Efficient and Format-Compliant Video Encryption Algorithm in Compressed Domain for H.264/AVC

Li ZHUO, Niansheng MAO, Haojie SHEN, Jing ZHANG, Xiaoguang LI

Signal and Information Processing Laboratory, Beijing University of Technology, Beijing, China

zhuoli@bjut.edu.cn, mns150@sohu.com, 13810761814 @139.com, zhj@bjut.edu.cn, lxg@bjut.edu.cn

***Abstract*—In this paper, an efficient video encryption scheme is proposed for protecting H.264 bitstream. The issues on the compressed domain video encryption have been pointed out and fully addressed. In the proposed scheme, only the most significant bits for video reconstruction in H.264 bitstream are extracted and encrypted, to optimize the trade-off between security level and computational complexity. For intra-frames, only the codewords of intra4×4 prediction mode and the sign bits of the low frequency DCT coefficient are encrypted. For inter-frames, the info_suffix of motion vector difference (MVD) are encrypted. Owing to the proposed scheme is independent of the compression process, thus does not need to modify the structure of H.264 standard codec. Experimental results show that the proposed scheme exhibits significant computational efficiency and reliable security, can resist not only perceptual attacks but also brute-force attacks. Furthermore, it adds a little memory overhead. Therefore, the proposed scheme will be well suited for real-time video applications and resource-limited systems such as smartphone and wireless sensor network.**

***Index Terms*—Video encryption, Security, H.264, Bitstream, Compressed domain**

I. INTRODUCTION

With the rapid development of computer and network technology, multimedia systems such as videophone, video surveillance and telemedicine, have been widely used. The security and privacy of multimedia content are becoming more and more prominent. Conventional cryptographic algorithms such as data encryption standard (DES) [1] and advanced encryption standard (AES) [2] are difficult to be applied directly to multimedia content duo to the large volume of data and real-time video requirements. Furthermore, in the case of the wireless mobile terminals, limited processing power, memory and bandwidth always fail to meet the encryption processing overhead. Thus, efficient video encryption schemes need to be designed.

In real-world applications, a video encryption scheme should take various requirements into account, such as security, computational efficiency, compression efficiency, format-compliance and so forth. Different video applications require variable levels of security. For example, for Video on Demand (VoD) or pay-TV, low security is often required, and even nonpaying users are allowed to access low quality versions to promote them to buy high quality versions, whereas for military secrets or financial information, strict security is demanded to completely prevent the unauthorized access. The computational efficiency means that the encryption or decryption process can not cause too much time delay, to meet the requirements of real-time applications. Video compression is employed to reduce the storage space and save bandwidth, so that the encryption process should have a least impact on the compression efficiency. The format-compliance, also known as syntax-compliance [3], means that the encryption scheme should do not change the syntax structure of the compressed bitstream, thus ensures features like cutting, copying, adding or removing, and ability of the encrypted bitstream still can be decoded by a standard decoder.

In recent years, many video encryption algorithms have been proposed. As pointed out in [4], these algorithms according to their association with video compression can be classified into two categories, called compression-joint encryption algorithms and compression-independent encryption algorithms. For the former, the encryption algorithms are embedded in a certain step of the compression process. For example, some algorithms permute or scramble the residual coefficients after the Discrete Cosine Transform (DCT) [5]-[7], some algorithms encrypt the signs of DCT coefficients or motion vector difference (MVD) after quantization [8], [9], and some algorithms selectively encrypt intra-prediction modes, DCT coefficients, and MVD during the entropy coding [10]-[12].

Manuscript received May 3, 2012. This work was sponsored by the Program for New Century Excellent Talents in University, the Excellent Science Program for the Returned Overseas Chinese Scholars of Ministry of Human Resources and Social Security of China, Scientific Research Foundation for the Returned Overseas Chinese Scholars of MOE.

Li ZHUO is currently a professor of the Beijing University of Technology, Beijing, China (email: zhuoli@bjut.edu.cn)

Niansheng MAO was a master student of the Beijing University of Technology, Beijing, China (email: mns150@sohu.com)

Haojie SHEN is currently a master student of the Beijing University of Technology, Beijing, China (email: 13810761814 @139.com)

Jing ZHANG is currently an associate professor of the Beijing University of Technology, Beijing, China (email: zhj@bjut.edu.cn)

Xiaoguang LI is currently an associate professor of the Beijing University of Technology, Beijing, China (email: lxg@bjut.edu.cn)

As these encryption algorithms are all accomplished before the last step of the video compression process, all the encrypted bitstreams can be decoded by a standard decoder without being decrypted, while only obtain the unintelligible video. However, encrypting or scrambling the DCT coefficients during the compression process usually destroys the inherent energy impact capability of the DCT transform, resulting in low compression efficiency.

Differently, for the compression-independent encryption algorithms, the compression and encryption process are carried out separately. These algorithms often directly encrypt the compressed bitstream, also known as compressed domain video encryption. In [13], the odd indexed bytes in video bitstream are firstly encrypted with a conventional cryptographic algorithm, and used as keys to XOR with the even indexed bytes. In [14], the bitstream according to their importance for decoding are divided into five types, and the first three are encrypted whereas others remain. Both of the above algorithms can ensure enough security, but are all of low computational efficiency and loss the format-compliance. In [3], the codewords of DCT coefficients and MVD in compressed bitstream are shuffled. In [15], the codewords of intra-prediction mode are encrypted. Both of them demonstrate high computational efficiency and maintain the format-compliance, but are of low security. As can be seen, the various existing compressed domain encryption schemes cannot optimize the trade-off between security level and computational complexity, and are often difficult to maintain the format-compliance. Therefore, the compressed domain video encryption algorithms need to be further studied.

In this paper, we propose an efficient compressed domain video encryption scheme for protecting H.264 bitstream. The proposed scheme directly extracts the most significant bits for video reconstruction in H.264 bitstream, concatenates them in an appropriate way to form a sub-bitstream, and then encrypts the sub-bitstream with a conventional cryptographic algorithm such as AES. After the encryption process, the encrypted bits are put back into their original positions.

The rest of this paper is organized as follows. Section II analyses the H.264 bitstream syntax structure. Details of the proposed video encryption scheme are described in Section III. The performance of the proposed scheme is discussed in Section IV. Section V presents some conclusions.

II. H.264 BITSTREAM SYNTAX STRUCTURE

H.264/AVC [16] is the state-of-the-art video coding standard. Compared with the previous standards such as MPEG-2, H.263, it not only has excellent compression performance, but also has a "network-friendly" bitstream structure. In general, the basic unit of the H.264 bitstream is variable length code (VLC) codewords and fixed length code (FLC) codewords, which are formed by a number of bits and represent different information types. These codewords play different roles in the decoding process. For example, the codewords of the header include synchronization information, and the codewords of MVD contain video motion information and so forth. In order to improve the encryption scheme pertinence and efficiency, the structure of the H.264 bitstream will be firstly analysed in this section.

To achieve higher compression efficiency, the H.264 bitstream is organized with a hierarchical structure, as shown in Figure 1. The H.264 bitstream can be divided into a series of Network Abstraction Layer (NAL) units. Each NAL unit contains NAL header information and a Raw Byte Sequence Payload (RBSP), which can be Sequence Parameter Set (SPS), Picture Parameter Set (PPS) or a coded slice. Among them, the SPS contains SPS_id, profile and level, the number of reference frames, image width and height, and so on. The PPS contains PPS_id, SPS_id, entropy coding mode, reference frame index, the initial quantization parameter (QP), and so on. The SPS and PPS do not correspond to a particular sequence or image, in other words, an SPS can be used for multiple sequences and a PPS can also be used for multiple images. The coded slice consists of slice header (including slice type, PPS_id and QP offset) and a number of macroblock (MB) data.

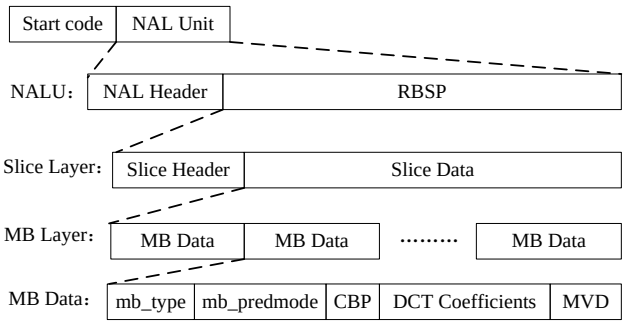


Fig. 1. H.264 bitstream hierarchical structure.

For video encryption, the SPS, PPS and slice header only provide nominal security, as these coding parameters do not contain too much information and usually have a fixed format. The MB data can be classed into intra-macroblock data (including MB_type, intra-prediction mode, coded block pattern (CBP) and DCT coefficients) and inter-macroblock data (including MB_type, inter-prediction mode, CBP, MVD and DCT coefficients). Among them, the DCT coefficients contain video texture information, the MVD contain video dynamic information, and the intra-prediction mode indicates the predicted direction. All these information are the most important for video reconstruction. Therefore, in order to obtain high security, the codewords of intra-prediction mode, DCT coefficient, and MVD in H.264 bitstream should be encrypted.

III. THE PROPOSED ENCRYPTION SCHEME

Based on the above analysis, an efficient compressed domain encryption scheme is proposed in this section. For intra-prediction mode, the codewords are encrypted with IPME algorithm [15], for the low frequency DCT coefficients of intra-frames, only the sign bits are extracted and encrypted, and for the motion vector difference, the info_suffix of the codewords are encrypted. The proposed scheme is shown in Figure 2.

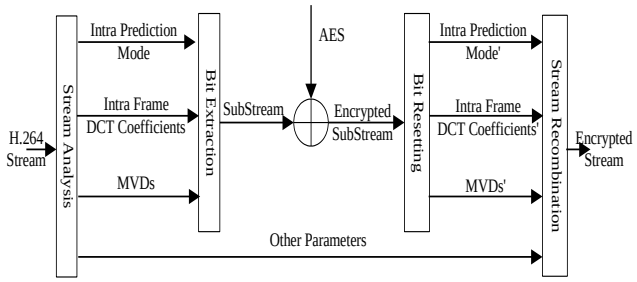


Fig. 2. Diagram of the proposed encryption scheme.

A. Intra-Prediction Mode Encryption

In H.264 bitstream, the intra4×4 prediction mode is denoted by two syntax elements, prev_intra4×4_pred_mode with 1bit and rem_intra4×4_pred_mode with 3 bits. If the prev_intra4×4_pred_mode is set to '1', the current block uses the most_probable_mode, which is the minimum of the prediction modes of its two neighboring upper and left blocks, and the rem_intra4×4_pred_mode is not adopted. Otherwise, the prev_intra4×4_pred_mode is set to '0', and the prediction mode of the current block is presented by the rem_intra4×4_pred_mode.

In IPME algorithm [15], only the codewords of the rem_intra4×4_pred_mode in H.264 bitstream are encrypted. The algorithm is simple and computationally efficient, but lacks of security due to the limited encryption space. In the improved algorithm [17], in order to obtain higher security, when the prev_intra4×4_pred_mode is set to '1', the encryption operation is to reset it to '0' and inserts 3 bits chaotic sequence as the rem_intra4×4_pred_mode, and all the intra4×4 prediction modes are encrypted by chaotic pseudo random sequence. However, the improved algorithm significantly increases the computational complexity, and bears a large amount of processing overhead and memory requirements. Thus, the codewords of intra4×4 prediction modes are encrypted with IPME in the proposed scheme.

Differently, the intra16×16 prediction modes are jointly encoded with the luma and chroma CBP using the unsigned Exp-Golomb entropy coding. The CBP indicates which blocks within a macroblock contain DCT coefficients, so that its values should not be changed during encryption, otherwise the encrypted bitstream will loss the format-compliance. Thus, the proposed scheme does not encrypt the intra16×16 codewords.

B. DCT Coefficients Encryption

The DCT coefficients in H.264 baseline profile are encoded with the context-based adaptive variable length coding (CAVLC). The encoding process can be described as follows [16]:

- Encoding the number of coefficients and trailing ones (coeff_token),
- Encoding the sign of each trailing ones,
- Encoding the levels of the remaining non-zero coefficients,
- Encoding the total number of zeros before the last coefficient, and
- Encoding each run of zeros.

After the CAVLC process, the residual data is represented by numerous coding parameters such as the number of nonzero coefficients and trailing ones (coeff_token), the sign of trailing ones (TrailingOnes), the remaining nonzero coefficients (NonCoeff), the total number of zeros before the last coefficient (TotalZeros) and each run of zeros (run_before). Since it is context adaptive, in order to maintain the format-compliance, the context adaptive property should not be destroyed during the encryption. In other words, the codewords of coeff_token, TotalZeros and run_before should not be changed. More specifically, only the sign bits of NonCoeff codeword and the codewords of TrailingOnes can be encrypted. For optimize the tradeoff between security and computational complexity, only the sign bits of the low frequency DCT coefficients of intra-frames are encrypted in the proposed scheme.

C. MVD Encryption

In H.264, each MVD is independently coded by the signed Exp-Golomb entropy coding. It means that the MVD codewords in H.264 bitstream are mutually independent. Furthermore, each MVD codeword in H.264 bitstream is constructed as [M Zeros][1][INFO], where INFO is a M-bit suffix information called info_suffix. Here, the MVD level is $X = 2^M + INFO - 1$ and the last one bit of the info_suffix is the MVD sign. Therefore, the entire info_suffix of the MVD codewords should be extracted and encrypted.

IV. PERFORMANCE ANALYSIS

In our experiments, a variety of standard video sequences in CIF and QCIF format, such as "Akiyo", "Foreman", "Mobile", "Football", "Tempete" and "Silent" are applied to demonstrate the performance of the proposed encryption scheme. Each video sequence contains 150 frames. These videos are all encoded by JM86 with a frame rate 15Hz, and the intra-frame period is set as 15. The performance of the proposed scheme, such as security, computational complexity and memory requirement, are analysed as follow.

A. Security

For video encryption, the security requires not only cryptographic security but also perceptual security. The former one specifically deals with the security against

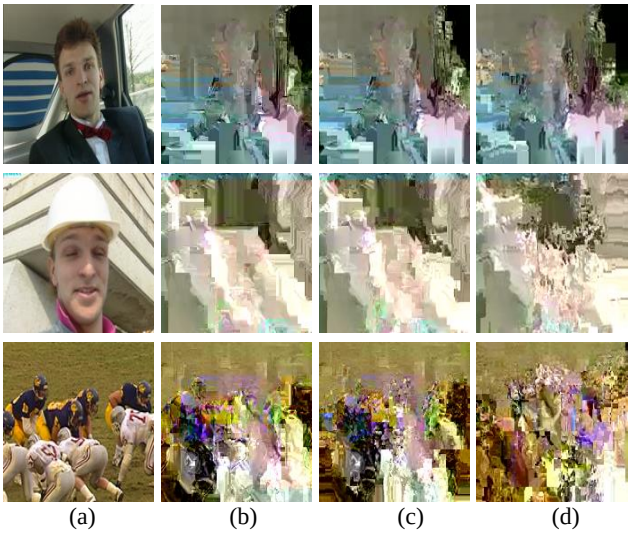
cryptographic attacks, for example, brute-force attacks. The perceptual security means that, whether or not the perceptual attacks such as the error-concealment-based attacks and the replacement attacks are used, the encrypted video remain appears unintelligible to a viewer without being decrypted.

1) Perceptual security

As we know, the most significant bits for video reconstruction in H.264 bitstream are encrypted in the proposed scheme. That is to say, the proposed scheme will make it difficult to recognize the encrypted videos. Figure 3 shows the encrypted results of several videos. It is obvious that all the encrypted videos appear unrecognizable. Besides, the quality of the encrypted videos is measured with the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity (SSIM) respectively. As can be seen from Table 1, for the encrypted videos, the PSNR value is all about 10 dB and the SSIM value is less than 0.3, both of them are much lower compared with the corresponding original videos. Thus, the proposed scheme can achieve a high perceptual security.

TABLE I
The encrypted videos quality

Size	Video	PSNR-Y(dB)		SSIM	
		Original	Encrypt	Original	Encrypt
QCIF	Akiyo	38.54	11.25	0.969	0.273
	Carphone	37.24	8.65	0.965	0.238
	Hall	37.43	9.38	0.971	0.208
	Silent	36.01	7.64	0.947	0.224
CIF	Foreman	36.82	7.81	0.936	0.257
	Football	36.53	12.77	0.933	0.282
	Harbour	34.41	9.99	0.962	0.057
	Tempete	34.67	9.01	0.961	0.094
	City	34.94	10.51	0.931	0.159



(a) (b) (c) (d)

Fig. 3. The encrypted results of several videos. The column (a) is the original frames, the column (b) is the encrypted intra-frames, and the column (c) and (d) are the firth and last inter-frames in a GOP respectively.

2) Perceptual attacks

The error-concealment-based attack means that the attackers usually treat the encrypted data as bit-error or packet-loss, and then try to minimize the impact on video reconstruction as a result of the encryption by using various error-concealment techniques. However, it is very difficult for an attacker to identify the encrypted parts from a format-compliant encrypted bitstream and therefore the error-concealment-based attacks become invalid. The replacement attack is to attempt to recover the encrypted information and make it more visually acceptable by replacing the encrypted data with some particular data. For example, the encrypted intra-prediction modes can be replaced by the most_probable_mode (the minimum of the prediction modes of its neighbouring blocks), since the adjacent blocks often have the same intra-prediction modes. Figure 4 shows the recovered frames with replacement attacks. As can be seen, the recovered frames remain unintelligible after replacement attacks. Therefore, the proposed scheme is secure enough against the replacement attacks.

(a) (b) (c)

Fig. 4. The recovered frames with replacement attacks. (a) and (b) are the recovered frames by replacing the intra-prediction mode, (c) is the recovered frame by replacing the sign bits of MVD.

3) Brute-force attacks

For video encryption algorithms, the brute-force attack is not only based on cryptographic system analysis trying to enumerate all the system keys but also to enumerate the intra-prediction modes, DCT coefficients and MVD. Since the AES supports 128, 192 and 256 bits key length, the minimum brute-force space is 2^{128}. That is to say, the brute-force space for each encrypted frame using the proposed scheme is 2^{128}. It is too large for attackers to break the cryptographic system. In addition, the brute-force space of the intra-prediction mode, the sign of DCT coefficient and MVD are 2^3, 2 and 2^R (R is the length of the info_suffix of MVD), respectively. Therefore, for a W×H size frame, the brute-force space of intra-frame is $S_{intra} = [2^3 \cdot 2^L]^M, L \geq 0, M = WH/256$, where L is the number of the encrypted low frequency DCT coefficients, and the brute-force space of inter-frame is $S_{inter} = [2^3]^{N_1} \cdot [2^R]^{2N_2}, R \geq 1$, $N_1 + N_2 = WH/256$, where N_1 and N_2 are the number of intra-coded macroblocks and inter-coded macroblocks respectively. Taking QCIF (W×H =176×144) for example, the brute-force space is $S_{intra} \geq 2^{297}$ and $S_{inter} \geq 2^{198}$. Similarly, this brute-force space is also large enough to resist brute-force attacks.

B. Computational complexity

The proposed scheme can be achieved after three steps, including bit extraction, encryption and bit resetting. Hence, the computational complexity of the proposed scheme will mainly depend on these three steps. In the bit extraction process, the codewords of intra-prediction mode, DCT coefficients and MVD can be quickly detected according to the H.264 bitstream hierarchical structure, and then the bits which should be encrypted are directly extracted from these codewords based on the corresponding entropy coding without being decoded firstly. For example, the info_suffix of MVD can be extracted according to the M-bit leading zeros. The encryption time consumption depends on the data volumes to be encrypted. Table 2 gives the ratio between the encrypted data and the entire bitstream (Edr) of various standard videos. The table clearly shows that all the Edr are no more than 15%. To save the bit resetting time consumption, the location information of the encrypted bits is recorded during the bit extraction processing, so that the encrypted bits can be easily put back into their original position just like a replacement. Thus, the computational complexity of the proposed scheme will be very low.

In our experiments, the Encryption-to-compression time ratio (Etr) and the Decryption-to-decompression time ratio (Dtr) are tested. Table 3 gives the experimental results of various videos, where the proposed scheme is called PEH264. As can be seen, most of the Etr of the proposed scheme is no more than 1%, and the Dtr of the proposed scheme is also no more than 5% and 10% for QCIF and CIF videos respectively. In addition, the Etr and Dtr of the proposed scheme are all superior in comparison to the SEH264 algorithm [11]. All in all, the proposed scheme obtains significant computational efficiency. Thus, it will be well suited for real-time video applications.

TABLE II
The Edr testing results

Size	Video	Edr	Size	Video	Edr
QCIF	Akiyo	10.02%	CIF	Akiyo	9.60%
	News	9.35%		Mobile	10.46%
	Mother	8.68%		Tempete	7.03%
	Salesman	11.76%		Football	11.09%
	Foreman	10.76%		Foreman	9.82%

TABLE III
The Testing Results of Computational Cost

Video	Size	Time ratio			
		Encryption/ Compression		Decryption/ Decompression	
		SEAH264	PVEA	SEAH264	PVEA
Foreman	QCIF	0.9%	0.5%	5.2%	2.9%
Akiyo	QCIF	1.1%	0.6%	4.9%	4.6%
Mother	QCIF	0.7%	0.3%	5.9%	2.8%
Akiyo	CIF	0.7%	0.4%	6.1%	3.6%
Foreman	CIF	1.0%	0.3%	6.2%	4.3%
Mobile	CIF	0.9%	0.8%	6.2%	5.8%

C. Memory requirement

Generally, the larger amount of data is processed in encryption, the more memory is required. Therefore, the memory requirement of the proposed scheme can be measured by the amount of the encrypted data. Figure 5 shows the ratio between the encrypted data and the corresponding slice data. As can be seen, for intra-frames, the encrypted data is about 15% of the corresponding slice data, and for inter-frames, the ratio is only about 5%. That is because, considering intra-frames are more important than inter-frames, the proposed scheme provides enhanced encryption to this kind of information. All in all, compared with the existing encryption schemes, the proposed scheme adds less overhead of memory requirement.

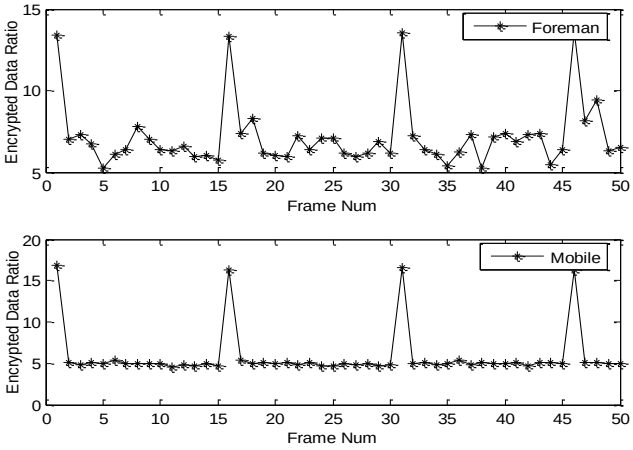


Fig. 5. The encrypted data ratio versus frame number

V. CONCLUSION

In this paper, an efficient video encryption scheme in H.264 compressed domain has been proposed. Firstly, the hierarchical structure of the H.264 bitstream is analysed, to detect the most significant bits for video reconstruction in H.264 bitstream. Then, the rem_intra4×4_pred_mode of the intra-prediction mode codewords, the sign bit of the low frequency DCT coefficients of intra-frames and the info_suffix of the MVD codewords are directly extracted and encrypted with the AES algorithm. Experimental results show that the proposed scheme exhibits reliable perceptual security, can secure against not only replacement attacks but also brute-force attacks, and meanwhile obtains significant computational efficiency. Furthermore, it maintains the format-compliance to the H.264 standard decoder and has no impact on the compression ratio. Thus, the proposed scheme will be well suited for real-time video applications and resource-limited systems such as smartphone and wireless sensor network.

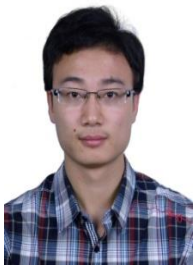
REFERENCES

[1] Data Encryption Standard (DES), FIPS PUB 46, Jan. 1977.
[2] Advanced Encryption Standard (AES), FIPS-PUB 197, Nov. 2001.

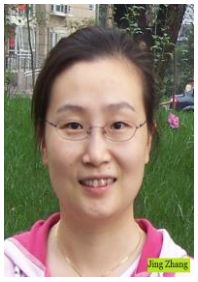
[3] J. Wen, M. Severa, W. Zeng, *et al*, "A format-compliant configurable encryption framework for access control of video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 6, pp. 545-557, Jun. 2002.
[4] F. Liu and H. Koenig, "A survey of video encryption algorithms," *Computers and Security*, vol. 29, pp. 3-15, Feb. 2010.
[5] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," *Proceedings of the 4th Multimedia Conference (ACM Multimedia 96)*, pp. 219-229, Boston, MA, USA, Nov. 1996.
[6] A. S. Tang and W. C. Feng, "Efficient multi-layer coding and encryption of MPEG video streams," *IEEE International Conference on Multimedia and Expo.*, vol. 1, pp. 119-122, Aug. 2000.
[7] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 118-129, Mar. 2003.
[8] C. Shi and B. Bharqava, "An Efficient MPEG video encryption algorithm," *Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems*, pp. 381-386, Oct. 1998.
[9] C. Shi, S. Wang, and B. Bhargava, "MPEG video encryption in real-time using secret key cryptography," *In Proc. of PDPTA'99*, Las Vegas, Nevada, pp.2822-2828, 1999.
[10] C. P. Wu and C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia*, vol. 7, no. 5, pp. 828-839, Oct. 2005.
[11] S. Lian, Z. Liu, Z. Ren and H. Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 2, pp. 621-629, May 2006.
[12] J. Zhou, Z. Liang, Y. Chen and O. C. Au, "Security analysis of multimedia encryption schemes based on multiple Huffman table," *IEEE Signal Processing Letters*, vol. 14, no. 3, pp. 201-204, Mar. 2007.
[13] L. Qao and K. Nahrstedt, "A new algorithm for MPEG video encryption," *Proceedings of the First International Conference on Imaging Science, Systems and Technology (CISST'97)*, pp. 21-29, Las Vegas, Nevada, July 1997.
[14] T. Shi, B. King and P. Salama, "Selective encryption for H.264/AVC video coding," *In SPIE International Society for Optical Engineering (San Jose, CA, USA)*, vol. 6072, pp. 171-179, Feb. 2006.
[15] J. Ahn, H. Shim, B. Jeon and I. Choi, "Digital Video Scrambling Method Using Intra Prediction Mode," *Advanced in Multimedia Information Processing PCM2004*, vol. 3333, pp. 386-393, Dec. 2004.
[16] T. Wiegand, G. J. Sullivan, G. Bjntegaard, *et al*, "Overview of the H.264/AVC video coding standard," *IEEE Tran. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560-576, July 2003.
[17] J. Jiang, S. Xing and M. Qi, "An intra prediction mode-based video encryption algorithm in H.264," *International Conference on Multimedia Information Networking and Security (MINES 2009)*, pp. 478-482, Hubei, China, Nov. 2009.
[18] Y. Mao, and M. Wu, "A joint signal processing and cryptographic approach to multimedia encryption," *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 2061-2075, July 2006.

Li ZHUO received the B.E degree in Radio Technology from the University of Electronic Science and Technology, Chengdu, China, in 1992, the M.E degree in Signal & Information Processing from the Southeast University, Nanjing, in 1998, and the PH.D degree in Pattern Recongnization and Intellectual System from Beijing University of Technology, in 2004. She has been a professor in Beijing University of Technology since 2007. She has published over 160 research papers and authored 4 books. Her research interest includes image/video coding and transmission， multimedia content analysis, Multimedia information security.

Niansheng MAO received the B.E degree in Electronic and Information Engineering from the Beijing University of Technology, Beijing, China, in 2005, the M.E degree in Information and Communication Engineering from the Beijing University of Technology, Beijing, China, in 2012. His research interest includes video coding, scalable video coding, multimedia information security.



Haojie SHEN received the B.E degree in Electronic and Information Engineering from the Beijing University of Technology, Beijing, China, in 2011. He is currently pursuing the M.E degree in Information and Communication Engineering from the Beijing University of Technology, Beijing, China. His research interest includes video coding, multimedia information security.



Jing ZHANG received the Ph.D degree from Beijing University of Technology. She is currently an associate professor and a master supervisor at Beijing University of Technology-China and the Signal & Information Processing Lab. Her research interests include image/video processing, retrieval.

Xiaoguang LI was born in Beijing, China. He received the B.E and Ph.D degrees in Electronic Engineering from the Beijing University of Technology, Beijing China, in 2003 and 2008 respectively. He is currently an Associate Professor and master student supervisor of the Beijing University of Technology. His research interests include image and video processing and computer vision.