Commutative watermarking and encryption for media data

Shiguo Lian, Zhongxuan Liu, Ren Zhen, and Haila Wang
France Telecom Research & Development Beijing
Beijing, 100080, China
E-mail: shiguo.lian@francetelecom.com

Abstract. A commutative watermarking and encryption scheme is proposed for media data protection. In the scheme, the partial encryption algorithm is adopted to encrypt the significant part of media data, while some other part is watermarked. The commutative property brings conveniences to practical applications in secure media transmission or distribution.
[DOI: 10.1117/1.2333510]

Subject terms: signal processing; image processing; multimedia.

Paper 060265LR received Apr. 27, 2006; revised manuscript received Jun. 1, 2006; accepted for publication Jun. 6, 2006; published online Aug. 23, 2006.

1 Introduction

Several means have been proposed to protect media data, among which, media encryption[1] and digital watermarking[2] have been attracting more and more researchers. Media encryption encodes media data into an unintelligible form, which protects media data's confidentiality. Digital watermarking embeds identification information into media data imperceptibly, which protects media data's ownership. Because they realize different functionalities, the two means are often applied independently. To remain secure, they can be used together. For example, media data are first watermarked, and then encrypted. However, in this case, the encrypted media data should be decrypted before the watermark can be extracted or another watermark can be embedded.

It is secure to commutate watermarking and encryption,[3] although it is still difficult to find a practical solution. As a commutative watermarking and encryption process, the following condition is satisfied:

$$\begin{cases} M = \mathrm{E_m}(C, W, K_w) = \mathrm{E_m}[\mathrm{E_n}(P, K_c), W, K_w] \\ M = \mathrm{E_n}(P', K_c) = \mathrm{E_n}[\mathrm{E_m}(P, W, K_w), K_c]. \end{cases} \tag{1}$$

Here, P, C, M, P', and W denote the original media, cipher media, watermarked cipher media, watermarked media, and watermark, respectively; and $E_n[\ ]$, $E_m[\ ]$, K_c, and K_w denote the encryption function, watermark embedding function, encryption key, and decryption key, respectively. If the scheme is practical, more convenience will result for media distribution. However, until now, no solutions have been reported.

In the past decade, some partial encryption algorithms have been reported that encrypt only some significant parts of the media data, such as the significant frequency bands, bit planes, and/or coding passes in JPEG2000 images,[4,5] the motion vectors or discrete cosine transform (DCT) coefficients in MPEG2 streams,[6,7] and the intraprediction modes and/or DCT coefficients in advanced video coding.[8,9] Similarly, media watermarking often embeds watermark information into parts of media data, such as the dc or ac's in DCT blocks,[10,11] and the wavelet coefficients in middle frequency bands.[12,13] Considering that these operations are often applied to media data partially, it is possible to combine watermarking and encryption together. In the following, we present a commutative watermarking and encryption scheme that encrypts and marks media data partially or selectively.

2 Proposed Commutative Scheme

The proposed scheme is shown in Fig. 1. Here, P, C, M, P', W, K_c, and K_w denote the original media, cipher media, watermarked cipher media, watermarked media, watermark, encryption key and decryption key, respectively; and $E_n()$, $D_e()$, $E_m()$, and $E_x()$ denote the encryption function, decryption function, watermark embedding function, and watermark extraction function, respectively. The original media P is partitioned into two parts: the significant part X and the other part Y. Among them, X will be encrypted, and Y will be watermarked. Thus, $P=X||Y$, $C=Z||Y$, $M=Z||Y'$, and $P'=X||Y$. The proposed commutative scheme is defined as follows.

1. The partial encryption/decryption process is

$$\begin{cases} C = \mathrm{E_n}(P, K_c) = \mathrm{E_n}(X||Y, K_c) = Z||Y \\ P = \mathrm{D_e}(C, K_c) = \mathrm{D_e}(Z||Y, K_c) = X||Y. \end{cases} \tag{2}$$

2. The selective watermark embedding/extraction process is

$$\begin{cases} P' = \mathrm{E_m}(P, W, K_w) = \mathrm{E_m}(X||Y, W, K_w) = X||Y' \\ W = \mathrm{E_x}(P', K_w) = \mathrm{E_x}(X||Y', K_w). \end{cases} \tag{3}$$

3. The commutative encryption and watermarking process is

$$\begin{cases} M = \mathrm{E_m}[\mathrm{E_n}(X||Y, K_c), W, K_w] = \mathrm{E_m}(Z||Y, W, K_w) = Z||Y' \\ M = \mathrm{E_n}[\mathrm{E_m}(X||Y, W, K_w), K_c] = \mathrm{E_n}(X||Y', K_c) = Z||Y'. \end{cases} \tag{4}$$

4. The watermark extraction process is

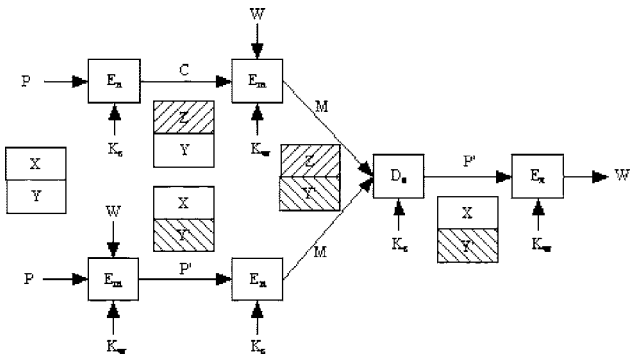

Fig. 1 Commutative encryption and watermarking based on partial encryption.

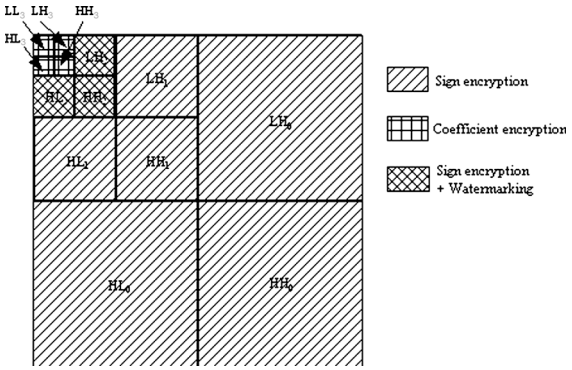

Fig. 2 Commutative encryption and watermarking based on wavelet codec.

$$W = \mathrm{E_x}(P', K_w) = \mathrm{E_x}[\mathrm{D_e}(M, K_c), K_w]$$
$$= \mathrm{E_x}[\mathrm{D_e}(Z \| Y', K_c), K_w] = \mathrm{E_x}(X \| Y', K_w). \quad (5)$$

3 Practical Scheme Based on Wavelet Codec

Based on wavelet transformation, we propose the commutative scheme shown in Fig. 2. Here, the $M \times N$ image is transformed by a four-level wavelet.

1. The subbands in the lowest level (LL_3, LH_3, HL_3, and HH_3), composed of $(M/8) \times (N/8)$ coefficients, are encrypted completely. The algorithms proposed in Refs. 4 and 5 can be used.
2. The subbands in the high level (LH_1, HL_1, HH_1, LH_0, HL_0, and HH_0), composed of $3 \times [(M/4) \times (N/4) + (M/2) \times (N/2)]$ coefficients, are encrypted with sign encryption, which keeps the coefficient amplitudes unchanged.
3. The subbands in the middle level (LH_2, HL_2, and HH_2), composed of $3 \times (M/8) \times (N/8)$ coefficients, are both encrypted and watermarked. The encryption algorithm is sign encryption, and the watermarking algorithm can be spread spectrum method,[14] the quantization index modulation (QIM) method,[15] the methods proposed in Refs. 12 and 13, etc.

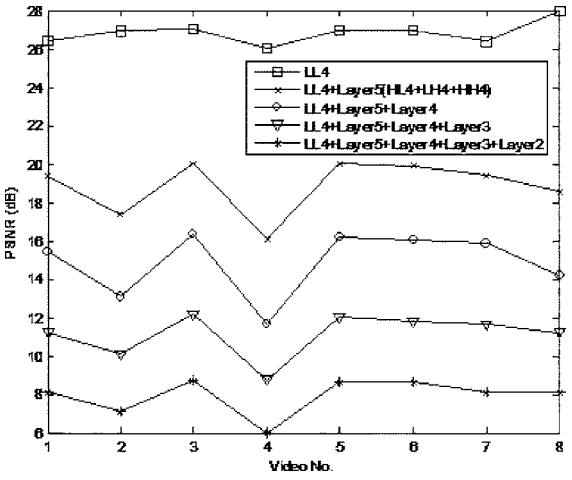

Fig. 3 Relation between the encrypted image's quality and the encrypted frequency band (5, level 9/7 wavelet; 1, "Lena;" 2, "Plane;" 3, "Crowd;" 4, "Baboon;" 5, "Bridge;" 6, "Couple;" 7, "Lake;" and 8, "Camera").

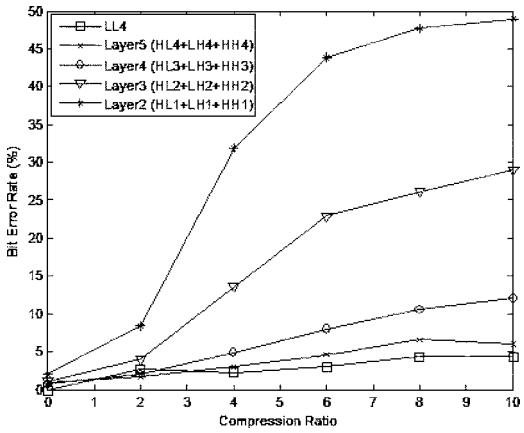

Fig. 4 Relation between the bit error rate and the watermarked frequency band.

In our scheme, the selection of the wavelet coefficients in middle frequency depends on the requirements of security and robustness. Without considering sign encryption, the more the coefficients in the low-frequency band are encrypted, the more confused is the encrypted image. Figure 3 shows the relation between the encrypted frequency band and the quality of the encrypted image. The coefficients are encrypted with the Advanced Encryption Standard (AES) as proposed in Ref. 4. Similarly, the more watermarked coefficients are in the low-frequency bands, the more robust the watermark is to signal processing operations (compression, noise, filtering, etc.). Figure 4 gives the relation between the watermarked frequency band and the robustness to JPEG2000 compression. The QIM method[15]

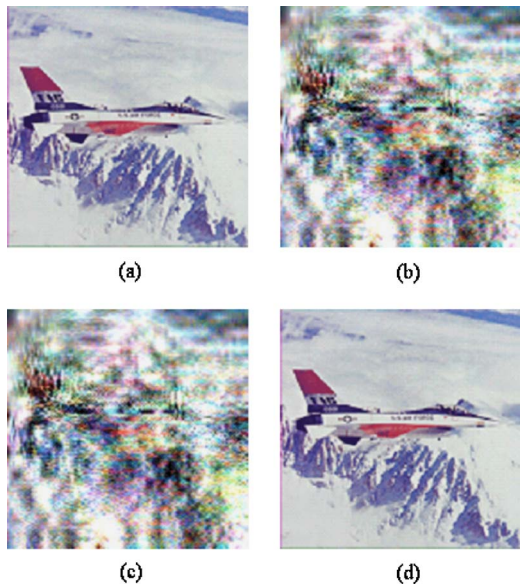

Fig. 5 Experimental results of commutative encryption and watermarking based on JPEG2000: (a) original image, (b) encrypted image, (c) watermarked image, and (d) decrypted image.

is used as the watermark algorithm. To obtain a trade-off between the security and robustness, the coefficients in the highest level frequency bands (LL_4, HL_4, LH_4, and HH_4) should be encrypted, and the coefficients in the second highest level frequency bands (HL_3, LH_3, and HH_3) can be watermarked.

This method can be combined with JPEG2000; that is, the image can be compressed and encrypted/watermarked simultaneously. The watermark is embedded immediately after quantization, coefficient encryption, and sign encryption can be applied following the entropy encoding process. As an example, "Airplane" (colorful, 256×256) is encrypted partially, then watermarked with QIM, finally decrypted and extracted. The results in Fig. 5 show that the scheme is commutative.

4 Conclusions and Future Work

We proposed a commutative encryption and watermarking scheme that is based on partial encryption. Based on the scheme, a commutative image encryption and watermarking algorithm in wavelet codec was presented, and the trade-off between security and robustness was analyzed. The encryption/watermarking algorithm can be combined with JPEG2000 codec, which is time-efficient compared with the compression process. In future work, the commutative scheme's security and robustness and its extension to other codecs will be further studied.

Acknowledgments

The authors want to thank editors for their great help and reviewers for their valuable advice.

References

1. W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video" *IEEE Trans. Multimedia* **5**(1), 118–129, (2003).
2. P. Moulin and R. Koetter, "Data-hiding codes," *IEEE Proc.* **93**(12), 2083–2127 (2005).
3. First summary report on hybrid systems, TR: IST-2002-507932 ECRYPT European Network of Excellence in Cryptology, 2005 (http://www.ecrypt.eu.org/documents/D.WVL.5-1.0.pdf).
4. S. Lian, J. Sun, D. Zhang, and Z. Wang, "A selective image encryption scheme based on JPEG2000 Codec," in *Proc. 2004 Pacific-Rim Conf. on Multimedia*, in Springer Lecture notes in Computer Science, Vol. **3332**, pp. 65–72 (2004).
5. A. Pommer and A. Uhl, "Selective encryption of wavelet-packet encoded image data: efficiency and security," *ACM Multimed. Syst.* **9**(3), 279–287 (2003).
6. L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," in *Proc. 4th ACM Int. Multimedia Conf. (ACM Multimedia'96)*, pp. 219–230, Boston, MA (1996).
7. C. Shi and B. Bhargava, "A fast MPEG video encryption algorithm," in *Proc. 6th ACM Int. Multimedia Conf.*, pp. 81–88, Bristol, UK (1998).
8. J. Ahn, H. Shim, B. Jeon, and I. Choi, "Digital video scrambling method using intra prediction mode," in *Proc. 2004 Pacific-Rim Conf. on Multimedia*, in Springer Lecture Notes on Computer Science Vol. **3333**, pp. 386–393 (2004).
9. S. Lian, Z. Liu, Z. Ren, and Z. Wang, "Selective video encryption based on advanced video coding," in *Proc. 2005 Pacific-Rim Conf. on Multimedia*, Part II, in Springer Lecture Notes on Computer Science, Vol. **3768**, pp. 281–290 (2005).
10. J. Huang, Y. Q. Shi, and Y. Shi, "Embedding image watermarks in DC components, "*IEEE Trans. Circuits Syst. Video Technol.* **10**(6), 974–979 (2000).
11. J. Hernández, M. Amado, and P. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Trans. Image Process.* **9**(1), 55–68 (2000).
12. K. Maeno, Q. Sun, S.-F. Chang, and M. Suto, "New semi-fragile image authentication watermarking techniques using random bias and non-uniform quantization," in *Security and Watermarking of Multimedia Contents IV*, Edward J. Delp III and Ping W. Wong, Eds., *Proc. SPIE* **4657**, 659–670 (2002).
13. R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," in *Proc. IEEE Int. Conf. on Image Processing*, Chicago (1998).
14. I. Cox, T. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.* **6**(12), 1673–1687 (1997).
15. B. Chen and G. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inf. Theory* **47**(4), 1423–1443 (2001).