基于 H.264 的混沌视频加密系统①

金成杨，王光义

(杭州电子科技大学 CAD 研究所，杭州 310018)

摘 要：为了解决视频信息的安全问题，提出了一种基于视频编码标准 H.264/AVC 的混沌视频加密算法。利用流密码加密简单、运算速度快等优点，采用 Logistic 离散混沌序列对 H.264/AVC 标准的 CAVLC（基于上下文的自适应变长编码）熵编码阶段的码流进行加密，并从算法的安全性、加密效率等方面进行分析。试验结果表明：该加密算法在保证视频内容信息安全性的前提下，不改变码流的结构，具有良好的实时性和快速性。

关键词：视频加密；Logistic；混沌序列；H.264/AVC 编码标准；CAVLC 熵编码

Chaos Encryption System for Video Based on H.264

JIN Cheng-Yang, WANG Guang-Yi

(School of Electronics Information, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: In order to solve the problem of security of video information, a chaotic video encryption algorithm based on H.264/AVC video coding standard is proposed. Because Stream cipher is simple, fast, etc., The proposed scheme uses discrete chaotic sequence of Logistic to encrypt the stream of CAVLC (Context-based Adaptive Variable Length Coding) entropy coding stage of H.264/AVC, and analyses the security and encryption efficiency of the algorithm. The results showed that the video encryption algorithm ensures the security of information, does not change the structure of the stream and the system has a good real-time and fast speed.

Keywords: video encryption; logistic; chaotic sequence; H.264/AVC coding standard; CAVLC entropy coding

1 引言

在当今这个信息爆炸的年代，计算机网络和多媒体技术得到了飞速的发展，视频会议、数字存储媒体、网络流媒体等各种视频信息已经广泛应用于社会各行业中。伴随着多媒体的应用，人们对多媒体加密的需求也越来越大，而其中视频的加密技术逐渐成为人们关注的焦点和急需研究的问题。视频加密算法除了要有较高的安全性外，还必须具有较快的加密速度和保持压缩效率与编码格式不变。

近年来，人们已经提出多种视频加密技术：1)完全加密算法，不考虑视频编码格式，将视频数据看作普通的二进制数据加密，常见的有 VEA 算法[1]、CSC 算法[2]，这类算法虽然安全性高并且不改变压缩比，但是计算复杂度很高[3]。2)部分加密算法，选择较敏感的部分加密，常见的有分层加密算法和基于帧结构的选择性加密算法，这类算法的计算复杂度仍然比较高。3)DCT 系数加密算法，采取对 DCT 数据置乱的方法[4]，常见的有 DCW 算法、DCF[5]算法，这类算法复杂度低，但是安全性低并且改变了压缩比。4)熵编码过程加密算法，常见的有 MHT 算法、MSI 算法，这类算法计算复杂度低，对压缩比改变很小，但是安全性一般。这些方法各有优缺点，针对应用的场合不同，选择合适的算法。

基于 H.264 的加密技术有良好的应用前景，可应用于视频会议、安防监控、数字存储媒体等领域；以及针对目前对 H.264/AVC 加密算法的研究不足，本文提出一种基于 H.264/AVC 的 CAVLC 熵编码过程的视频加密算法。

① 基金项目:国家自然科学基金(60971046)

收稿时间:2010-09-26;收到修改稿时间:2010-11-09

2　H.264/AVC加密算法

2.1 H.264/AVC 标准

H.264 是由 ITU-T 视频编码专家组(VCEG)和 ISO/IEC 运动图像专家组(MPEG)联合开发，于 2003 年 3 月正式被 ITU-T 所通过并在国际上正式颁布的新一代视频压缩编码标准[6]。新的标准与 H.263，MPEG-4 相比，视频压缩比提高了一倍，并且具有良好的网络亲和性，即可适用于各种传输网络。

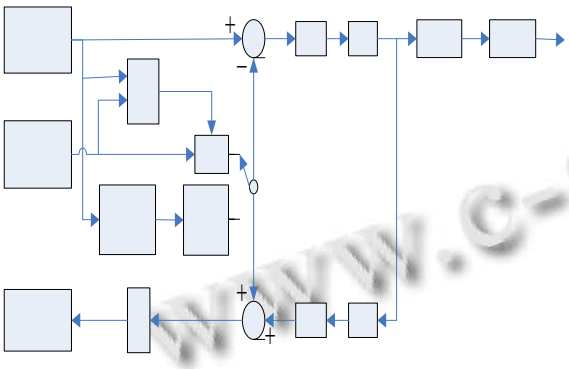


图 1　H.264 编码器

H.264 编码器的功能组成如图 1 所示，编码器包括两个数据流路径，一个“前向”路径和一个“重构”路径。

“前向”路径：当一个输入帧 Fn 被提交编码，该帧以宏块(相当于 16X16 像素的原始图像)为单位来进行处理。每个宏块被编码成帧内模式或帧间模式，在这两种情况下，会产生一个基于重建帧的预测宏块 P。预测 P 被从当前宏块中减去来产生一个残留的或差异宏块 D_n，它以量化变换系数集 X 变换(使用块变换)并量化，这些系数被重新排序并进行熵编码。在宏块解码时需要的熵编码系数和边信息（如宏块预测模式、量化步长，描述宏块如何运动补偿的运动矢量等等）组成了压缩的比特流。它被传输到网络抽象层(NAL)进行传输或保存。

“重构”路径：为了编码更进一步的宏块，需要通过解码宏块量化系数 X 来重建一帧。系数 X 被重新调整(Q-1)并且进行逆变换(T-1)来产生一个不同的宏块 D’n，这与原始的差异宏块 D_n 不同；它在量化过程中有了损耗，所以 D’n 是 D_n 的一个失真版本。预测宏块 P 被加到 D’n 中来创建一个重建宏块 uF’n(原始宏块的一个失真版本)。为了减少阻断失真的影响使用了一个滤镜，重建参考帧从一系列的宏块 F’n 中创建[7]。

2.2 CAVLC 基本原理

在 H.264 中，CAVLC(基于上下文自适应的可变长编码)用于亮度和色度残差数据的编码。残差经过变化量化后的数据表现出如下特性：4x4 块数据经过预测、变换、量化后，非零系数主要集中在低频部分，而高频系数大部分是零；量化后的数据经过 Zig-Zag 扫描，DC 系数附近的非零系数值较大，而高频位置上的非零系数值大部分是+1 和-1；相邻的 4x4 的非零系数的数目是相关的。CAVLC 充分利用残差经过整数变换、量化后数据的特性进行压缩，进一步减少数据中的冗余信息[8]。CAVLC 的编码过程如下：

(1) 对非零系数的数目以及拖尾系数的数目进行编码；

(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的幅值进行编码；

(4) 对最后一个非零系数前零的数目进行编码；

(5) 对每个非零系数前零的个数进行编码。

2.3 加密原理

假设{P_n}是明文信息序列，{K_n}是密钥信息序列，由 Logistic 混沌方程迭代产生序列后，进行二值化处理后所得整数混沌序列，{C_n}是密文信息序列。

加密算法：{C_n}={P_n}⊕{K_n}；

解密算法：{C_n}={P_n}⊕{K_n}。

上式中，“⊕”表示异或运算，初始值 X_0 和 μ 是 Logistic 方程的参数，同时也是加密系统的密钥参数 K={X_0, μ}。

基于 CAVLC 熵编码加密算法是利用流密码算法加密码字索引，根据加密后新的索引号在原码表中找到对应新码字作为码流输出。加密算法和编码过程同时进行，熵编码在数据打包之前进行，未破坏格式信息，视频具有可操作性。

对拖尾系数的符号进行编码并加密：对于每个拖尾系数(±1)，只需要指明其符号，其符号用一个比特表示(0 表示+，1 表示-)，编码顺序是按照反向扫描的顺序，从高频数据开始。对于一个拖尾系数只需要一个比特密钥序列进行加密。

对除了拖尾系数之外的非零系数幅值 Levels 进行编码并加密：非零系数幅值(Levels)按照反向扫描顺序进行编码，即从高频向低频顺序编码。非零系数的幅

值的组成分为两个部分：前缀(level_prefix)和后缀(level_suffix)。需要对前缀和后缀两部分都进行加密。

3 密钥的产生-Logistic混沌序列

混沌产生方式简单而动力学行为复杂。混沌的非线性，初值敏感性和随机性等特性，使得其产生的伪噪声（PN）序列性能优良，具随机性与长周期特性，适合作为密钥使用。本方案采用 Logistic 产生序列密码，序列密码加密速度快，适合于大数据量、实时性要求较高的加密场合[9]。

Logistic 方程如下:

$$X_{n+1} = \mu X_n (1 - X_n), n = 0,1,2\cdots \quad (1)$$

$X_n \in (0,1)$，$\mu \in (0,4)$,当 μ 取值[3.571448,4]时， logistic 映射进入混沌态，并表现出复杂的的动力学特性。

对方程(1)进行简化:

$$X_{n+1} = f(\mu, X_n) = 1 - \mu X_n^{\ 2}, n = 0,1,2\cdots \quad (2)$$

其中，X_n 分布在(-1，+1)的区间上，当 $\mu = 2$ 时，称为满映射[10]。基于 FIPS 标准(频率测试、串列测试、Poker 测试、游程测试和自相关测试五个指标)测试 Logistic 映射的随机性，发现 Logistic 映射的性能较优[11]，故采用 Logistic 映射进行加密。

获取密钥的步骤：

1）令 $\mu = 2$，初值 X[0] = 0.1，进行方程的迭代；

2）对迭代的序列值 X_n 进行移位：

$$y = F(X_n) = X_n * pow(2, m), m > 0 \quad (3)$$

函数 pow(x,y)表示 x 的 y 次方，上式表示将 X_n 的二进制值左移 m 位；

3）取偏移后的结果的绝对值：

$$y = f(x) = abs(x) \quad (4)$$

函数 abs(x)表示取绝对值，返回 x 的绝对值；

4）对每个 y 取 1 比特组成序列密钥；

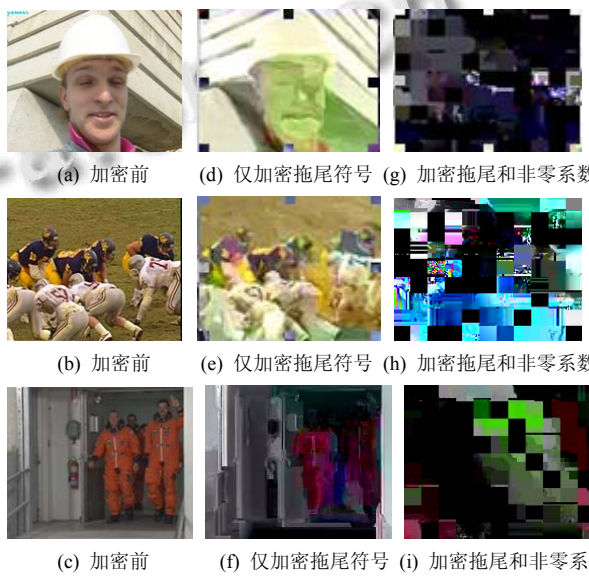
对方程(3)进行迭代，取每个 X_n 的第 n 位值形成一组序列密码，本方案取每个 X_n 的第 8 位值作为视频加密的序列密码。

4 实验结果与分析

4.1 实验结果

本文采用 H.264 参考软件 JM86，对 foreman、football、crew 三个 QCIF(176x144)序列进行混沌加密。实实验硬件环境是 Intel Core 2 Duo 2.53GHz，内存为 2.0GB，软件环境是 Windows XP，VC++ 6.0。通过 Elecard StreamEye 查看经过加密后的.264 文件。

图(a),(b),(c)为原始序列的某一帧，图(d),(e),(f)是仅加密熵编码阶段的拖尾系数的符号的效果图，从图中仍然可以看到原始帧的大致的视频内容，由于没有对 DC 系数和 AC 系数进行加密，所以加密的安全性不够，图(g),(h),(i)是对拖尾系数的符号及非零系数加密，在图(d),(e),(f)的加密基础上又对 DC 系数和 AC 系数进行加密，加密效果得到明显的改善。



(a) 加密前 (d) 仅加密拖尾符号 (g) 加密拖尾和非零系数

(b) 加密前 (e) 仅加密拖尾符号 (h) 加密拖尾和非零系数

(c) 加密前 (f) 仅加密拖尾符号 (i) 加密拖尾和非零系数

图 2 加密效果图

4.2 性能分析

1) 安全性

从密码分析来看，安全性依赖于所选的流密码的安全性，混沌序列在理论上类似噪声，高度随机，没有周期。但在实际工程中发现，由于实现工具的有限精度效应，混沌系统的动力学特性被弱化，产生的序列从混沌无周期信号转为周期信号，但本方案通过 Logistic 序列获取的密钥具有较大的密钥空间，并且由于混沌系统对初始值和参数的敏感性，在不知道加密的混沌系统和初始值的情况下，破译难度非常大。

2) 编码压缩性能

本加密方案在变换和量化后加密，加密算法没有破坏 H.264 的编码原理。对拖尾系数的符号、AC 系数和 DC 系数进行加密，加密的数据量小，加密算法复杂度低，并且加密之后的码流长度没有改变，因此本方案对压缩效率几乎没有影响。

3) 加密效率

对 foreman.yuv 的编码时间进行比较，序列类型为 IPPP，共 3 帧，帧率为 30f/s，量化参数 QP=28，使用 Hadamard 变换和 CAVLC 熵编码。未加密的编码总时间为 2.296s，运动估计总时间为 0.627s；进行混沌加密的编码总时间为 2.329s，运动估计总时间为 0.663s，加密效率较好。

5 结语

本文通过 Logistic 映射产生用于加密的混沌序列，然后对 H.264 的 CAVLC 熵编码阶段进行加密。相对于完全加密算法和部分加密算法，计算复杂度低；相对于 DCT 系数加密算法，没有改变压缩比。实验结果表明，该加密系统不改变视频码流的格式，加密速度快，对密钥非常敏感，并且具有很大的密钥空间，对各种攻击具有较强的抵抗性，具有良好的应用价值。

参考文献

1 Qao L, Nahrstedt K. A new algorithm for MPEG video encryption. Proc. of the First International Conference on Imaging Science, Systems and Technology (CISST'97). LasVegas, Nevada, 1997:21–29.

2 Chiaraluce F, Ciccarelli L, Gambi E, Pierleoni P, Reginelli M. A new chaotic algorithm for video encryption. IEEE Trans. on Consumer Electronics, 2002,48(4):838–844.

3 廉士国,孙金生,王执铨.集中典型视频加密算法的性能评价.中国图像图形学报,2004,9(4):483–490.

4 Tang L. Methods for encrypting and decrypting MPEG video data efficiently. Proc. of the Fourth ACM International Multimedia Conference(ACM Multimedia'96). Boston, MA, 1996:219–230.

5 Tosun AS, Feng WC. Efficient multi-layer coding and encryption of MPEG video streams. IEEE International Conference on Multimedia and Expo. New York, 2000, 1:119–122.

6 Draft ITU-T recommendation and final draft international standard of joint video specification(ITU-T Rec. H.264/ISO/IEC 14 496-10 AVC. In Joint Video Team(JVT) of ISO/IEC MPEG and ITU-T VCEG, JVTG050, 2003).

7 毕厚杰.新一代视频压缩编码标准:H.264/AVC.北京:人民邮电出版社,2005.

8 李晓举,冯战申,胡友情.基于 H.264 CAVLC 熵编码的视频加密方案.计算机工程与应用,2009,45(34):114–117.

9 于志宏,王静波,刘喆,等.基于 Logistic 和 Baker 映射的视频加密方法.吉林大学学报,2008,26(3):253–258.

10 严三国,陈永彬.Logistic 满映射混沌序列性能分析.电子技术,2009:194–196.

11 张波.混沌 PN 序列的性能分析与优化设计[硕士学位论文].杭州:杭州电子科技大学 CAD 研究所,2009.25–28.

(上接第 191 页)

从统计数据可以看出，回写条件下性能比透写提高了 10 倍左右，由此可见，CACHE 极大的提高了系统的性能，同时 IO 的波动范围也都在 20%左右，系统运行比较稳定。

6 总结

(1) 文中的 CACHE 设计采用多线程，多个线程可以并行处理，极大的节约了读写 IO 的时间，提高了 CACHE 和存储阵列的整体性能。

(2) 同时设置了高低水位，根据系统实现情况来判断是否刷脏数据，提高性能的同时也提高了系统的稳定性。

参考文献

1 Chen TF, Baer J. Eeffetive hardware-based data prefetching for high-performance processors. IEEE Trans. on Computers, 1995,44(5).

2 Hsu WC, Smith JE. A perofrmance study of instruction cache prefetching methods. IEEE Trans. on Computers, 1998, 47(5):497–508.

3 Stallings W.计算机组织与结构—性能设计.第 5 版.张昆藏等译.北京:电子工业出版社,2001.

4 汤子瀛.计算机操作系统.西安:西安电子科技大学出版社,1994.