第35卷 第14期 计 算 机 工 程 2009年7月
Vol.35 No.14 Computer Engineering July 2009
·安全技术· 文章编号：1000—3428(2009)14—0158—02 文献标识码：A 中图分类号：TP309

基于混沌的AVS视频压缩加密算法

宋永中[1,2]，王 毅[1]，刘东华[3]
(1. 湘潭大学信息工程学院，湘潭 411105；2. 上海中科计算技术研究所，上海 201203；
3. 国防科技大学电子科学与工程学院，长沙 410073)

摘 要：针对AVS的编码结构，提出一种基于混沌理论的AVS视频加密算法，并集成到AVS编/解码器中。该算法采用实值混沌序列加密和置乱DCT非零系数来加密视频信息。采用3个标准视频序列进行算法仿真，在为AVS编写的rm52j软件平台上进行实验，结果表明，该算法加密速度快，安全性高，对压缩比影响较少。

关键词：混沌；加密；视频压缩

Chaos-based Encryption Algorithm for AVS Video Compression

SONG Yong-zhong[1,2], WANG Yi[1], LIU Dong-hua[3]
(1. College of Information Engineering, Xiangtan University, Xiangtan 411105;
2. Shanghai Division Institute of Computing Technology, Chinese Academy of Sciences, Shanghai 201203;
3. School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073)

【Abstract】 An approach of utilizing the chaos to Audio Video coding Standard(AVS) encoded frame is proposed, and it is integrated into the AVS CODEC. This algorithm encrypts DCT nonzero coefficients by using real-value chaotic sequence and then confuses DCT nonzero coefficients. Conducts simulate on three standard video sequence. Simulation results are tested on rm52j software platform, which indicates this algorithm is fast at encrypting data, good at security and affects little to compression.

【Key words】 chaos; encryption; video compression

1 概述

随着多媒体技术及网络通信技术的飞速发展和普及，无线通信技术被广泛使用，人们更容易接触和获取传输存储处理中的数字视频，因此，视频信号的保密工作及其加密技术的研究就显得十分紧迫和重要。

最初的视频加密方法为直接加密算法，它们没有利用视频数据的任何特性，仅将视频比特流与传统的文本数据同等对待，直接将视频图像数据用标准加密算法，如用DES, AES进行加密。虽然这可能是最安全的视频图像加密方法，但由于视频数据量非常大，使得该算法计算复杂度较高，实时性较差，因此在实际中很少使用。另外一类视频图像加密算法为选择性加密(selective encryption)算法，如 Aegis, zig_zag, VEA[1]等算法。这类视频图像加密算法不同于传统的加密算法，它们利用了视频数据的特性，仅仅对全部数据的一小部分进行加密，在多媒体数据传输过程中能用很小的计算复杂度来达到较高的安全性。

2 AVS介绍

AVS(Audio Video coding Standard)是我国自主制定，拥有自主知识产权的音视频编码标准。与世界其他知名音视频编码标准相比，它具有如下特点：

(1)性能高，编码效率比MPEG2高2倍以上，与H.264的编码效率相当；

(2)算法复杂度比H.264低；

(3)软硬件实现成本都比H.264低；

(4)专利授权模式简单，费用明显低于同类标准。在码率和*PSNR*相当时，AVS的编码速度是H.264的4倍以上[2]。

AVS是基于8×8的DCT变换，DCT变换可表示如下：

$$Y_{xy}=C_xC_y\sum_{i=0}^{7}\sum_{j=0}^{7}X_{ij}\cos\frac{(2j+1)y\pi}{16}\cos\frac{(2i+1)x\pi}{16}$$

其中，$C_x,C_y=\begin{cases}1/2\sqrt{2} & x,y=0\\ 1/2 & \text{其他情况}\end{cases}$。也可表示成矩阵形式：$\boldsymbol{Y}=\boldsymbol{AXA}^{\mathrm{T}}$，其反变换为$\boldsymbol{X}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{YA}$。其中，$\boldsymbol{X}$表示采样矩阵；$\boldsymbol{Y}$表示变换后的系数矩阵；$\boldsymbol{A}$是1个8×8转换矩阵：

$$A_{ij}=C_i\cos\frac{(2j+1)i\pi}{16}$$

AVS采用I, P, B帧的结构。I帧的编码无须参考别的帧，它提供了对编码图像数据序列的访问点，使解码可由此点开始，但仅采用了最普通的压缩方法；P帧采用更有效的压缩编码方法，它使用运动补偿法，通过过去的I帧或P帧来预测，一般也可作为后面预测的参考帧；B帧实现了最高程度的压缩，但需要使用过去的和未来的参考帧来进行运动补偿，B帧不能再作为其他预测帧的参考帧。序列中I帧、P帧和B帧的组织是非常灵活的，由编码器根据实际情况来选择其安排[3]。I帧是解码的开始点，对I帧进行加密，则加密结果将通过P帧和B帧扩散到整个视频文件中。因此，本文采用只加密I帧的加密方法。

3 基于混沌理论的视频压缩加密方案设计

3.1 总体方案

混沌理论是一门专门研究奇异函数、奇异图形的数学理

作者简介：宋永中(1976－)，男，硕士研究生，主研方向：嵌入式系统设计，信源编码；王 毅，副教授；刘东华，博士

收稿日期：2008-11-01 **E-mail：**asengo_008@sina.com

论，研究自然界有序、无序规律的学科。混沌系统有 2 个主要特征：对初始条件的敏感性和系统变化的不可预测性。它们是密码学随机序列的重要特征，因此，混沌理论也被加入到密码学基础理论中[4]。

本文采用的加密过程取在量化之后熵编码之前，这样可以简化加密算法、减少运算量、减小密钥的开销且不影响压缩效率。如按传统方法在量化之前对 DCT 系数加密，那么等于 0 的系数很少，就需要很多的密钥来分配。然而经过量化以后，很多系数会变成 0，在一般运动场景下，对 AVS 的 8×8 块量化后进行统计，在量化参数 *QP* 取 28 的情况下，大约 2/3 的系数量化后变为 0，那么分配给这些系数的密钥就完全浪费掉了。量化之前的加密，出于不破坏 DCT 系数自身统计特性和 zigzag 特性(以便于后面的熵编码，且不会对比特率造成很大影响)的考虑，只能在同阶次的系数之间置乱(直流与直流之间，同阶交流之间置乱)。由 DCT 变换的特性可知，这种同阶的置乱效果不是最理想。然而，量化之后(特别是在 zigzag 排序之后)的置乱就可以在高频和低频系数之间进行，由于熵编码是根据系数的概率进行的，这样就不会破坏 DCT 系数的统计特性而不会对压缩比和码率有较大影响，因此能获得非常好的加密效果[5]。另外密钥要经过 DES 加密后传到解密端。

本方案具体实施如下：由于 AVS 是基于 8×8 的 DCT 变换，因此首先对 16×16 亮度宏块中 4 个 8×8 块进行随机洗牌，打乱 4 个 8×8 块的顺序。然后利用实值混沌序列对量化后的 8×8 块非零系数进行比例变换，只变换非零系数。量化后的 8×8 块中的非零系数已经很少了。这样加密的速度很快，最后置乱变换后的 8×8 块，置乱在非零系数之间进行，这样不会破坏 DCT 系数的统计特性，对压缩比和码流影响较少。其中置乱矩阵由混沌序列的大小序号生成，由于混沌序列对初始值非常敏感，即使密钥值有微小的变化也会得到完全不同的解密结果。

3.2 对 8×8 块的随机洗牌

把一个 16×16 宏块中每 1 个 8×8 块作为 1 个基本单位(AVS 是基于 8×8 的 DCT 变换)进行随机置乱，而 8×8 块内的系数的相对位置不变。8×8 块的随机洗牌没有改变 DCT 系数的统计特性。对压缩比和码流影响较少。

3.3 实值混沌序列的产生及加密

笔者所采用的实值混沌序列是由 Logistic 迭代序列 $X_{n+1}==\lambda X_n(1-X_n)$, $X_n\in[0, 1]$生成的，$X_0=0.607$ 作为系统的密钥，参数 λ 的值设定为 4，利用生成的序列$\{X_k\}(k=1, 2,\cdots,64)$排列成一个 8×8 的矩阵 ***P***，只生成与 8×8 的 DCT 非零系数对应位置的元素。假设 8×8 的 DCT 矩阵为 ***D***。将 ***P*** 与 ***D*** 做点积完成一次加密：$\boldsymbol{T}=\boldsymbol{P}\otimes\boldsymbol{D}$。

3.4 置乱加密

将生成的实值混沌矩阵 ***P*** 按数据大小排序，按数据序号生成置乱矩阵，置乱在非零元素之间进行。假设生成的置乱矩阵 ***M*** 为

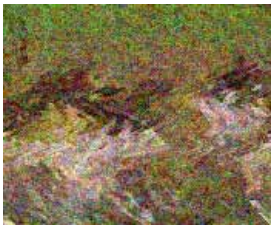
$$\boldsymbol{M}=\begin{vmatrix} 13 & 4 & 7 & 14 & 8 & 5 & 10 & 0 \\ 6 & 12 & 9 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 11 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}$$

则可采用如下方式置乱，如：14 号数据和 1 号数据交换位置，13 号数据和 2 号数据交换位置，12 号数据和 3 号数据交换位置等。

4 实验结果及分析

实验采用专门为 AVS 编写的 rm52j 软件平台测试，通过应用上述加密方案，对 football_qcif.yuv, bus_qcif.yuv, silent_qcif.yuv 这 3 个序列进行了加密，其中，序列 football_qcif.yuv 的 I 帧加密效果如图 1 所示，可以看出，加密后的图像已经无法识别。

(a)Football_qcif.yuv 原始图像



(b)Football_qcif.yuv 加密后的图像

图 1 序列 football_qcif.yuv 的 I 帧加密

3 个序列加密前后的数据对比如表 1、表 2 所示。

表 1 序列加密前的数据对比

序列	码率/(bit·s^{-1})	*QP*	*SnrY*	*SnrU*	*SnrV*	编码时间/ms
Football_qcif	334 120	28	38.259 8	38.978 4	38.957 0	7 891
Bus_qcif	278 800	28	38.529 2	39.525 8	39.462 4	6 984
Silent_qcif	215 664	28	39.003 1	39.681 1	40.061 9	5 922

表 2 序列加密后的数据对比

序列	码率/(bit·s^{-1})	*QP*	*SnrY*	*SnrU*	*SnrV*	编码时间/ms
Football_qcif	334 152	28	38.245 8	38.975 2	38.925 6	7 896
Bus_qcif	278 834	28	38.502 1	39.523 1	39.435 4	6 988
Silent_qcif	215 695	28	39.001 5	39.678 5	40.059 8	5 926

由以上实验结果可以看出：加密后，码流增加不大，对信噪比的影响主要在小数点后 2 位，I 帧编码时间增加 4 ms~5 ms，这样的结果完全可以接受。在安全性方面，由于混沌系统对初始值和参数非常敏感，可以提供很大的密钥集合，完全满足加密的需要。

5 结束语

本文针对 AVS 编码框架的特点，提出一种基于混沌加密理论的视频加密方案并加以实现。从实验结果可以看出，该方案在安全性、效率方面有很大优势，而且因为主要时间花费在对图像的 DCT 变换量化之后进行，所以在时间上的开销不会增加很多，可适用于基于 AVS 的视频监控领域。

参考文献

[1] Tang Lei. Methods for Encrypting and Decrypting MPEG Video Data Efficiently[C]//Proceedings of the ACM Multimedia. Boston, USA: [s. n.], 1996.

[2] 张欣佑, 张晓东, 王 浩. AVS 编码与 DSP 实现的视频编码器[J]. 单片机与嵌入式系统应用, 2006, (12): 16-18.

[3] 国家标准化管理委员会. GB/T20090.2-2006 信息技术先进音视频编码第 2 部分: 视频[S]. 2006.

[4] Weisstein E W. Logistic Map[DB/OL]. (2004-09-26). http://m-athworld.wolfram.com/LogisticMap.html.

[5] 曹 奕, 张 荣. H.264 标准中基于 DCT 的视频加密的研究[J]. 中国图象图形学报, 2005, 10(8): 1047-1051.

编辑 顾姣健