Transactions Letters

Commutative Encryption and Watermarking in Video Compression

Shiguo Lian, *Member, IEEE*, Zhongxuan Liu, *Member, IEEE*, Zhen Ren, and Haila Wang

***Abstract*—A scheme is proposed to implement commutative video encryption and watermarking during advanced video coding process. In H.264/AVC compression, the intra-prediction mode, motion vector difference and discrete cosine transform (DCT) coefficients' signs are encrypted, while DCT coefficients' amplitudes are watermarked adaptively. To avoid that the watermarking operation affects the decryption operation, a traditional watermarking algorithm is modified. The encryption and watermarking operations are commutative. Thus, the watermark can be extracted from the encrypted videos, and the encrypted videos can be re-watermarked. This scheme embeds the watermark without exposing video content's confidentiality, and provides a solution for signal processing in encrypted domain. Additionally, it increases the operation efficiency, since the encrypted video can be watermarked without decryption. These properties make the scheme a good choice for secure media transmission or distribution.**

***Index Terms*—DRM, partial encryption, video encryption, video watermarking.**

I. Introduction

WITH the rapid development of Internet technology, such media data as images, audios or videos are used more and more widely in human's daily life. This makes media data not only easy to be transmitted, but also easy to be copied and spread out. Thus, the legal issue rises that some media data should be protected against unauthorized users or operations. To protect media data, two means have been proposed and highlighted since the past decade, i.e., media encryption and media watermarking.

Media encryption [1]–[3] encrypts media data into unintelligible ones with ciphers, which protects media content's confidentiality. Taking video encryption [3], [4] for example, the encrypted videos are often difficult to be understood. Different from text/binary data encryption [7], video encryption often requires the scheme be time efficient and format complaint [5], [6] in order to meet real time applications. It is not practical to encrypt video data completely with traditional ciphers [7], such as data encryption standard (DES) or advanced encryption standard (AES), because of high computational cost. Alternatively, partial encryption encrypts only a fraction of video data and improves the efficiency. For example, some schemes have been proposed to encrypt the videos encoded with advanced video coding (H.264/AVC) [8]. The scheme proposed in [9] encrypts videos by scrambling the intra-prediction mode (IPM) of intra-macroblocks. Its security is analyzed in [10] followed with an improved scheme that encrypts not only IPM but also the motion vector difference (MVD). Another scheme [11] encrypts some parameters of video stream including picture parameter, intra-coded frame, slice header and macroblock header of P-slice, and dc's.

Compared with media encryption, media watermarking [12]–[16] embeds some information into media data perceptibly or imperceptibly, which protects media data's ownership or identification. For invisible video watermarking [15], [16], imperceptibility and robustness are often required. The imperceptibility means that the watermarked video is perceptually same to the original video, and the robustness means that the watermark survives such operations as recompression or signal processing. Taking the algorithms robust against H.264/AVC compression for example, they can be classified into three types: raw video watermarking, compression domain watermarking and compressed data watermarking. The first type of algorithm embeds watermarks into videos before video compression. For example, the dc's in each 8 ×8 discrete cosine transform (DCT) block are transformed with 1-D DCT and then watermarked [17]. The second type of algorithm embeds watermarks into DCT coefficients during H.264/AVC encoding [18]–[20]. For example, the algorithm proposed in [20] embeds a watermark by modifying the quantized ac's in 4 × 4 DCT blocks. The third type of algorithm embeds watermarks into the compressed data stream. For example, the watermark is embedded into the skipped macroblocks [21]. Generally, the first type of algorithm is robust against recompression or signal processing operations, but has high computational cost. The second one is time efficient, can be combined with compression process, but is only robust against recompression or few signal processing operations. The third one is time efficient, but not robust against recompression or signal processing operations.

For video encryption and video watermarking realize different functionalities, they can be combined together to protect both the confidentiality and the ownership/identification. Generally, it is implemented according to two steps [22], [23]. Firstly, media data are watermarked. Secondly, the watermarked media data are encrypted. In this case, if the encryption process

Manuscript received August 3, 2006; revised December 14, 2006. This work was supported in part by France Telecom R&D Beijing, Beijing, China, under Grant PEK06-ILAB-008. This paper was recommended by Associate Editor Q. Sun.

The authors are with France Telecom R&D Beijing, Beijing 100080, China (e-mail: shiguo.lian@orange-ftgroup.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSVT.2007.896635

and watermarking process cannot be commutated, media data must be decrypted before the watermark can be detected or another watermark can be embedded. In some applications, if they are commutative, some computing cost will be saved. For example, the watermark can be directly extracted from the encrypted media data, or the encrypted media data can be directly watermarked. Additionally, the direct operation in encrypted domain can be supported, which is suitable for some secure applications. For example, the watermark is embedded into the encrypted media data directly without knowing the decryption key, which avoids the leakage of media content. Till now, no solutions to this problem have been reported.

In this letter, we propose a video encryption and watermarking scheme based on H.264/AVC codec, which gives a solution to the commutation of encryption and watermarking. In this scheme, such parameters as IPM, MVD and residue coefficient's sign are encrypted, while the amplitude of dc or ac is watermarked. To reduce computational cost, the selected parameters are encrypted partially. To keep sign encryption and amplitude watermarking independent, traditional watermark embedding method is modified. To keep robust and imperceptible, the coefficients are selected adaptively according to macroblock type. The rest of the letter is arranged as follows. In Section II, the commutative watermarking and encryption scheme is presented. Its performances, including the security, imperceptibility, robustness and commutative property, are analyzed in Section III. In Section IV, conclusions are drawn and future work is presented.

II. Proposed Watermarking and Encryption Scheme

In the proposed scheme, media data X is encrypted and watermarked partially. Set X be composed of two independent parameters, i.e., Y and Z. Among them, Y is encrypted, and Z is watermarked. The process is defined as

$$\begin{cases} Y' = \mathrm{E}(Y, K_e) \\ Z' = \mathrm{W}(Z, B, K_w) \end{cases}. \tag{1}$$

Here, Y', K_e, E(), Z', B, K_w, $W()$ are the encrypted copy of Y, encryption key, encryption algorithm, watermarked copy of Z, watermark, watermark key and watermark algorithm, respectively. The produced media data X' is composed of Y' and Z'. The watermark can be extracted from Z' without decrypting Y', and another watermark can be embedded into Z' without decrypting Y'. Thus, if Y is independent from Z, the scheme is commutative.

Based on the architecture, we propose the scheme combined with H.264/AVC codec, which encrypts and marks suitable H.264/AVC parameters independently. The scheme, shown in Fig. 1, is composed of several components: the compression component, encryption component and watermarking component. Here, the compression component includes intra-prediction, inter-prediction, variable length coding (VLC), etc., the encryption component includes IPM encryption, MVD encryption and residue encryption, and the watermarking component refers to residue watermarking. The encryption process and watermarking process are controlled by independent keys.

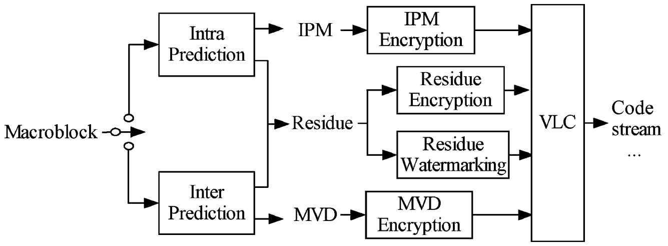


Fig. 1. Proposed watermarking and encryption scheme based on H.264/AVC.

TABLE I
Comparison of Coefficient Re-Watermarking (Original Coefficient Sequence: 2, 1, 0, -1, -2)

Iterated watermark bit	Traditional method	Traditional method with the first change	The proposed method
Original	2 1 0 -1 -2	2 1 0 -1 -2	2 1 0 -1 -2
'0'	2 2 0 -2 -2	2 0 0 0 -2	2 0 0 -2 -2
'1'	3 3 1 -3 -3	3 1 1 1 -3	3 1 1 -3 -3
'0'	4 4 2 -4 -4	2 0 0 0 -2	2 0 0 -2 -2
'1'	5 5 3 -5 -5	3 1 1 1 -3	3 1 1 -3 -3

A. Proposed Encryption Process

In [11], it is recommended to encrypt both motion information (MVD) and texture information (IPM and residue data), since encrypting only IPM is not secure enough [9], [10]. In the proposed scheme, to decrease the time cost, MVD, IPM, and residue data are all encrypted partially with a cipher [7].

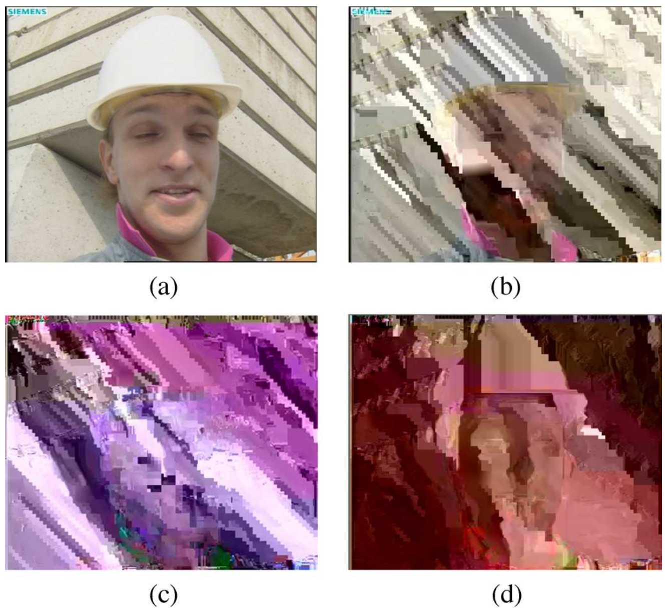
MVD Encryption: For each macroblock, the signs ("0"—positive, "1"—nonpositive) of MVD $[x, y]$ are encrypted with a cipher. That is, MVD is encrypted from $[x, y]$ to $[x', y']$ with the following condition being satisfied:

$$\begin{cases} |x'| = |x| \\ |y'| = |y| \end{cases} \tag{2}$$

where "$|x|$" denotes the absolute value of x. The encrypted MVD is then encoded with Exp-Golomb code [8]. The change of the sign of x or y does not affect the length of the codeword. For example, the codewords corresponding to "1" and "-1" are "010" and "011", respectively, which have the same length.

IPM Encryption: IPM is encoded with Exp-Golomb code [8]. In Exp-Golomb code, each $2M + 1$-length codeword is composed of M zeros, "1" and M bits of information. To keep format compliant, the proposed scheme encrypts only M bits of information with a cipher while leaving $M + 1$ bits (M zeros and "1") unencrypted. Taking the 7-length codeword "0001011" for example, only the last 3 bits "011" are encrypted while the first 4 bits "0001" (3 zeros and "1") are left unchanged.

Residue Encryption: For each non-zero residue macroblock, DCT coefficients are encrypted partially. That is, only the first 8 coefficients' signs in each 4 × 4 DCT block are encrypted with a cipher. Taking 16 × 16 luma intra-macroblock for example, there are totally 17 DCT blocks, and thus, totally 8 × 17 bits are encrypted.



(a) (b)

(c) (d)

Fig. 2. Videos are encrypted with different methods. (a) Original. (b) Encrypted with the method [9]. (c) Encrypted with the method [11]. (d) Encrypted with the proposed method.

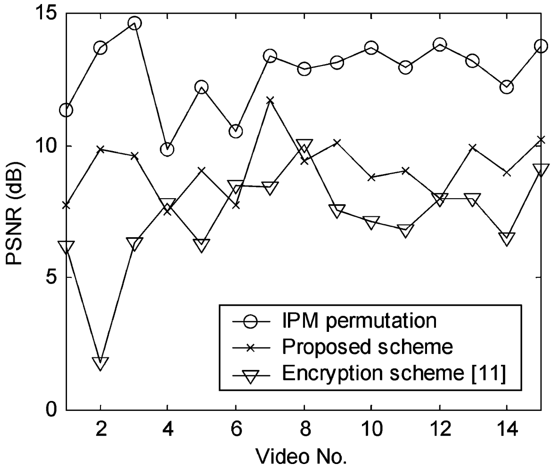


Fig. 3. Different encryption methods' perceptual security is compared. Here, the peak signal-to-noise ratio (PSNR) of the encrypted video is tested. The tested videos include 1—tempete/CIF, 2—football/CIF, 3—akiyo/CIF, 4—mobile/CIF, 5—foreman/QCIF, 6—mobile/QCIF, 7—mother/QCIF, 8—salesman/QCIF, 9—foreman/CIF, 10—news/QCIF, 11—container/QCIF, 12—silent/QCIF, 13—flower/CIF, 14—waterfall/CIF, and 15—stefan/CIF.

B. Proposed Watermarking Process

The watermark embedding process is composed of three steps: block selection, coefficient selection and watermark embedding.

Block Selection: Only the Luma blocks satisfying the following conditions are watermarked.

1) The residue block is nonzero.
2) For I/P-frame, the residue DCT block is composed of only ac's.
3) For B-frame, the residue DCT block is composed of either dc's or ac's.

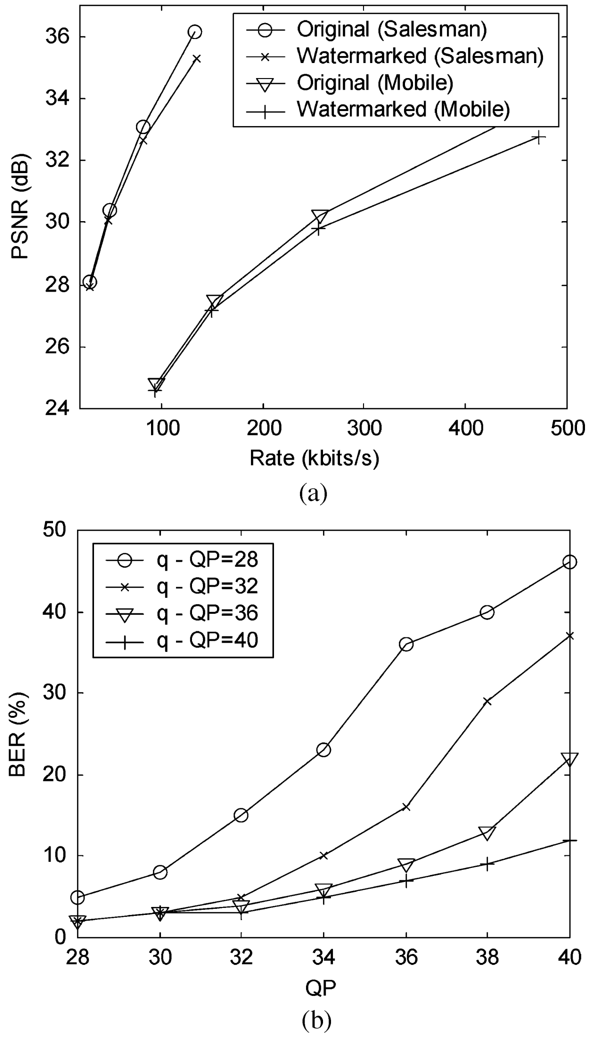


Fig. 4. obustness and imperceptibility are tested. (a) Imperceptibility of the proposed method. Here, q is the one corresponding to $\mathrm{QP} = 28$. (b) Robustness against recompression. Here, QP ranges from 28 to 40, and the test video is Salesman-QCIF/30 fps.

Coefficient Selection: The coefficients in middle frequency are preferred. Here, only M $(0 < M \leqslant 8)$ coefficients are selected randomly from the 8 ones proposed in residue encryption. The selection process is controlled by a key in order to keep secure.

Watermark Embedding: In previous art, several embedding methods have been reported [17]–[20], which can be used to watermark the selected coefficients' amplitude. The difficulty is to make watermarking and encryption commutative. As coefficients' signs are encrypted, iterated watermark embedding should not affect coefficients' signs. According to this case, traditional methods are not suitable. Here, we propose a method based on quantization embedding [20].

Set the original coefficient be z and the watermark w. To keep secure, the watermark is firstly encrypted by a stream cipher. The watermarked coefficient z' is defined as follows.

If $w = 1$

$$z' = \begin{cases} z, & \text{if } \lceil |z|/q \rceil \%2 = 1 \\ (\lceil |z|/q \rceil + 1)\, q \cdot \mathrm{Sign}(z), & \text{if } \lceil |z|/q \rceil \%2 = 0 \end{cases}. \tag{3}$$

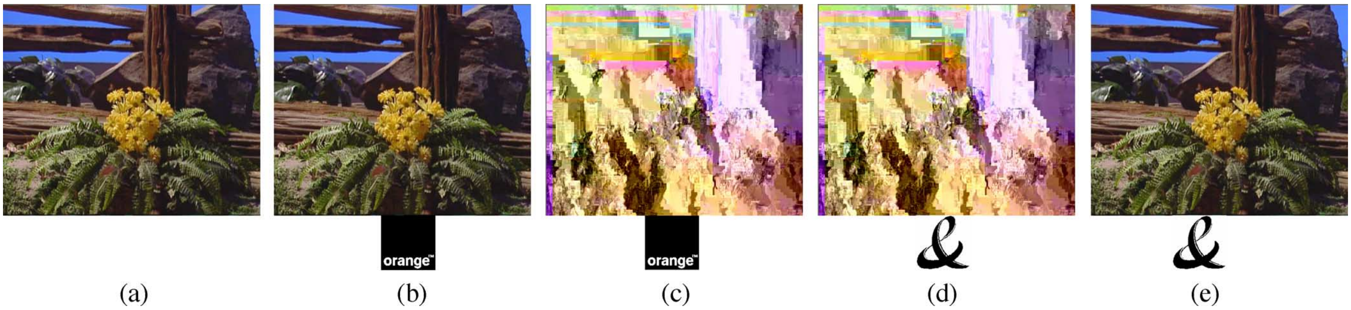


Fig. 5. Videos are produced in the commutative encryption and watermarking scheme. (a) Original. (b) Watermarked video and the detected watermark. (c) Encrypted video and the detected watermark. (d) Re-watermarked video and the detected watermark. (e) Decrypted video and the detected watermark.

Otherwise

$$z' = \begin{cases} z, & \text{if } \lceil |z|/q \rceil \% 2 = 0 \\ \left(\lceil |z|/q \rceil - 1\right) q \cdot \mathrm{Sign}(z), & \text{if } \lceil |z|/q \rceil \% 2 = 1 and z \neq -q \, . \\ 2q \cdot \mathrm{Sign}(z), & \text{if } z = -q \end{cases} \tag{4}$$

Here, $\mathrm{Sign}(z)$ denotes the sign of z, $|z|$ denotes the absolute value of z, $\lceil a \rceil$ is the minimal integer no smaller than a, % is the operation of getting remainder, and q is the quantization step.

Two differences are introduced compared with the traditional one [20]: 1) Use "+" in (3) while "−" in (4); 2) Set z be $2q \cdot \mathrm{Sign}(z)$ when z equals to $-q$. The first one makes the coefficient change in a small range after iterated watermarking, while the second one keeps the coefficient's sign unchanged. As an example, we compare the modified method and the traditional one through re-watermarking the quantized coefficients "2,1,0,−1,−2" for four times, as shown in Table I. In the traditional method, the watermarked coefficient's amplitude increases with the iteration time (e.g., from −1 to −5). In the traditional method with the first change, the coefficient's sign changes from negative to positive (e.g., from −1 to 1). In the proposed method, the coefficient's sign keeps unchanged and the amplitude changes slightly. Additionally, the proposed scheme and the traditional one keep similar robustness against some attacks in StirMark 4.0 [24]. Thus, the proposed method is more suitable for commutative encryption and watermarking.

C. Watermark Extraction and Re-Watermarking

In this scheme, the watermark can be extracted from the encrypted video directly, and a new watermark can also be embedded into the encrypted video directly. The decryption operation is symmetric to encryption operation. The watermark extraction operation is defined as

$$w = \begin{cases} 0, & \text{if } \lceil |z|/q \rceil \% 2 = 0 \\ 1, & \text{if } \lceil |z|/q \rceil \% 2 = 1. \end{cases} \tag{5}$$

III. Performance Analysis

A. Security

For the proposed scheme, the security includes both cryptographic security and perception security.

Cryptographic Security: Cryptographic security depends on the ciphers adopted by the scheme. In the proposed scheme, traditional ciphers are adopted, which confirms the scheme's security. In the following content, the 128-bit AES cipher is used to encrypt the selected parameters, and the stream cipher [7] is used to encrypt the watermark.

Perception Security: For video encryption, it is important to keep the encrypted video unintelligible, which is regarded as perception security. Generally, it depends on the encryption scheme's properties. For example, encrypting only prediction information [9] can not keep secure enough, since the encrypted video is intelligible. The proposed scheme encrypts both prediction information and residue, which keeps perception security. The comparison is shown in Figs. 2 and 3, in which, each video frame is encrypted with a subkey. As can be seen, the proposed method ranks second in perception security. Some attacks adopt the unencrypted parameters to reduce media content's distortions, such as replacement attack [10] or Said's attack [25]. They are effective when the media content is slightly distorted, such as IPM scrambling [9] or sign encryption of ac's [25]. However, in the scheme proposed by us, ac's sign, dc's sign, IPM and MVD are all encrypted, which distorts media content greatly and thus enlarges the attacks' difficulty greatly.

B. Robustness and Imperceptibility

The proposed watermarking scheme's imperceptibility and robustness are tested. Fig. 4(a) shows the proposed scheme's imperceptibility. Generally, the imperceptibility decreases with the quantization step q. The robustness against recompression is shown in Fig. 4(b). The detected bit-error rate (BER) rises with quantization paramter (QP) when q is certain, while decreases with q when QP is certain. Generally, to keep BER small, the q with big value is preferred. For example, to keep BER no bigger than 80%, the q corresponding to QP $= 36$ is preferred.

C. Commutation

Fig. 5 shows the videos and the contained watermarks in the commutative encryption and watermarking process. Here, the video is watermarked, encrypted, re-watermarked and decrypted in order. As can be seen, the first watermark can be extracted from the encrypted video, and the second watermark can be extracted from the decrypted and re-watermarked video. Thus, the encryption and watermarking operations are commutative in this scheme. Compared with the traditional watermarking method [20], the proposed method obtains the

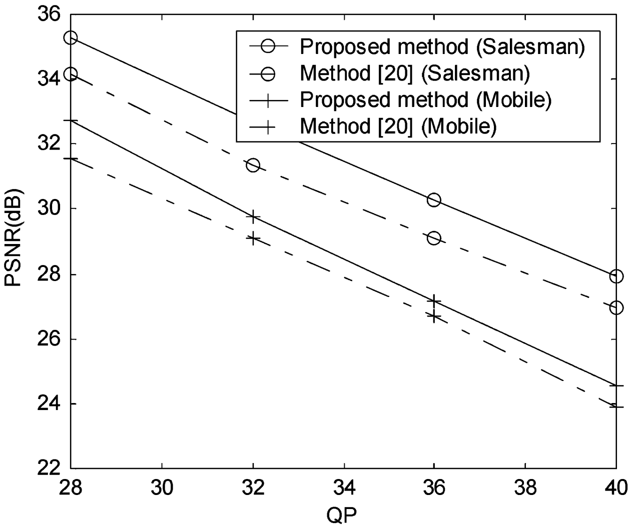


Fig. 6. Traditional watermark and commutative watermark are compared. The encrypted videos are watermarked iteratively for five times.

video with better quality after multiple re-watermarking, as shown in Fig. 6. Thus, the proposed watermarking method is more suitable for the commutative watermarking and encryption scheme.

IV. Conclusions and Future Work

In this paper, a commutative video watermarking and encryption scheme based on H.264/AVC codec is presented. The video is watermarked and/or encrypted during H.264/AVC compression process. The modified watermarking algorithm makes the watermarking operation and encryption operation commutative. The scheme keeps secure against present attacks, is efficient in implementation, keeps imperceptible, and is robust against recompression in some extent. These properties make the scheme a choice for secure video transmission or distribution. In future work, the encryption algorithm's security against such new attack as replacement attack or Said's attack will be evaluated, and some means will be taken to improve the watermark's robustness against such attack as collusion or desynchronization.

References

[1] S. S. Maniccam and G. B. Nikolaos, "Image and video encryption using SCAN patterns," *Pattern Recognit.*, vol. 37, no. 4, pp. 725–737, 2004.

[2] E. I. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in digital video content protection," *Proc. IEEE*, vol. 93, no. 1, pp. 171–183, Jan. 2005.

[3] C. Wu and C. C. J. Kuo, "Efficient multimedia encryption via entropy codec design," in *Proc. SPIE Int. Symp. Electronic Imaging 2001*, Jan. 2001, vol. 4314, pp. 128–138.

[4] L. Qao and K. Nahrstedt, "A new algorithm for MPEG video encryption," in *Proc. 1st Int. Conf. Imaging Science, Syst. Technol. (CISST'97)*, Las Vegas, Nevada, Jul. 1997, pp. 21–29.

[5] L. Qiao and K. Nahrstedt, "Comparison of MPEG encryption algorithms," *Int. J. Comput. Graph., Special Issue on Data Security in Image Communication and Network*, vol. 22, no. 4, pp. 437–448, 1998.

[6] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 118–129, Jan., 2003.

[7] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone*, Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 2001.

[8] *Advanced Video Coding. Final Committee Draft, Document JVT-E022*, ITU-T Rec. H.264/ISO/IEC 11496-10, Sep. 2002.

[9] J. Ahn, H. Shim, B. Jeon, and I. Choi, "Digital video scrambling method using intra prediction mode," in *Proc. PCM 2004*, Nov. 2004, vol. 3333, pp. 386–393.

[10] S. Lian, Z. Liu, Z. Ren, and Z. Wang, "Selective video encryption based on advanced video coding," in *Proc. PCM 2005, Part II*, 2005, vol. 3768, pp. 281–290.

[11] T. Shi, B. King, and P. Salama, "Selective encryption for H.264/AVC video coding," in *Security, Steganography, Watermarking Multimedia Contents VIII*, 2006, vol. 6072, p. 607217.

[12] P. Moulin and R. Koetter, "Data-hiding codes," *Proc. IEEE* , vol. 93, no. 12, pp. 2083–2126, Dec. 2005.

[13] C.-P. Wu and C.-C. J. Kuo, "Fragile speech watermarking for content integrity verification," in *Proc. IEEE 2002 Int. Symp. Circuits Systems*, 2002, vol. 2, pp. 436–439.

[14] J. A. Bloom, I. J. Cox, T. Kalker, J. P. Linnartz, M. L. Miller, and C. B. Traw, "Copy protection for digital video," *Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information*, vol. 87, no. 7, pp. 1267–1276, Jul. 1999.

[15] E. Hauer and S. Thiemert, "Synchronization techniques to detect MPEG video frames for watermarking retrieval," in *Proc. SPIE Security Watermarking Multimedia Contents IV*, 2004, vol. 5306, pp. 315–324.

[16] H. Joumaa and F. Davoine, "An ICA based algorithm for video watermarking," in *Proc. ICASSP 2005*, vol. 2, pp. 805–808.

[17] T.-H. Chen, S.-H. Liu, H.-X. Yao, and W. Gao, "Robust video watermarking based on dc coefficients of selected blocks," in *Proc. 4th Int. Conf. Mach. Learning Cybernetics*, Aug. 2005, pp. 5273–5278.

[18] G. Qiu, P. Marziliano, A. T. S. Ho, D. He, and Q. Sun, "A hybrid watermarking scheme for H.264/AVC video," in *Proc. 17th Int. Conf. Pattern Recognit. (ICPR'04)*, 2004, vol. 4, pp. 865–868.

[19] J. Zhang and A. T. S. Ho, "An efficient digital image-in-image watermarking algorithm using the integer discrete cosine transform (IntDCT)," in *IEEE Joint Conf. 4th Int. Conf. Information, Commun. Signal Process. 4th Pacific-Rim Conf. Multimedia*, Dec. 2003, pp. 1163–1167.

[20] M. Noorkami and R. M. Mersereau, "Compressed-domain video watermarking for H.264," in *IEEE Conf. Image Process.*, Sep. 2005, vol. 2, pp. 890–893.

[21] D. Profrock, H. Richter, M. Schlauweg, and E. Muller, "H.264-AVC video authentication using skipped macroblocks for an erasable watermark," in *Proc. SPIE Visual Commun. Image Process.*, 2005, vol. 5960, pp. 1480–1489.

[22] T. Wu and S. Wu, "Selective encryption and watermarking of MPEG video," in *Proc. Int. Conf. Image Science, Syst. Technol. CISST'97*, Los Angeles, CA, Feb. 1997, pp. 261–269.

[23] D. Simitopoulos, N. Zissis, P. Georgiadis, V. Emmanouilidis, and M. G. Strintzis, "Encryption and watermarking for the secure distribution of copyrighted MPEG video on DVD," *ACM Multimedia Syst. J., Special Issue on Multimedia Security*, vol. 9, no. 3, pp. 217–227, Sep. 2003.

[24] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. Inf. Hiding, 2nd Int. Workshop, IH'98*, D. Aucsmith, Ed., Portland, OR, Apr. 1998, vol. 1525, pp. 219–239.

[25] A. Said, "Measuring the strength of partial encryption schemes," in *Proc. 2005 IEEE Int. Conf. Image Process. (ICIP 2005)*, vol. 2, pp. 1126–1129.