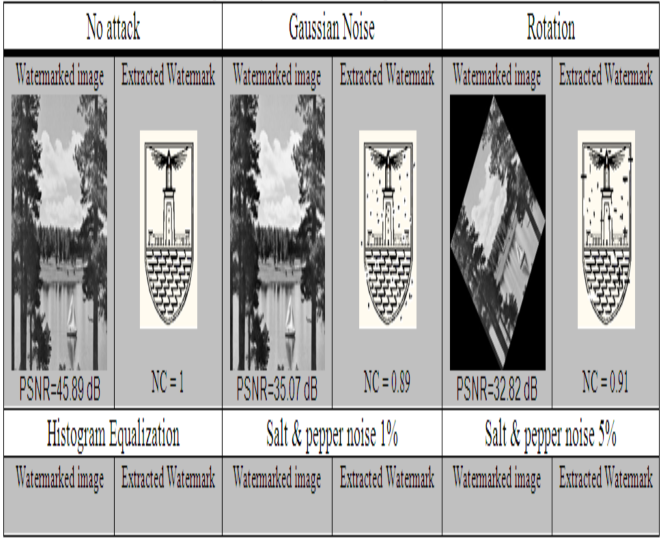
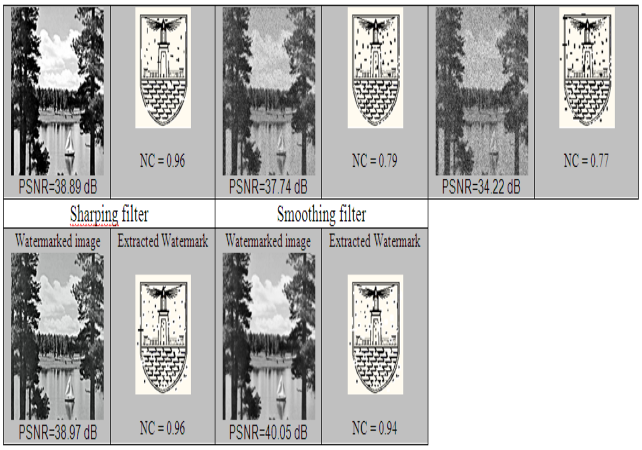

Original image (Airplane) 512×512
Watermark logo (32x45)
Watermarked image with PSNR = 40.97 dB
Extracted watermark logo NC =1
Original image (House). 512×512
Watermark logo (32x45)
Watermarked image with PSNR = 41.67 dB
Extracted watermark logo NC =1

Table 4 :Comparability of watermarked image under different attacks


No attack
Gaussian Noise
Rotation
Watermarked image
Extracted Watermark
Watermarked image
Extracted Watermark
Watermarked image
Extracted Watermark
PSNR=45.89 dB
NC = 1
PSNR=35.07 dB
NC = 0.89
PSNR=32.82 dB
NC = 0.91
Histogram Equalization
Salt & pepper noise 1%
Salt & pepper noise 5%
Watermarked image
Extracted Watermark
Watermarked image
Extracted Watermark
Watermarked image
Extracted Watermark


PSNR=38.89 dB
NC = 0.96
PSNR=37.74 dB
NC = 0.79
PSNR=34.22 dB
NC = 0.77
Sharping filter
Smoothing filter
Watermarked image
Extracted Watermark
Watermarked image
Extracted Watermark
PSNR=38.97 dB
NC = 0.96
PSNR=40.05 dB
NC = 0.94

5. Conclusions and Future Work

Commutative Encryption and watermarking provide a method to combine encryption and watermarking to protect both confidentiality and integrity of digital media.

In this paper, we propose a CEW scheme that integrated with the jpeg2000 compression standard. The main idea is to partition the data after quantization into two parts; one part is encrypted while the other is watermarked. This partition must achieve a high perceptual security of encryption, and the imperceptibility and robustness of the embedded watermark. The proposed scheme allow extract watermark in the encrypted domain, moreover, allow watermark to be embed in the encrypted content. Experimental results confirmed the robustness of the proposed scheme against most common signal processing attacks. Moreover, the proposed is secure and suitable for real time application. In future we will extend this scheme to other codecs and its performance will be evaluated.

References

[1.] ITU-T, Rec. X.800 Security architecture for Open Systems Interconnection, 1991.

[2.] R. Shirey, Internet Security Glossary, RFC 2828, GTE/BBN Technologies, May 2000.

[3.] A. Adelsbach, U. Huber, A.S. Sadeghi, “Fingercasting– joint fingerprinting and decryption of broadcast messages, Australasian Conference on Information Security and Privacy, vol. 4058 of Lecture Notes in Computer Science, pp. 136–147, 2006.

[4.] M. Celik, A.N. Lemma, S. Katzenbeisser, M. van der Veen, “Secure embedding of spread spectrum watermarks using look-up-tables,” International Conference on Acoustics, Speech and Signal Processing, IEEE Press, vol. 2, pp.153–156, 2007.

[5.] L. Shiguo, L. Zhongxuan, R. Zhen, W. Haila, “Joint fingerprint embedding and decryption for video distribution,” IEEE International Conference on Multimedia and Expo, pp. 1523–1526, 2007.

[6.] L. Shiguo, L. Zhongxuan, R. Zhen, W. Haila, “Commutative encryption and watermarking in video compression,” IEEE Transactions on Circuits and Systems for Video Technology, pp. 774–778, 2007.

[7.] J. Herrera-Joancomart, S. Katzenbeisser, D. Megias, J. Minguillon, A. Pommer, M. Steinebach, A. Uhl, “ECRYPT European Network of Excellence in Cryptology, First Summary Report on Hybrid Systems,” 2005.

[8.] S. Lian, Z. Liu, R. Zhen, and H. Wang, “Commutative watermarking and encryption for media data,” Optical Engineering, vol. 45, no. 8, pp. 080510, 2006.

[9.] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative Encryption and Watermarking in Video Compression,” IEEE Transactions On Circuits And Systems For Video Technology, vol. 17, no. 6, pp. 774 -778 , 2007.

[10.] JTC 1/SC 29, ISO/IEC 10918-1:1994 Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines, ISO/IECStd., 1994.

[11.] JTC 1/SC 29/WG 1, ISO/IEC 15444-1:2004 Information technology – JPEG 2000 image coding system: Core coding system, ISO/IEC Std., 2004.

[12.] J.M. Shapior, “Embedded image coding using zerotrees of wavelet coefficients,” IEEE Transactions on Signal Processing, pp. 3445–3462, 1993.

[13.] A. Said, W.A. Pearlman, “A new, fast, and efficient image codec based on set partitioning in hierarchical trees,” IEEE Transactions on Circuit and Systems for Video Technology, pp. 243–250, vol.6, 1996.

[14.] D.Taubman, “High performance scalable image compression with EBCOT,” IEEE Transactions on Image Processing, vol. 9, no. 7, pp.1158 – 1170, 2000.

[15.] C. Lui, “A Study of the JPEG-2000 Image Compression Standard,” 2001.

[16.] C. Christopoulos (editor), “JPEG2000 Verification Model 8.0 (technical description),” ISO/IEC JTC1/SC29/WG1 N1822, July 21, 2000.

[17.] M. Boliek, C. Christopoulos and E. Majani (editors), “JPEG2000 Part I Final Draft International Standard,” (ISO/IEC FDIS15444-1), ISO/IEC JTC1/SC29/WG1 N1855, August 18, 2000.

[18.] L. Gaudart, J. Crebassa , and J..P. Petrakian, “Wavelet transform in human visual channels,” AppliedOptics, vol.32, no.22, pp. 4119-4127, 1993.

[19.] G. H-ying, L.G-qiang, L. Xu, X. Yin, “A Robust Watermark Algorithm for JPEG2000 Images,”International Conference on Information Assurance and Security, IEEE Press, vol. 2, pp.230–233, 2009.

[20.] R. Enayatifar, “Image encryption via logistic map function and heap tree,” Int. J. Phys. Sci, vol. 6, no. 2, p. 221, 2011.