基于 CAC的数字视频安全编码研究

汪银苗[1),2),3)] 包先雨[1),3)]

[1)] (合肥工业大学计算机与信息学院, 合肥 230009) [2)] (安徽职业技术学院基础部, 合肥 230051)

[3)] (安全关键工业测控技术教育部工程研究中心, 合肥 230009)

摘 要 对于视频压缩领域, 基于上下文的自适应编码 (CAC)是一类新出现的高效熵编码方法。为了对数字视频进行实时安全编码, 提出了一种基于 CAC的数字视频安全编码方案, 并首先建立了以 CAC安全编码器为核心的安全编码链, 然后给出了基于上下文的自适应二进制算术安全编码 (CABASC)和基于上下文的自适应变长安全编码 (CAVLSC)两种安全编码操作。实验结果表明, 该方案具有较好的安全性、实时性和软件易实现性, 可作为进一步研究 CAC安全编码的基础。

关键词 安全编码 视频加密 基于上下文的自适应二进制算术安全编码 基于上下文的自适应变长安全编码

中图法分类号: TN918 74 **文献标志码**: A **文章编号**: 1006-8691(2010)01-0001-06

Study of CAC-based Secure Coding of Digital Video

WANG Yin-miao[1),2),3)], BAO Xian-yu[1),3)]

[1)] *(Department of Computer and Information, Hefei University of Technology, Hefei 230009)*

[2)] *(Department of Fundamentals, Anhui Vocational and Technical College, Hefei 230051)*

[3)] *(Engineering Research Center of Safety Critical Industrial Measurement and Control Technology, Ministry of Education, Hefei 230009)*

Abstract Context-based adaptive coding (CAC) is a class of new high-efficient entropy coding techniques for video compression. In this paper, a CAC-based scheme is presented to achieve realtime secure coding for digital video, and a secure coding chain is built based on CAC secure coder. Two kinds of secure coding operations, including context-based adaptive binary arithmetic secure coding (CABASC) and context-based adaptive variable length secure coding (CAVLSC), are given. The experimental results show that this scheme has significant improvement on security, real-time performance and flexibility of software implementation. These properties make it a sound foundation for further research on CAC secure coding.

Keywords secure coding, video encryption, context-based adaptive binary arithmetic secure coding(CABASC), context-based adaptive variable length secure coding(CAVLSC)

0 引 言

随着多媒体编码技术在数字电视广播、视频实时通信、网络流媒体传递以及多媒体短信等领域的广泛应用, 多媒体安全编码技术, 特别是数字视频安全编码技术正逐渐成为研究的热点。

1) 相关的工作分析

早期的数字视频安全编码方法是在编码后将视频数据直接应用密码技术 (如 DES(data encryption standard), IDEA (international data encryption algorithm)和 RSA(Rivest Ron, Shamir Adi and Adleman Leonard)等)对全部数据进行加密, 但从应用的角度看, 其加密过程将严重阻碍视频处理的实时性。近

基金项目: 国家自然科学基金项目 (60474035); 安徽省自然科学基金项目 (070412035)

收稿日期: 2008-06-23; **改回日期**: 2008-11-28

第一作者简介: 汪银苗 (1963—), 男。合肥工业大学在职硕士研究生, 安徽职业技术学院副教授。主要研究兴趣为多媒体加密。

E-mail: wymaher@163.com

年来,国内外研究者已提出了许多加密算法,并取得了丰硕的研究成果。根据压缩编码中加密位置和编码方式的不同,本文将其归类为压缩前加密、压缩域加密、熵编码加密和分层/可分级加密 4类。

其中压缩前加密是对信源数据先进行加密后,再压缩,使数据在存储和传输之前,实现加密过程与压缩过程的完全分离,其密钥随机性要求低。但一般观点认为,压缩前加密方法会显著地改变信源结构和句法,对后续编码效率影响很大。值得提及地是,国外学者 Johnson等人最近提出的对理想 Gaussian信源先加密后,再进行分布信源编码(DSC)压缩的方法[1],其不仅能够满足数据安全性要求,而且对压缩增益影响很小,而不足之处在于,对非理想 Gaussian信源先加密后再进行 DSC压缩,其编码效率降低明显。Schonberg等人提出了改进的加密数据盲压缩算法[2],但低密度奇偶校验码(LDPC)测试其码长增加了约 49%。

围绕压缩域加密展开的研究主要是基于信源特征,选择加密图像/视频重建中的关键数据,如离散余弦变换(DCT)系数、运动矢量、预测模式、头信息和编码参数等信息。目前,国内具有代表性的研究成果有清华大学袁春博士等人提出的基于混沌的视频流分层加密算法[3],上海交通大学王慈博士等人提出的参数可调型变换域 DCT系数透明加扰算法[4],合肥工业大学李援博士等人提出的图像信息与运动信息相结合的视频加密算法[5];国外有 Zeng等人提出的分别基于 Wavelet变换和 DCT变换的 Segment/Slice频域内 DCT系数加密方法[6],Ahn等人提出的帧内预测模式加扰方法[7],Spinsante等人提出的量化参数和环路滤波系数加密方法[8]。该类算法可以根据实际应用需求选择加密关键数据,一般支持多重安全级别,其缺点是加密强度与加密复杂度互相矛盾,而且加密过程在熵编码之前,对后续熵编码的编码效率影响较大。另外,编码的帧间相关性和错误隐藏也可能会泄露信息。

熵编码加密是将标准码表进行修改后使用,由于可将保密的码表内容和顺序作为解密的密钥,因而接收方无此特殊码表不能正确解码。该方法若能实现编码数据的位组合模式的出现概率与对应的标准码表字长度一致,则可保持原编码效率,但同时会使安全性降低,其另一缺点是密钥较长。目前具有代表性的研究成果为 Mao等人提出的码字序号加密算法[9],Wu等人提出的基于 Huffman编码的多 Huffman树(MHT)置乱方法和基于 Q和 M编码(QM coder)的多状态索引(MSI)置乱方法[10]。

基于精细可伸缩性(FGS)编码的分层/可分级加密是分别针对基本层(BL)和增强层(EL)进行加密,其目标是提供多质量的访问控制,以支持多类型用户的不同访问权限,其难点在于,当网络传输中出现丢包时,如何进行正确解码,即密钥的动态重构问题。一种简单的方法是仅加密 BL层数据,但安全性较差[11];SMLFE(scalable multlayer FGS encryption)算法[12]可以根据商业需求来分割 EL层中的峰值信噪比(PSNR)层和码率层,以便提供多质量的访问控制。其中,PSNR层是由 EL层视频对象平面(VOP)中多个相邻的位平面组成,而码率层则是由 EL层 VOP中多个视频包构成。

2) 本文工作

基于上下文的自适应编码(CAC)是一类新出现的用于视频压缩的高效熵编码方法,已应用于新一代视频压缩标准 H.264/AVC中,但据笔者所知,目前还没有开展专门针对其安全编码的研究。为此,本文的主要贡献是:提出了一种新的基于 CAC的数字视频安全编码方案,即首先建立以 CAC安全编码器为核心的安全编码链,然后分别针对基于上下文的自适应二进制算术编码(CABAC)和基于上下文的自适应变长编码(CAVLC),给出了 CABASC和 CAVLSC两种安全编码操作,最后将本文的加密效果与文献[5]和文献[7]算法进行了比较分析。对比实验结果表明,本文方案具有更高的安全性、较好的实时性和软件易实现性,可作为进一步研究 CAC安全编码的基础。

1 方案设计

用于数字视频的安全编码方案应建立在视频信源特征的基础之上。因为视频信源具有数据量大、实时在线处理能力要求高和单位比特信息价值低等特点,所以数字视频安全编码方案应具有以下优点:首先在保证安全性的条件下,算法应简单,易于实现,并具备实时的在线处理能力;其次应尽量减少对编码码长的影响;最后,加密数据还应完全保持视频格式的不变性和传输误码的鲁棒性。

本文提出的基于 CAC的数字视频安全编码方案旨在满足上述各种要求。如图 1所示,该方案以 CAC安全编码器为核心,建立了视频采集→图像压

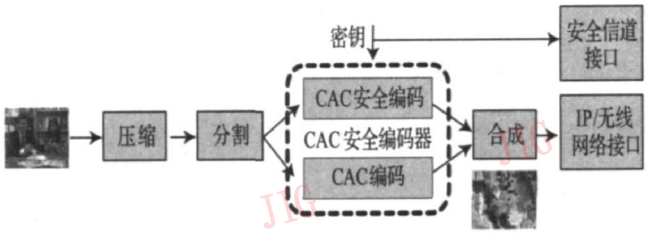

图 1　基于 CAC的数字视频安全编码方案

Fig. 1 CAC-based secure coding scheme for digital video

缩→分割→CAC安全编码器→合成→网络传输的安全编码链, 其安全解码链是安全编码链的逆过程。在具体实现中, 可先使用分割过程来提炼高效率的待加密关键数据, 如预测模式(PM)、变换量化系数(QTC)和运动矢量差(MVD)等; 然后使用混沌伪随机序列作为密钥来控制这些关键数据的 CAC安全编码过程; 对于其他非高效率的关键数据, 则采用常规的 CAC编码方法。

2　两种操作

为了阐述本文方案的合理性, 本文给出了 CABASC和 CAVLSC两种具体的安全编码操作。

2.1　CABASC操作

CABAC[13]是基于上下文的自适应二进制算术编码方法, 其主要用于对宏块层语法元素进行编码, 其编码步骤如下: 1)二进制化, 即将非二进制的语法元素转换成二进制比特序列, 其基本转换类型有一元编码、截断一元(TU)编码、Kth Exp-Golomb(EGk)编码和固定长度(FL)编码; 2)上下文建模, 即为已二进制化的语法元素比特序列的每一位提供概率模型, 并进行概率预测; 3)二进制算术编码, 包括规则编码器(regular coder)和旁路编码器(bypass coder), 其中前者使用了上下文建模。

基于 CABAC的编码过程, 一种最直观的安全编码方法是置乱所有的上下文模型。因为 CABAC采用了 399种上下文模型(纯帧或纯场编码时, 实际使用 277种), 每种模型都是针对某一位, 且有的位有多个模型可供选择, 所以明文置乱空间很大, 但由于置乱过程同时改变了相邻(左边和上面)块的已编码符号信息, 因此对编码效率影响较大, 另外, 加密流也不支持标准解码器回放, 即不兼容标准视频格式。因此本文主要针对步骤(1)和步骤(3)进行 CABASC操作(如图 2所示)。该操作包括 PM加扰以及 QTC和 MVD加密两个部分。

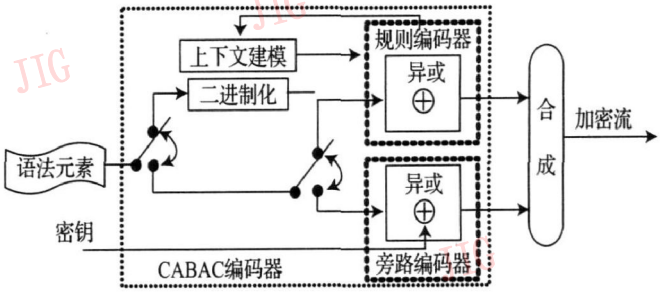

图 2　CABASC操作

Fig. 2　CABASC operation

1) PM加扰: 帧内预测时, 每个 4×4亮度块采用了两个独立的概率模型来进行 PM编码: 一个用于编码标记信息; 另一个使用 FL来编码 8种可能预测模式。对于后者概率模型, 本文使用了 3 bits伪随机序列对 FL编码中的 8种模式进行了随机加扰。

帧间预测时, 每个 16×16宏块可以分割成 16×16、16×8、8×16和 8×8 4种宏块类型(如图 3(a)所示); 而每个 8×8块还可以继续分割成 8×8、8×4、4×8和 4×4 4种子宏块类型(如图 3(b)所示)。从编码角度看, 这些分割方法大大提高了各种块模式的编码效率和块间关联性, 如 8×16块模式编码为“010”, 其符号概率 $P(8\times16)=P(C_0)\times P(C_1)\times P(C_3)$。但从加扰角度看, 由于每种块模式编码的唯一性以及需要与其对应的块编码模式(CBP)进行联合编码, 如果随机扰乱各种块模式则无法正确解码。为了兼容标准视频格式, 本文仅对运动补偿方式相同的块模式对进行了加扰, 如 16×8和 8×16, 8×4和 4×8等。

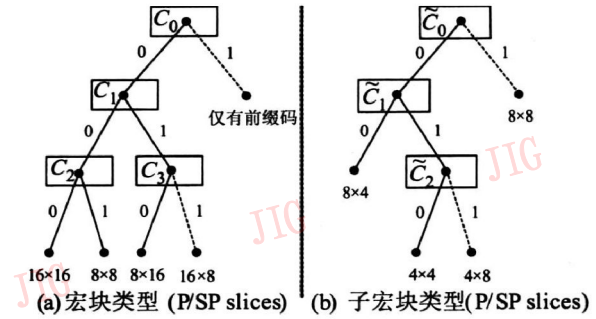

图 3　帧间预测模式二进制化

Fig. 3　Inter prediction mode binarization

2) QTC和 MVD加密　CABAC在对 QTC和 MVD进行编码时, 使用了相同的二进制化结构, 即 TU前缀码和 EGk后缀码。当对 |QTC|>1的系数进行编码时(|·|为绝对值), TU前缀码阈值 $S=$

14, EGk后缀码 $k=0$, 当对 |MV |进行编码时, $S=9$, $k=3$。由于 TU 的编码过程在规则编码器中进行, EGk的编码过程在旁路编码器中进行, 因此本文使用等长的伪随机序列分别在这两种编码器中对 TU 前缀码字和 EGk后缀码字的序号进行加密。另外, 考虑到变换量化后许多 QTC 系数值为 ±1, 且由于 CABAC仅对这些系数符号位进行编码, 并使用块编码标记和重要性图等指示其位置信息, 因此为了保障这些系数的安全, 本文使用了 1 bit伪随机序列对其符号位也进行了加密处理。

2.2 CAVLSC操作

在 CAVLSC操作中, 对 PM 和 MVD等关键数据使用指数哥伦布 (Exp-Golomb)进行编码, 其加密过程参考文献 [14]。CAVLC[15]是仅用于 QTC 系数的基于上下文的自适应变长编码方法, 它根据已编码句法元素的情况, 通过动态调整编码中使用的码表, 可以获得极高的编码效率, 其编码步骤如下:

1)对非零系数的总个数和拖尾系数的个数进行编码;

2)对每个拖尾系数的符号进行编码;

3)对除了拖尾系数之外的非零系数幅值进行编码;

4)对最后一个非零系数前为零的系数总个数进行编码;

5)对每个非零系数之前为零的系数个数进行编码.

对应于该编码过程, 本文提出了如图 4所示的 CAVLSC安全编码操作。同时注意到, 之所以没有对步骤 1)和步骤 4)中的系数总个数进行加密, 这是因为加密这些数据会改变块内 QTC 系数编码的控制信息, 从而会造成解码端解码错误。

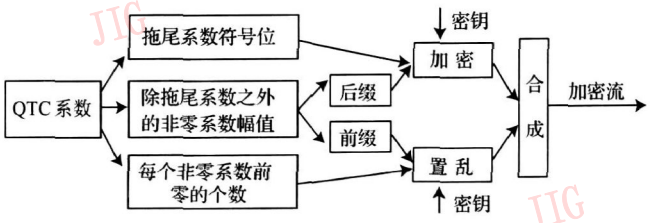

图 4 CABASC操作

Fig. 4 CABASC operation

QTC 系数经过 Zigzag扫描后, 高频位置上的非零系数值大部分是 ±1, 而 CAVLC 则使用拖尾系数来表示这些 ±1的个数, 其区间范围为 [0, 3]。因为步骤 2)中对每个拖尾系数进行编码时, 只需用 1 bit来表示其符号位 (0= +, 1= -), 所以使用不超过 3 bits伪随机序列就可以通过对一个 4×4块中的所有拖尾系数进行加密来获得加密符号流。步骤 3)中的系数幅值组成包括前缀和后缀: 当对前缀进行编码时, 先加密与码字对应的原始码表序号, 再将原始码表中与加密序号对应的码字作为编码输出; 当对后缀进行编码时, 则使用比特数与后缀码长相等的伪随机序列来进行加密。另外, 还通过置乱每个非零系数之前的零个数来增强图像纹理信息的安全性。

3 性能分析与实验

实验测试条件如下: H. 264/AVC标准, JM 82版本 (主要档次), 300帧, I帧间隔为 30, P帧: B帧 = 1: 1, Pentium Ⅳ 2. 60GHz处理器, 256MB RAM。

3.1 加密效果主客观分析

由于本文是在熵编码过程中对关键数据进行加密, 其加密位数与关键数据的码流长度相等, 因此 |明文加密空间 |大于等于 |密钥空间 |, 其中 |• | 为集合的势, 当且仅当“一次一密”时等号成立。考虑到本文方案使用了混沌伪随机序列作为加密密钥, 其密钥空间非常大, 因此只要保证每帧使用的密钥流位数不小于 128 bits, 即 |密钥空间 |大于等于 2^{128}, 就可以防止穷尽式密钥搜索攻击。另外, 由于混沌伪随机序列在每帧图像加密时是实时变化的, 因此使用已知明文攻击和选择明文攻击来进行解密也是极为困难的。以下主要从主、客观两个方面对加密效果进行评估。

1)主观视觉效果分析 选取 Foreman和 Football两个标准 CIF序列分别进行测试, 其加密效果如图 5所示。从图中可以看出, 文献 [7]算法的视觉安全性最差, 文献 [5]算法的视觉安全性则相对较好, 这是因为文献 [7]算法在预测编码过程中只对帧内预测模式进行了加扰, 而文献 [5]算法在此基础上又对 DCT变换域中的 QTC符号位和预测残差 MVD的大小进行了加密处理, 从而增强了纹理信息和前景运动信息的安全性。但与本文方案相比较, 本文方案在熵编码过程中给出的 CABASC操作和 CAVLSC操作的主观视觉安全性都相对更高, 如图 5 (c)和图 5 (d)所示, 其图像纹理信息和运动信息都异常混乱而根本无法辨别, 其原因是由于这两

种操作都与熵编码过程同步进行, 熵编码可进一步剔除图像的冗余信息, 因而所选关键数据的幅值更小、数据的加密效率更高、视觉影响更明显 (图中呈暗黑色)。

图 5　各种操作的加密效果图

Fig 5　Visual encryption effects using different operations

2)客观加密效果分析　对视频序列的加密效果可采用峰值信噪比 PSNR 作为客观评价标准。图 6显示了不同的加密操作对加密视频的 PSNR 值的影响。由图 6可见, 对于各种不同的视频序列, 其加密后视频的 PSNR 值 (Y、U 和 V 各分量 PSNR 的平均值)变化都呈现“文献[7]算法 < 文献[5]算法 < CABASC操作 < CAVLSC操作”的特点, 即本文给出的两种操作对视频序列 PSNR 值的影响明显较大, 显著地降低了图像质量, 且图像质量降低均超过 25dB。

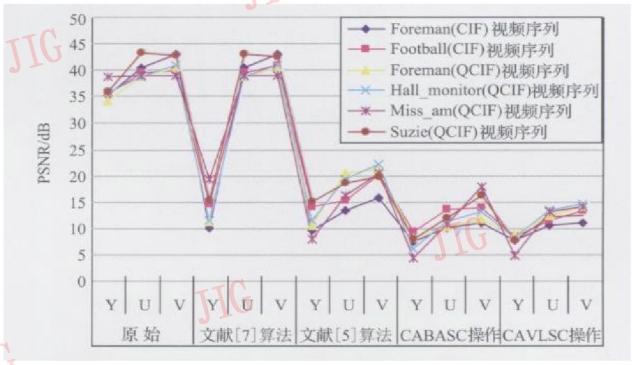

图 6　各种操作对 PSNR 的影响

Fig 6　PSNR influences using different operations

3.2　加密对平均码长的影响

本文还选用 9个标准 QCIF序列来测试两种操作对平均码长的影响, 其测试结果如图 7所示。

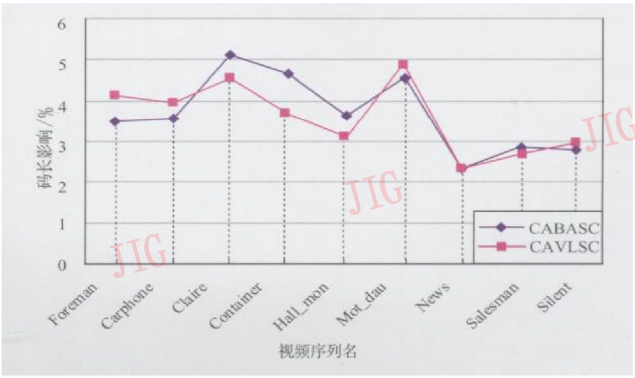

图 7　加密对平均码长的影响

Fig 7　Increased average code length after encryption

从对平均码长的影响来看, 两种操作对码长的改变都很小, 均控制在 5% 以内。其原因如下: 1)帧内 PM 和 QTC 符号位实际上使用的都是定长编码, 其加扰和加密过程不会改变码长, 另外, 通过使用等长伪随机序列加密 QTC 和 MVD 的后缀码, 其对码长也不会有影响; 2)帧间 PM 加扰对码长的影响非常有限 (如图 3所示), 每个宏块对 (如 8×4和 4×8)加扰至多增加或减少 1 bit码长, 而且这种过程是随机的, 即可能优化对码长的影响, 也可能使其变差; 3)码长变化主要来自于 QTC 和 MVD 前缀码的加密, 但由于通过熵编码能去除尽可能多的冗余信息和能加密尽可能高效的关键数据, 因此可以尽量降低对平均码长的影响。

3.3　加密对其他性能的影响

从视频处理的实时性来看, 图 8显示两种操作对不同视频序列进行编码, 其操作时间占编码过程总时间的比例都不超过 4.5%, 这表明操作复杂度

低、速度快,与熵编码过程相结合,即能够满足视频实时在线处理的需求。

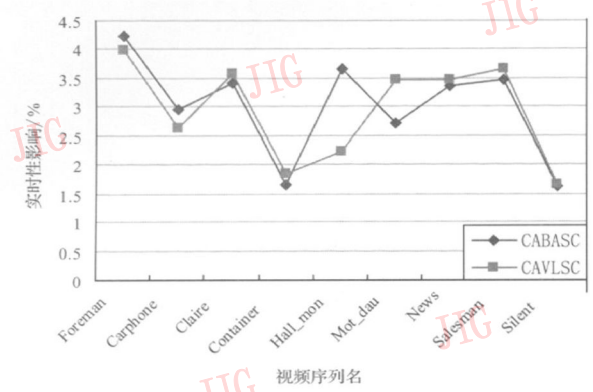

图 8 加密对实时性的影响

Fig. 8 Increased complexity after encryption

从码流的误码鲁棒性来看,由于加密操作没有改变视频中任何格式信息和控制信息,因此加密流兼容标准视频格式,也不影响码流的误码鲁棒性。又由于使用伪随机序列作为加密密钥,可以将码流控制精度保持在位一级,因此可使得网络传输中密文出错也不会带来错误的扩散,这进一步增强了码流的传输误码鲁棒性。

另外,整个加密过程主要进行的是异或、比较和判断等运算,因此操作简单,易于软件的实现。

4 结 论

针对用于视频压缩的一类高效熵编码方法——CAC,本文提出了一种新的基于 CAC的数字视频安全编码方案,并首先建立了以 CAC安全编码器为核心的安全编码链,其安全解码链是安全编码链的逆过程;然后分别针对 CABAC和 CAVLC两种熵编码的特点,给出了 CABASC和 CAVLSC两种安全编码操作;最后将本文加密效果与已有研究成果进行了比较分析。对比实验结果表明,本文方案具有更高的安全性、较好的实时性和软件易实现性,可作为进一步研究 CAC安全编码的基础。

本文使用了混沌伪随机序列作为加密密钥,但没有给出具体的密钥建立与管理方法,这应是下一步的工作重点;另一个可能的研究兴趣是基于 CAC的水印嵌入与提取工作。

参考文献 (References)

[1] Johnson M, Ishwar P, Prabhakaran V M, et al. On compressing encrypted data [J]. IEEE Transactions on Signal Processing, 2004, 52(10): 2992-3006.

[2] Schonberg D, Draper S C, Ramchandran K. On Blind Compression of Encrypted Data Approaching the Source Entropy Rate [EB/OL]. www.eecs.berkeley.edu/~dschonbe/pubs/eusipco2k5.pdf, 2005.

[3] Yuan Chun, Zhong Yu-zhuo, He Yu-wen. Chaos based encryption algorithm for compressed video [J]. Chinese Journal of Computers, 2004, 27(2): 257-263. [袁春,钟玉琢,贺玉文. 基于混沌的视频流选择加密算法[J]. 计算机学报, 2004, 27(2): 257-263.]

[4] Wang C, Yu Hong-bin, Zheng Meng. A DCT-based MPEG-2 transparent scrambling algorithm [J]. IEEE Transactions on Consumer Electronics, 2003, 49(4): 1208-1213.

[5] Li Yuan, Liang Lirwei, Su Zhao-pin, et al. A new video encryption algorithm for H.264 [C]//Proceedings of IEEE International Conference on Information, Communications, and Signal Processing. Bangkok, Thailand: IEEE Press, 2005: 1121-1124.

[6] Zeng W, Lei S. Efficient frequency domain selective scrambling of digital video [J]. IEEE Transactions on Multimedia, 2003, 5(1): 118-129.

[7] Ahn J, Shim H J, Jeon B, et al. Digital video scrambling method using intra prediction mode [C]//Proceedings of the 5th Pacific-Rim Conference on Multimedia. Tokyo, Japan, 2004: 386-393.

[8] Spinsante S, Chiaraluce F, Gambi E. Masking Video Information by Partial Encryption of H.264/AVC Coding Parameters [EB/OL]. www.epf.ch/ltsftp/EUSIPCO2005/defevent/papers/cr1338.pdf, 2005.

[9] Mao Y, Wu M. A joint signal processing and cryptographic approach to multimedia encryption [J]. IEEE Transactions on Image Processing, 2006, 15(7): 2061-2075.

[10] Wu C, Kuo C J. Design of integrated multimedia compression and encryption systems [J]. IEEE Transactions on Multimedia, 2005, 7(5): 828-839.

[11] Yuan C, Zhu B B, Wang Y, et al. Efficient and fully scalable encryption for MPEG-4 FGS [C]//Proceedings of the 2003 International Symposium on Circuits and Systems. Bangkok, Thailand, 2003: 620-623.

[12] Zhu B B, Yuan C, Wang Y, et al. Scalable protection for MPEG-4 fine granularity scalability [J]. IEEE Transactions on Multimedia, 2005, 7(2): 222-233.

[13] Marpe D, Schwarz H, Wiegand T. Context-based adaptive binary arithmetic coding in the H.264/AVC video compression standard [J]. IEEE Transactions on Circuits and Systems, 2003, 13(7): 620-636.

[14] Jiang Jian-guo, Bao Xian-yu, Li Hua-lei, et al. FVEA-H: A fast video encryption algorithm for H.264 [J]. Journal of System Simulation, 2008, 20(16): 4363-4367. [蒋建国,包先雨,李化雷,等. FVEA-H:一种用于 H.264的快速视频加密算法[J]. 系统仿真学报, 2008, 20(16): 4363-4367.]

[15] Chen T, Huang Y, Tsai C. Architecture design of context-based adaptive variable length coding of H.264/AVC [J]. IEEE Transactions on Circuits and Systems, 2006, 53(9): 832-836.