H.264 视频加密算法的研究及改进

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

摘 要: 本文提出将帧内、帧间预测模式置乱, 量化系数与运动矢量加密相结合的 H.264 视频加密方法, 试验表明此方法具有良好的加密效果, 其算法复杂度低, 对编码效率影响小, 适合实时应用; 在此基础上我们进一步提出了一套完整的视频加密系统, 通过将二层序列密钥同步与告知机制相结合的方法实现了快速序列密钥同步, 多用户访问控制, 并扩大了序列密钥的产生空间, 增加了系统的安全性.

关键词: 视频加密; 置乱; 混沌随机序列
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2007) 09-1724-04

Research and Improvement of the Video Encryption Algorithm for H.264

JIANG Jian-guo, LI Yuan, LIANG Li-wei
(Hefei University of Technology, Hefei, Anhui 230009, China)

Abstract: A new video encryption method which utilized Intra, Inter prediction mode scrambling, transform results and motion vector encryption is proposed in this paper based on the formers' research work. Test showed that this method exhibits nice security; moreover its computational complexity is rather low, has little impact on encoding efficiency and can be realized in real time environment. A video encryption system based on the algorithm is also put up, the fast synchronize of the streaming key and multiple user access is achieved by two-level synchronization and telling mechanism.

Key words: video encryption; scrambling; chaos pseudo sequence

1 引言

随着多媒体技术和计算机网络的发展, 图形、图像、音频和视频等多媒体信息得到了日趋广泛的应用, 如: 视频点播、视频会议、监控系统等, 而这对视频数据的产权保护和安全传输提出了相应的要求, 视频信息的网络安全已成为当前亟待解决的问题. 早期的安全方法主要依赖于对访问者的身份认证, 而视频本身并未经过加密, 因此存在传输过程中易被窃取、解码、播放的问题. 针对这种情况, 特别是对关系军事、政治、经济等敏感视频信息的保护, 有必要对视频数据加密方法进行研究.

视频数据信息量大, 具有特殊的编码结构, 且其实时性要求强. 这些特点对现有的加密系统提出了新的要求, 即: 被加密的视频在保证其安全性的同时, 须保持码流结构不变, 减小对于编码效率的影响, 保证应用的实时性以及对网络传输错误的健壮性强等.

2 前人工作

视频保密的研究工作始于 90 年代中期, 当时使用的是传统加密方案, 但应用中发现其难以满足视频加密的各项需求. 此后通过对视频编码结构的研究, 人们认为应当选择对视频信息重建具有重大意义的部分进行加密, 即选择性加密. 而人们对视频中关键信息的认识也是在不断发展的: 从仅加密 *I* 帧, 到发现 P、B 帧中 *I* 块对于视频安全的重要性[1], 进而提出对 *I* 帧加密同时应对 P、B 帧中的 *I* 块进行加密, 但这也使加密的时间复杂度增加到全加密的 70~80%. 于是出现了其他的选择性加密方法: Adnan 等提出仅加密视频流中第 n 个 *I* 块和第 n 个预测宏块头部信息的方法[3]; Tang、Tosum 等人进一步提出了将 DCT 变换系数置乱加密的方法[2,4]; 文献[5]中则提出了对 DCT 系数符号进行加密的思想. 2004 年, Zheng Liu 等提出一种在无图形信息的前提下, 仅使用运动矢量进行视频图像恢复, 对视频中重要对象识别的方法, 这进一步将对运动矢量的加密提到重要的位置上[6]. 因此, 一般认为, 视频中 DCT 变换系数和运动预测得到的运动矢量是视频加密的关键.

近年来, 人们在流密码对于视频数据中变长块的加密方面进行了大量的研究, 基于混沌映射生成伪序列的加密方法是其中典型的代表, 其加密算法安全性好、复杂度低, 执行效率高, 但是对于密码系统的同步、用户管理方面却很少涉及, 本文在总结前人工作的基础上, 以新的视频编码标准: H.264 为目标, 改进其加密方法并以此为基础提出了一套视频安全系统, 解决了视频加密, 密钥序列同步, 多用户访问管理的问题. 文章主要分为以下几个章节: 第 3 章介绍改进的 H.264 视频加密算法; 第 4 章讨论视频安全系统, 包括: 密钥序列同步策略

收稿日期: 2006-04-03; 修回日期: 2007-02-09
基金项目: 国家自然科学基金(No. 60474035); 国家教育部博士点基金(No. 20060359004)

和用户管理方案; 第5 章分析了本文加密算法的性能及系统的安全性; 最后, 小结本文, 提出今后进一步的研究目标.

3　改进的 H. 264 视频加密算法

3. 1　H. 264 视频加密标准

H. 264 是由 ISO 和 ITU 联合专家组(JVT) 提出的新一代视频编码国际标准. 在原有的视频压缩算法的基础上, H. 264 提供比 H. 263 和 MPEG4 更高的压缩性能: 在同等视频重建质量情况下使码率降低 30-50% . 其基本编、解码框架(如图 1) 仍采用基于块的运动补偿和变换编码的混合编码架构, 在继承许多优秀编码技术的同时 H. 264 也采用了很多全新的编码方法, 如: 帧内预测, 可变大小的图像分块, 多预测参考帧, 1/ 4 和 1/ 8 像素精度运动估计, 残差图像的整数变换编码等. H. 264 标准的优良性能决定了其广泛的应用范围, 因此, 对 H. 264 视频加密方法的研究是非常有意义的.

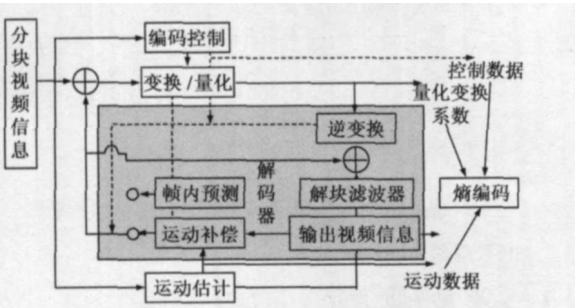

图 1　H.264/AVC 编码和解码结构框图

3. 2　H. 264 视频加密算法

3. 2. 1　已有算法

文献[7] 提出了一种 H. 264 视频的加密方案, 其中使用了帧内预测模式置乱的方法来进行视频加密: 通过将 I 帧中 4 × 4 和 16 × 16 尺寸编码块的帧内预测模式进行置乱, 在不改变编码方式及码率的前提下对视频数据提供了一定程度的保护. 这种方案在算法执行效率和视频压缩率保持上无疑是很好的, 但是从算法分析、加密后视频性质及结果图可知该方法对于视频信息提供的保护相当有限: (1) 为了保证置换后编码的长度不变, 文献[7] 中算法使用定长伪随机序列进行帧内预测模式置乱, 其置乱空间为: 在 4 × 4 分块的方式下, 除使用 1 个比特表示使用了最可能的预测模式外, 每个 4 × 4 块有 2^3 种可能预测模式, 而 16 × 16 块则只有 2 种可能. 根据 H. 264 编码规范和实验统计可知: 在 QP 为 30 的情况下, 视频中约 50% 的 4 × 4 块会使用 3 比特方式编码, 而在 QP 为 48 的情况下仅有 20% . 按照一 CIF 帧完全由 4 × 4 块组成来计算, 暴力破解空间仅为: $[352 \times 288/(4 \times 4)/2]^8 < 2^{32}$. (2) 其次, 在伪随机序列较短的情况下, 可以提取置乱块中的加密部分, 使用 Friedman 攻击[8] 确定密钥长度后猜解密钥, 从而完成攻击. (3) 未对敏感的运动矢量数据提供任何保护. 对此, 我们在详细研究了 H. 264 视频标准的结构特点的基础上, 对上述方法进行改进, 提出一种新的 H. 264 视频加密算法.

3. 2. 2　改进的 H. 264 视频加密算法

(1) 改进的帧内预测模式置乱方法: 原算法中使用定长伪随机序列进行帧内预测模式置乱, 在序列长度有限的条件下无法抵抗密码分析的攻击; 因此, 使用混沌序列发生器产生无重复的伪随机值对帧内预测模式进行置乱, 以增强对密码分析的抵抗性.

(2) 帧间预测编码模式置乱: 由于帧间运动预测 7 种块划分模式中 4 × 8 和 8 × 4 块得到的运动矢量数目相同, 对它们进行置乱不会影响视频编码, 因此, 随机置乱这两种模式的编码, 方法如下:

```
产生一伪随机值
if( 随机值 mod 2= = 1) then
    置乱 4 × 8 和 8 × 4 块模式
else 保持原块模式不变
```

(3) 由于H. 264 中整数变换量化后结果为有符号整数, 可以使用混沌序列对块中变换、量化的块中非零系数进行加密. 同时, 为减少对码率的影响, 我们将量化系数划分{ 0~ 15} , { 16~ 31} , { 32~ 63} , { > 64} 几个区间, 在各区间使用不同位数的随机序列进行加密. 具体方法如下:

```
if( 量化系数 ≠0) then {
  产生一伪随机值
  if( 随机值 mod 2= = 1) then{
    if( 0= abs( 量化系数) < 15) then
      加密量化系数= 量化系数 ⊕( 密钥 mod 8)
    if( 16= abs( 量化系数) < 32) then
      加密量化系数= 量化系数 ⊕( 密钥 mod 16)
    else if( 32= abs( 量化系数) < 64) then
      加密量化系数= 量化系数 ⊕( 密钥 mod 32)
    else
      保持原量化系数不变
  }
  else 加密量化系数= 量化系数 × ( - 1)
}
```

(4) 视频中大、小运动矢量的边界是进行运动矢量图形恢复重要依据[6], 为防止通过运动矢量对图形的重建, 定义 $F_1(x)$ 和 $F_2(x)$ 为区间{ 4~ 15} 和{ 20~ 31} 上的受随机值控制的两个置换, 将 P、B 帧中由预测得到的运动矢量用如下方式进行加密:

```
产生一伪随机值
if( abs( 运动矢量) < 4) {
```

加密的运动矢量= 运动矢量 ⊕(随机值 mod4)

}

else if(4 ≤abs(运动矢量) < 15){

if(随机值 mod2= = 1) then{

加密的运动矢量= F_1(运动矢量)

}

else if(20= abs(运动矢量) < 31){

if(随机值 mod2= = 1)then

加密的运动矢量= F_2(运动矢量)

}

else 保持原运动矢量

测试中使用线性置换函数 $F_1(x) = 35 - x$, $F_2(x) = x - 16$. 这样, 不同大小的运动矢量被随机混迭, 为对抵抗基于运动矢量的图像恢复技术提供了有效的保证. 同时, 置换区间内的运动矢量二进制位数值大致相当, 控制了对编码效率的影响.

(5) 由于人眼对亮度信息较色度信息更加敏感, 为减小加密操作带来的性能损失, 对视频中的色度信息只进行了简单的随机符号置反.

4 基于 H.264 的视频加密系统

流密码加密必须对加、解密双方的密钥序列同步的基础上才能正确工作, 因此, 多用户访问加密视频时各用户对同一视频序列必须进行密钥同步, 对此提出两层的密钥序列同步方法和基于告知机制的视频加密系统.

4.1 密钥序列发生器

文献[9]对流密码系统的同步进行了研究并提出了基于图组的流密钥同步策略, 其每个图组的计算初值是在上一图组计算初值基础上增加固定增量, 这样, 若序列中任何一个图组的初始计算密钥被攻破, 那么整个加密序列将被完全解密. 因此本文提出下面的两层加密系统(如图 2, 上层利用散列函数计算为每一个图组加密产生初始密钥, 下层混沌序列发生器计算图组中每帧加密需要的密钥序列, 这样, 即使视频中一图组的初始密钥被破解, 攻击者也只能得到此后序列的图像. 同时, 由于加密视频是按照图组进行同步的, 当网络传输时出现丢帧, 丢包时, 对下一图组的正常解密不会产生任何影响.

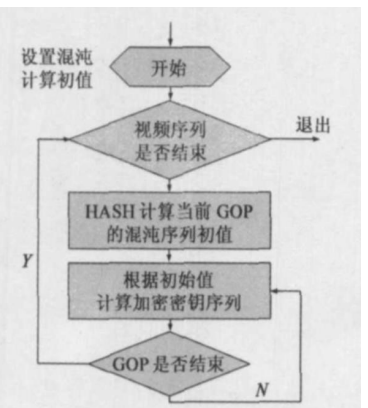

图 2 两层的混沌密钥序列产生器

4.2 视频加密系统

多用户共享的视频加密系统存在新接入用户时的流密钥同步问题, 新接入用户为了同步视频流中的密钥而必须进行繁重的混沌迭代计算, 这显然不利于视频加密系统的应用. 因此设计图 3 所示的视频加密系统: 客户在向视频服务器认证后建立会话密钥和本轮会话标识; 此后客户请求视频时, 视频服务器首先将与下一图组对应的密钥初始值用会话密钥加密传输给客户, 客户再利用此值进行密钥序列发生器的初始化, 当客户接收到新的图组后就可以对接收到的视频进行正确的解密、解码、回放. 这样通过视频服务器"告知"的方式实现了客户的快速流密码同步工作, 显著减少了客户计算量; 此外, 由于传输的同步信息使用密钥加密, 保证了系统的安全性.

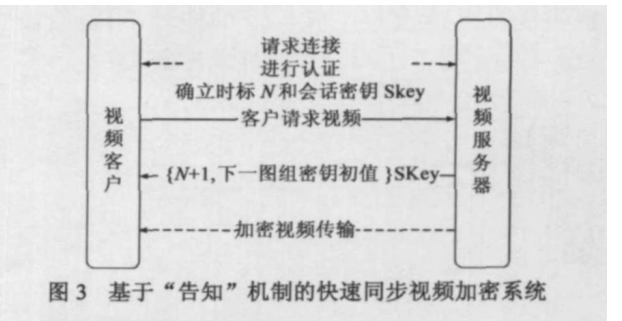

图 3 基于"告知"机制的快速同步视频加密系统

5 加密系统的性能分析

5.1 计算复杂度

对于 *I* 帧: 算法中仅需要处理两种数据: 亮度分量整数变换结果中不为零的部分和帧内预测模式的置乱. 按照 QP= 30 时全部使用 4×4 块进行编码, 有 50% 左右的块可以进行预测模式置乱, 需要处理的数据量小于(3/2) × $W \times H \times 16/(4 \times 4)$, 其中 W 和 H 分别为视频的宽度和高度. 同样, 对 P、B 帧中运动矢量加密需要处理的运动矢量数目则小于 $W \times H/(4 \times 4)$. 由于实际进行视频编码过程中不可能仅使用 4×4 块进行编码, 因此对于 cif 大小的视频, 其 I 帧加密需要进行的混沌迭代次数在 10^5 左右, 而对于 B, P 帧则小于 6×10^3; 同时, 由于算法中仅使用比较、异或, 符号置反等操作, 因此, 加密运算复杂度很低, 适合实时实现; 这也可以从表 1 中执行加密和不执行加密时的编码效率以及每帧数据处理百分数看出.

5.2 系统安全性分析

从加密的效果图(图 4~ 6)中可知, 原始图像经加密后已难以确认. 另外, 从密码分析来看, 对帧内和帧间预测模式的置乱使用混沌随机序列而不是定长随机序列, 大大加强了加密视频的安全性. 对于 CIF 图像, 每个 *I* 帧图像使用的密钥序列长度大于 10^5 位, 对含运动矢量的 B、P 帧密钥序列长度也有 6×10^3 位, 这样, 对单

个 I 帧, 还是 B、P 帧的穷举攻击都是不可能实现的. 即使攻击者已知视频明文但图组密钥序列发生器的初始密钥是一个随机值, 这样, 每次加密使用的流密钥都是一随机序列, 因此, 本方法可以抵抗已知明文攻击和选择明文攻击. 混沌加密系统的安全性与数据计算精度密切相关, 也既是混沌序列发生器的循环窗问题, 由前人的研究, 可用的平均混沌迭代次数为 $N(p) \approx 1.8 \times 10^{0.142p}$ [10], 其中 p 是二进制精度的位数, 在本系统中我们使用双精度数据进行混沌迭代, $p = 64$, 则 $N(p)$ 约为 2.2×10^{9}, 可见本文算法的迭代次数远小于混沌序列循环的限定值.

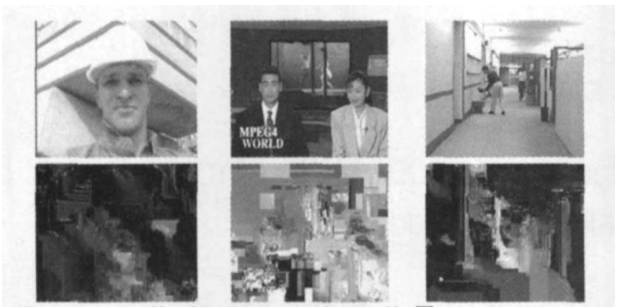

图 4　foreman 第 1 帧　图 5　news 第 198 帧　图 6　hall_mornitor 第 100 帧

5.3　对编码效率的影响

从加密过程可以看出本文的算法对后续熵编码过程基本无任何影响, 因此, 本方法对视频压缩率的影响较小; 从表 1 中测试结果也可以看出, 对不同运动状况视频序列本文的加密算法都有良好的加密效果. 另外, 由于加密中使用流密码加密, 因此码流对传输过程中的传输错误具有较好的健壮性.

表 1　加密前后视频序列大小

(200 帧, I 帧间隔 25, P 帧: B 帧 = 1∶1, 测试平台为 P4 2.2GHz 512MB 内存)

视频序列	文件大小(Byte)		对码率的	每帧数据	编码效率(fps)	
	加密前	加密后	影响(%)	处理(%)	未加密	加密
Foreman	100,933	105,622	4.65	22.91	42.96	41.56
News	73,971	76,590	3.54	26.13	50.00	49.42
hall_monitor	54,298	55,728	2.63	19.07	50.20	50.00

6　结论

本文提出了一种基于 H. 264 视频编码标准的加密算法, 通过算法分析, 实验测试及安全性分析证明此算法复杂度低, 具有良好的安全性和实时性; 同时本文对流密码系统中密钥同步、多用户访问控制进行了研究, 提出两层流密钥序列发生器和基于"告知"机制的快速流密钥同步方法, 既保护了视频的安全性也实现了多用户的快速视频访问, 为 H. 264 在安全应用提供了的基础.

参考文献:

[1] Agil Gong L. An empirical study of MPEG video transmissions [A]. Proceedings of the Internet Society Symposium on Network and Distributed System Security [C]. San Diego, CA: PISSNDSS, 1996. 137- 144.

[2] Tang L. Methods for encrypting and decrypting MPEG video data efficiently [A]. Proceedings of the Fourth ACM International Multimedia Conference [C]. Boston, MA: Proceedings of the Fourth ACM IMC, 1996. 219- 230.

[3] Adnan A, Ghassan A R, et al. Improved selective encryption techniques for security transmission of MPEG video bit-streams [A]. Proceedings of 6th IEEE International Conference on Image Processing [C]. Kobe, Japan: IEEE, 1999. 256- 260.

[4] Tosum A S, Feng W C. Efficient multi-layer coding and encryption of MPEG video streams [A]. IEEE International Conference on Multimedia and Expo [C]. New York: IEEE, 2000. 119- 122.

[5] Shi Changui, Bhargava Bharat. A fast MPEG video encryption algorithm [A]. Proceedings of the 6th ACM International Multimedia Conference [C]. Bristol, UK: Proceedings of the 6th ACM IMC, 1998. 81- 88.

[6] Zheng Liu, Xue Li. Motion vector encryption in multimedia streaming [A]. Proceedings of the 10th International Multimedia Modeling Conference [C]. Washington USA: P of the 10th IMMC, 2004. 1- 8.

[7] Jinhaeng Ahn, Hiuk Jae Shim, et al. Digital video scrambling method using intra prediction mode [A]. Pacific Rim Conference on Multimedia [C]. Tokyo, Japan: PRCM, 2004. 386- 393.

[8] W F Friedman. The Index of Coincidence and Its Applications in Cryptography [M]. USA: Riverbank Publication, Repainted by Aegean Park Press, 1987.

[9] Yuan Chun, Yu Zhuo Zhong, et al. Selective video stream encryption algorithm based on chaos [J]. Chinese Journal of Computers, 2004, 27(2): 257- 263.

[10] Robert Matthews. On the derivation of a "chaotic" encryption algorithm [J]. Cryptologia, 1989, 8(1): 29- 41.

[11] Shiguo Lian, Zhiquan Wang, Jinsheng Sun. A fast video encryption scheme suitable for network applications [A]. IEEE International Conference on Communication, Circuits and Systems [C]. Chengdu, China: IEEE, 2004. 566- 570.

作者简介:

蒋建国　男, 教授、博士生导师, 合肥工业大学计算机与信息学院. 主要研究方向: 多媒体智能监控系统、基于多 Agent 的分布式智能控制系统、DSP 技术应用, E-mail: jgjiang@hfut.edu.cn