一种适合于 H.264 实时视频传输的新型加密方案

包先雨, 蒋建国, 李 援
(合肥工业大学计算机与信息学院, 安徽合肥 230009)

摘 要: H.264 是由 ITU-T 和 ISO/IEC 联合制定的最新视频编码标准, 其安全加密技术正成为研究的热点. 文章通过研究适合于 H.264 加密的侯选域, 提出了一种加密与压缩相结合的新型视频加密方案, 该方案包括崭新的 CAVLC (基于上下文的自适应变长编码) 与 QTC (量化变换系数) 加密同步, 预测模式置乱和运动矢量置乱. 理论分析和实验结果表明, 此方案速度快, 安全性高, 传输误码鲁棒性较强, 并对压缩比影响小.

关键词: H.264; CAVLC 与加密同步; 视频加密; 置乱
中图分类号: TN309.7 文献标识码: A 文章编号: 0372-2112 (2006) 11-2099-04

A New Encryption Scheme for H.264 Real-Time Video Transmission

BAO Xiao-yu, JIANG Jian-guo, LI Yuan
(*School of Computer & Information, Hefei University of Technology, Hefei, Anhui 230009, China*)

Abstract: H.264 is the latest video coding standard developed by ITU-T and ISO/IEC, and its security is becoming a research focus. Several candidate domains are investigated to apply encryption for H.264 and, a new video encryption scheme combining encryption with compression is proposed in this paper. It includes novel simultaneous CAVLC (Context-based Adaptive Variable-Length Coding) and QTC (quantized transform coefficients) encryption and prediction mode, motion vectors scrambling. Theoretical analysis and experimental results show that the scheme is fast, secure, and robust to transmission errors, moreover, it has very limited adverse impact on the compact ratio.

Key words: H.264; simultaneous CAVLC and encryption; video encryption; scrambling

1 引言

H.264[1]是由 ITU-T 和 ISO/IEC 联合制定的最新视频编码标准, 能提供比 H.263 和 MPEG-4 更高的压缩性能, 在图像重建质量相同时, 能够节省 30% ~ 50% 的码率. 其主要新特性是:

①帧内编码采用了帧内预测方法, 以减小 Intra 帧的空间冗余度.

②帧间预测支持 7 种可变块大小, 并且每块都包含明确数目的运动矢量, 提高了运动估计精度.

③熵编码使用了两种编码方法, 即 CAVLC 和 CABAC (基于上下文的自适应二进制算术编码), 极大地提高了编码效率.

新标准 H.264 优异的压缩性能必将使其在多媒体应用的各个领域发挥重要作用, 如视频点播, 视频监控和视频会议等, 因而其安全加密技术正成为研究的热点.

因为视频数据具有编码结构特殊、数据量大和实时性要求高等特点, 所以需要针对 H.264 的编码结构设计特殊的加密方案. 如图 1 所示, 适合于多媒体加密有两个最直接的区域[2]. 一是在压缩编码前加密多媒体流 (图 1 中①), 但这类方法通常会显著地改变多媒体信源结构和句法, 并降低了压缩性能. 值得提及的是, 文献[3]提出的先加密后压缩的视频加密策略, 不仅能够满足视频安全性要求, 而且对压缩增益的影响很小. 另一是在压缩编码后对码流进行加密 (图 1 中 ⑤和⑥), 这类方法的缺点是没有利用视频格式, 计算复杂度很高[8].

为此, 本文通过研究图 1 中其他可加密区域, 提出了一种基于 H.264 的新型视频加密方案.

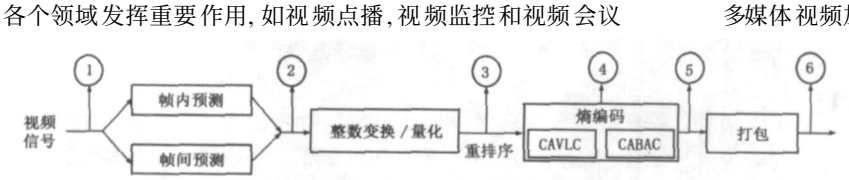


图 1 适合于 H.264 加密的侯选域

2 方案概述

多媒体视频加密在保证安全性的前提下, 首先应算法简单, 易于实现, 并具备适合于实时应用的低复杂度, 其次应尽量减小对压缩比的影响. 另外, 加密后的码流传输误码鲁棒性要强.

本文建议的加密方案 (如图 2) 就是要尽力满足上述要求. 在 H.264 编码器中, 帧内

收稿日期: 2005-11-22; 修回日期: 2006-07-10
基金项目: 国家自然科学基金 (No. 60474035); 安徽省"十五"二期科技攻关重大计划项目 (No. 04002038)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

编码采用了帧内预测(特性①),如 INTRA_4×4 块 9 种预测模式使用 3 比特就可以正确编码;帧间预测支持 7 种可变块大小(特性②),每块预测模式和块内运动矢量必须经过编码传输.因此,我们可以置乱帧内、帧间预测模式以及块内运动矢量.预测、变换、量化之后,每个 4×4 块的 QTC 使用 CAVLC 编码(特性③),因而我们可以在 CAVLC 中对 QTC 进行加密,实现编码与加密同步.此外,我们还使用了混沌序列发生器生成的混沌流密码控制这些置乱和加密过程.

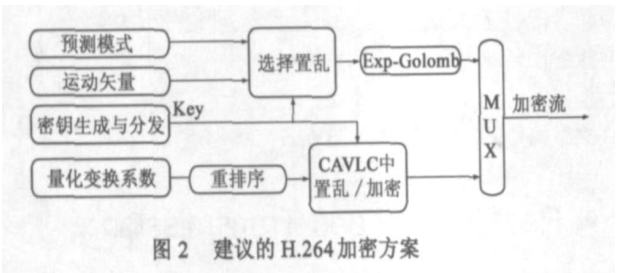


图 2 建议的 H.264 加密方案

3 建议的 H.264 加密方案

基于以上分析,建议的加密方案采用了适合于 H.264 加密的其他 3 个侯选域(图 1 中②,③,④).考虑到 H.264 特殊的编码结构,此方案包含 3 个部分:CAVLC 与 QTC 加密同步,预测模式置乱和运动矢量置乱.以上所有加密和置乱过程都由密钥生成与分发系统控制.

3.1 CAVLC 与 QTC 加密同步

文献[4]首次提出 CAVLC 编码方法.在 CAVLC 中,通过根据已编码句法元素的情况,动态调整编码中使用的码表,获得了极高的编码效率.其编码过程如下:

Step 1. 对非零系数的数目和拖尾系数的数目进行编码.

Step 2. 对每个拖尾系数的符号进行编码.

Step 3. 对除了拖尾系数之外的非零系数幅值进行编码.

Step 4. 对最后一个非零系数前零的数目进行编码.

Step 5. 对每个非零系数前零的数目进行编码.

对应于该编码过程,我们提出将 CAVLC 与 QTC 加密相结合,使得熵编码与加密同步进行,如图 3 所示.同时注意到,我们没有对 Step 1 和 Step 4 中类似系数头信息的数据进行加密.原因一是这些数据包含了很多对图像重建并不重要的标准信息;原因二是加密后会改变视频格式.

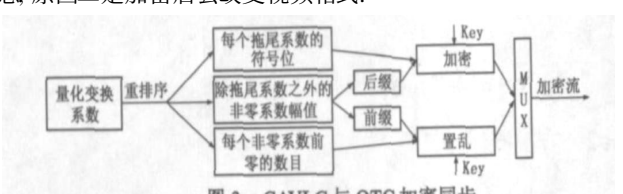


图 3 CAVLC 与 QTC 加密同步

QTC 经过 zigzag 扫描后,高频位置上的非零系数值大部分是±1,CAVLC 利用拖尾系数来表示这些±1 个数,其范围是从 0~3.因为 Step 2 中每个拖尾系数编码时只需 1 比特来表示其符号(0=+,1=-),所以至多使用 3 比特伪随机序列就可以对拖尾系数符号位进行加密,获得加密符号流.Step 3 中幅值组成分为前缀和后缀:前缀编码时,先使用 4 比特伪随机序列加密其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;后缀编码时,则使用比特数与后缀相同的伪随机序列对后缀进行加密.另外,我们还置乱了每个非零系数前零的数目,增强了纹理信息的安全性.

3.2 预测模式置乱

H.264 中的预测技术包括帧内预测和帧间预测.文献[5]提出的帧内预测模式置乱方法是简单且有效的,但其安全性主要取决于其使用的定长序列,在序列长度有限的条件下无法防止 Friedman 密钥猜解[6]和已知明文攻击.本文采用混沌伪随机序列分别对 INTRA_4×4 块和 INTRA_16×16 块预测模式进行置乱,不仅增强了对密码分析的抵抗性,而且扩大了密钥空间.

帧间预测支持 7 种可变块大小(16×16,16×8,8×16,8×8,8×4,4×8 和 4×4),而且每块都有明确数目的运动矢量.因此,对于一对具有相同数目运动矢量的块,如 16×8 和 8×16,8×4 和 4×8,我们可以根据生成的 1 比特伪随机序列奇偶性来置乱它们.

3.3 运动矢量置乱

每个帧间块都有明确数目的运动矢量,其范围从 0~16.为了使得置乱方法简单有效,我们仅对块中每个运动矢量不相等的两个分量(水平分量和垂直分量)进行了随机置乱.这种方法置乱前后码长相等,但改变了块内运动矢量在码流中的出现次序,而且变化规则由混沌序列发生器控制.

3.4 密钥生成与分发

混沌系统的主要特性是对初值极端敏感,即初值的微小变化可以生成完全不同的伪随机序列.在建议的方案中,混沌序列发生器采用了改进的二维 Baker map[7].系统初始化时,用户密钥用来生成混沌序列发生器的初值,初值一旦确定,就可以得到随机性能很好的伪随机序列.我们将此序列二值化,然后分别用于 QTC、预测模式和运动矢量的加密和置乱.

4 方案评价

4.1 安全性

本文建议的压缩与加密相结合的方案包括了崭新的 CAVLC 与 QTC 加密同步、预测模式置乱和运动矢量置乱.这样,整个视频系统完全被加密和置乱.方案安全性主要包含两个方面:加密视觉效果和加密安全性.

加密视觉效果:选取 Foreman、Mobile 和 Paris 三个标准视频序列进行测试,序列大小为 CIF(352×288).当加密流回放时,它们的背景纹理信息和前景运动信息都异常混乱,已经不可理解,如图 4 所示.可见,本方案视觉安全性较高.

加密安全性:帧内预测模式置乱改进了文献[5]中 INTRA_4×4 和 INTRA_16×16 置乱方法,可以防止 Friedman 密钥猜解和已知明文攻击.因此,I 帧的安全性得到增强.对于 P、B 帧,CIF 系列的运动矢量置乱空间为 $[2^{[352\times288/(16\times16)\times R]}=2^{396\times R}, 2^{[352\times288/(4\times4)]\times16\times R}=2^{101376\times R}]$,其中 $R=$(总运动矢量数目-水平垂直分量相等的运动矢量数目)/总运动矢量数目,因此采用穷举攻击来解密是极为困难的;帧间预测模式置乱可以进一步改变块内运动矢量在码流中的出现次序,增强运动内容的安全性.另外,CAVLC 与 QTC 加密同步是很有前途的研究方向,该方法在熵编码过程中同时进行加密,安全性

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

很高.

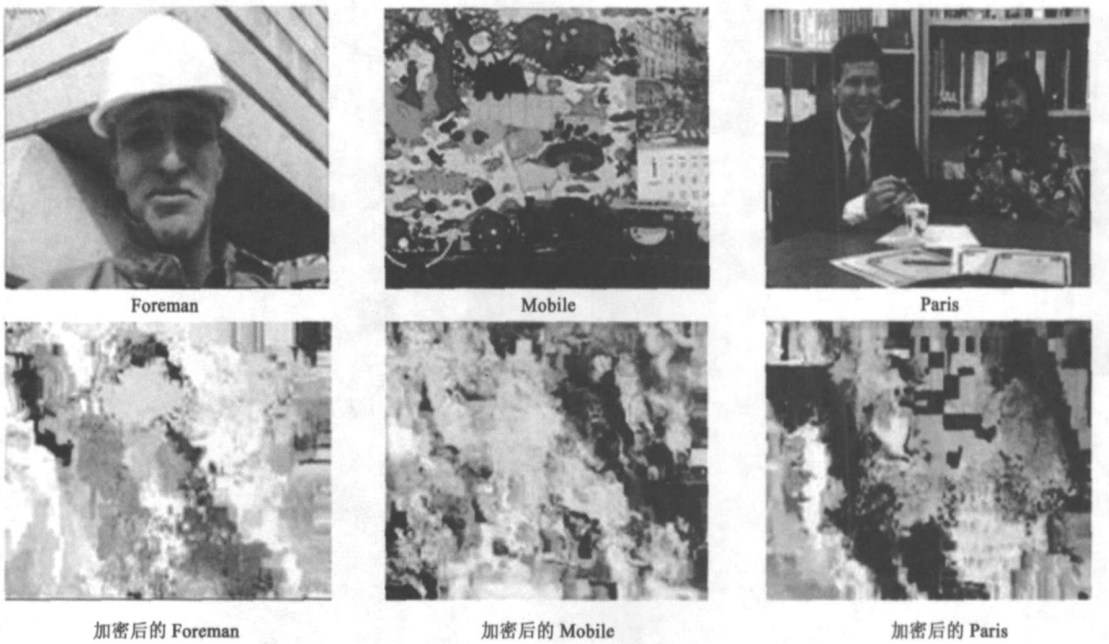


图 4　加密测试效果图

4.2　计算复度杂

现有视频加密算法存在的主要问题是加密复杂度高, 影响视频实时性. 本文将加密过程与压缩过程相结合, 极大地减小了加密处理延时. 例如 CAVLC 与 QTC 加密同步是在 CAVLC 中进行加密, 对复杂度影响很小; 预测模式置乱使用了简单的异或和判断操作, 几乎不影响复杂度; 随机置乱每个运动矢量不相等的两个分量, 显然不会增加复杂度. 因此, 本文方案适合于 H. 264 的实时安全实现.

4.3　压缩比

从整个加密过程可以看出, 本文方案对 CAVLC 编码几乎没有影响: 预测模式和运动矢量置乱前后码长相等, 不影响压缩比; 在 CAVLC 中, 拖尾系数和系数后缀加密前后码长不变, 但加密前缀对应的原始码表中序号时, 轻微地改变了信源统计特性, 降低了压缩比. 选取三个 CIF 序列进行测试, 其结果如表 1 所示.

表 1　加密前后压缩比比较

视频序列 (I P B)	加密前压缩比	加密后压缩比
Foreman(12 89 98)	78.61	76.83
Mobile(13 87 99)	25.52	24.31
Paris(10 90 99)	64.16	60.93

4.4　传输误码鲁棒性

因为加密过程没有改变视频中任何格式信息和控制信息, 加密流兼容标准视频格式, 所以不影响 H. 264 的传输误码鲁棒性. 又由于使用流密码加密, 可以将码流控制精度保持在位一级, 使得网络传输中密文出错不会带来错误的扩散, 进一步增强了传输误码鲁棒性.

5　结论和未来工作

本文通过研究适合于 H. 264 加密的后选域, 提出了一种加密与压缩相结合的新型视频加密方案. 该方案的特点是: (1) 首次将 CAVLC 与 QTC 加密相结合, 使得熵编码与加密同步进行; (2) 改进了文献[5] 中帧内预测模式置乱方法, 可以防止 Friedman 密钥猜解和已知明文攻击; (3) 帧间预测模式置乱改变了块内运动矢量在码流中的出现次序, 使得其置乱结果与运动矢量置乱结果能够相互保护, 增强了运动内容的安全性.

H. 264 建议了两种类型的熵编码方法: CAVLC 和 CABAC. 如何实现 CABAC 编码过程与加密过程相结合是我们下一步的工作重点.

参考文献:

[1] ITU-T Rec. H. 264 ISO/IEC 14496-10: 2005(E). Advanced Video Coding for Generic Audiovisual Services[S].

[2] Yinian Mao, Min Wu. A joint signal Processign and cryptographic approach to multimedia encryption[J]. IEEE Transactions On Image Processing, 2006, 99: 1- 15.

[3] M Johnson, P Ishwar, V M Prabakaran, D Schonberg, K Ramchandran. On compressing encrypted data[J]. IEEE Transactions on Signal Processing, 2004, 52(10): 2992- 3006.

[4] Bjontegaard, Lillevold. Context-adaptive VLC(CAVLC) Coding of Coefficients[S]. JVT Document JVT-C028, Fairfax, Virginia, 2002.

[5] J Ahn, H J Shim, B Jeson, I Choi. Digital video scrambling method using intra prediction mode[A]. Pacific Rim Conference on Multimedia[C]. Tokyo, Japan, 2004. 386- 393.

[6] W F Friedman. The Index of Coincidence and Its Applications in Cryptography[M]. Riverbank Publication No 22, River bank Labs 1920, Repainted by Aegean Park Press, 1987.

[7] J Fridrich. Image encrytion based on chaotic maps[A]. IEEE International Conference on Systems, Man, and Cybernetics[C]. Orlando: IEEE,

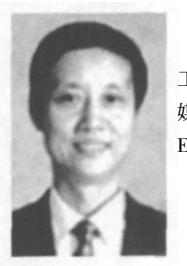
© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

1997. 2. 1105- 1110.

[8] Dahua Xie, C J Kuo. Enhanced multiple huffman table(MHT) encryption scheme using key hopping[A]. Proceedings of the 2004 International Symposium on Circuits and Systems[C]. Vancouver, Canada: IEEE, 2004. 5. 568- 571.

作者简介:

包先雨 男, 1981 年出生于安徽桐城, 现为合肥工业大学计算机与信息学院博士研究生, 主要研究方向为多媒体安全、视频压缩编码等.
E-mail: baoxianyu@ 163. com



蒋建国 男, 1955 年出生于安徽黄山, 合肥工业大学教授, 博士生导师, 主要研究方向为多媒体信息处理、DSP 技术与应用等.
E-mail: jjg@ ah165. net

李 援 男, 现为合肥工业大学计算机与信息学院博士研究生, 主要研究方向为计算机网络安全等.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net