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. © 2006 Society of Photo-Optical Instrumentation Engineers.
[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 encryption1 and digital watermarking2 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 commute 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:

\[
\begin{align*}
M = E_m(C, W, K_w) &= E_m(E_m(P, K_c), W, K_w) \\
M = E_n(P', K_c) &= E_n(E_n(P, W, K_w), K_c).
\end{align*}
\]

(1)

Here, \(P, C, M, P', W, K_c,\) and \(K_w\) denote the original media, cipher media, watermarked media, 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 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 \(E_m[·], D_m[·], E_n[·],\) and \(D_n[·]\) 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

\[
\begin{align*}
C &= E_m(P, K_c) = E_m(X\|Y, K_c) = Z\|Y \\
P &= D_m(C, K_c) = D_m(Z\|Y, K_c) = X\|Y.
\end{align*}
\]

(2)

2. The selective watermark embedding/extraction process is

\[
\begin{align*}
P' &= E_m(P, W, K_w) = E_m(X\|Y, W, K_w) = X\|Y' \\
W &= E_m(P', K_w) = E_m(X\|Y', K_w).
\end{align*}
\]

(3)

3. The commutative encryption and watermarking process is

\[
\begin{align*}
M &= E_m[E_m(X\|Y, K_c), W, K_w] = E_m(Z\|Y, W, K_w) = Z\|Y' \\
M &= E_m[E_m(X\|Y, W, K_w), K_c] = E_m(X\|Y', K_c) = Z\|Y'.
\end{align*}
\]

(4)

4. The watermark extraction process is

Fig. 1 Commutative encryption and watermarking based on partial encryption.
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, the quantization index modulation (QIM) method, the methods proposed in Refs. 12 and 13, etc.

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.

$$W = E_x(P', K_w) = E_x[D_c(M, K_c), K_w]$$
$$= E_x[D_c(Z[Y', K_c], K_w)] = E_x(X[Y', K_w]).$$

$$W = E_x(P', K_w) = E_x[D_c(M, K_c), K_w]$$
$$= E_x[D_c(Z[Y', K_c], K_w)] = E_x(X[Y', K_w]).$$

$$W = E_x(P', K_w) = E_x[D_c(M, K_c), K_w]$$
$$= E_x[D_c(Z[Y', K_c], K_w)] = E_x(X[Y', K_w]).$$

$$W = E_x(P', K_w) = E_x[D_c(M, K_c), K_w]$$
$$= E_x[D_c(Z[Y', K_c], K_w)] = E_x(X[Y', K_w]).$$
is used as the watermark algorithm. To obtain a trade-off between the security and robustness, the coefficients in the highest level frequency bands (LL₄, HL₄, LH₄, and HH₄) should be encrypted, and the coefficients in the second highest level frequency bands (HL₃, LH₃, and HH₃) 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