文章编号:1002-8692(2009)04-0033-03

基于达芬奇平台的 H.264 视频流加密终端的设计

·实用设计·

李　丹,王　健,季晓勇
(南京大学 电子科学与工程系,江苏 南京 210093)

【摘　要】设计了基于 TI 公司达芬奇芯片 TMS320DM6446 的 H.264 视频流选择加密终端。针对 H.264 视频编码结构的特点,提出一种基于数据分割模式的视频流选择加密策略,详细描述了终端的硬件系统和软件设计。实验结果表明,待加密的数据量大为减少,能够对 CIF 格式 H.264 视频流进行实时加密。

【关键词】H.264;TMS320DM6446;数据分割模式;视频加密
【中图分类号】TP309.7　　【文献标识码】B

Design of Encryption Terminal for H.264 Video Based on DaVinci Platform

LI Dan, WANG Jian, JI Xiao-yong
(*Department of Electronic Science and Engineering, Nanjing University, Nanjing 210093*)

【**Abstract**】A kind of encryption terminal using TMS320DM6446 is designed in this paper. Considering the structure of H.264 bit-stream, the policy of selected video encryption based on H.264 Data Partition Mode (DPM) is presented. The hardware and software design of the terminal is described. The experimental results show that the system can encrypt real-time H.264 video stream in CIF mode with a lower complexity.

【**Key words**】H.264; TMS320DM6446; DPM; video encryption

1 引言

H.264/AVC[1]是由 ITU-T 和 ISO/IEC 联合制定的最新视频编码标准,其优异的压缩性能和网络亲和性使其在多媒体应用的各个领域发挥越来越重要的作用。目前视频加密算法大体可以分为全部加密和选择性加密两类[2]。其中,全部加密算法不考虑视频编码结构,将视频压缩数据看作二进制数据进行处理;选择性加密算法则考虑编码过程和结构,选择较敏感的关键信息进行部分加密。

笔者在 TI 的达芬奇平台上设计一种安全的 H.264 视频终端。其中,针对 H.264 视频编码结构的特点,提出并实现了一种利用编码中的数据分割功能对最重要的部分视频数据进行加密的算法,无需对编解码器硬件系统做较大改动,对于编码压缩性能影响小,具有一定的数据可操作性,符合视频数据实时加密的要求。

2 基于 DaVinci 的视频流加密终端的硬件设计

H.264 视频终端的硬件设计如图 1 所示,主要完成视频编解码、视频流加解密和网络传输等功能。系统采用达芬奇技术的 TMS320DM6446(后简称"DM6446")为核心[3],外设包括 64 Mbit SDRAM,Flash 单元、视频解码芯片 SAA7115H 和视频编码芯片 SAA7121H,ATA 硬盘和以太网接口、外接时钟以及电源模块等。

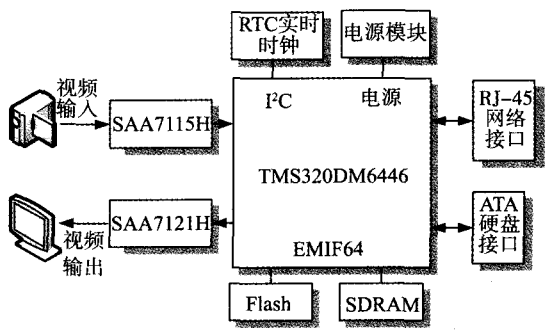

图 1　终端硬件系统框图

视频数据压缩和加密流程为:由摄像机采集的 PAL 视频信号经过视频解码器 SAA7115H 解码变成 CCIR656 标准 4:2:2 数字信号,通过 DMA 方式直接读入内存后由 DM6446 完成数据的压缩编码和加密,然后通过网络控制器后传到以太网或硬盘。

视频数据解压缩和解密流程为:来自以太网或硬盘的视频数据经过网络控制器后由 DM6446 完成数据的解压,解压后的 CCIR656 标准数字信号再通过 DMA 方式传输到视频编码器 SAA7121H 进行编码,最终,编码后的 PAL 视频信号在屏幕上显示出来。

3 H.264 视频流加密终端的软件设计

3.1 H.264 编码结构分析

H.264/AVC 编码器采用了两层结构：视频编码层(Video Coding Layer,VCL) 和网络抽象层(Network Abstraction Layer,NAL)[4-5]。VCL 对编码视频信息进行有效地描述，获得高效的压缩数据;NAL 对编码信息进行打包封装并通过特定网络传输编码视频信息。NAL 工作模式分为单片模式(Single Slice Mode,SSM)和数据分割模式(Data Partition Mode,DPM)。

在 DPM 模式中,Slice 被分为 3 个分区,每个分区里包含不同重要程度的宏块信息,称为 Partition A,Partition B和 Partition C,如表 1 所示。这种数据分割方式下,B 类和 C 类数据各自独立,但它们的解码必须依赖于 A 类数据,这就意味着在发送端可以选择对重要的数据进行加密处理,这些重要的信息在接收端接收到后确保正确解密才能正常解码。当采用了数据分割模式后,3 类数据被编码器放入不同的 NAL 单元分别进行传输。

表 1 DPM 模式中不同分区的信息内容

	Partition A	Partition B	Partition C
内容	片头信息、宏块类型、量化参数、运动矢量信息	帧内编码数据块的编码方式信息、帧内变换系数	帧间编码块的编码方式信息和帧间变换系数
重要性	最高	中等,依赖于 Partition A	最低,依赖于 Partition A

每一个 NAL 单元包含两个部分:1 byte 的 NAL 头信息和一个原始字节序列载荷 (Raw Byte Sequence Payload,RBSP)。NAL 头信息中的 NAL_Type 有 5 bit,其值为 1~31,标记本单元内 RBSP 数据结构的类型。根据 RBSP 的类型,NAL 单元分为 VCL-NAL 单元和非 VCL-NAL 单元。NAL 单元的 NAL_Type 为 1~5,包含图像采样值的数据,当 NAL_Type 为 1 表示 Partition A,为 2 和 3 分别表示 Partition B 和 Partition C。非 VCL-NAL 单元则包含参数集和 SEI 信息。

3.2 视频流加解密模块的软件设计

H.264 视频终端程序包括视频压缩编解码模块和加解密模块。其中加解密模块采用了选择性加密算法的思想,结合 H.264 的数据分割模式,对 H.264 视频码流的关键数据进行加密,其流程框图如图 2 所示。

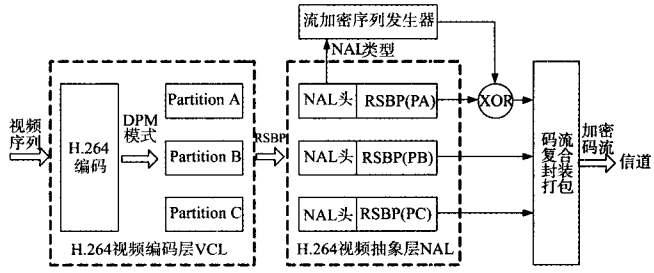

图 2 基于 H.264 的数据分割模式的选择性视频流加密软件框图

首先,H.264 视频编码器的编码选择数据分割模式,视频编码层 VCL 根据重要程度划分视频编码数据:编码视频中数据片和宏块的头部信息、运动矢量信息以及宏块类型信息等最重要的数据封装在 Partition A，其他次重要的帧内变换信息和最次要的帧间变换信息则分别封装在 Partition B 和 Partition C。其次,这 3 类数据被送入视频编码抽象层 NAL 分别进行封装，通过 NAL 单元中的 NAL 头可以标识其载荷 RBSP 的类型，然后根据 NAL 单元类型的表示，只对 Partition A 的数据进行异或加密处理,最后将 3 类 NAL 单元经码流复合打包送入信道传输。需要补充的是,非 VCL-NAL 单元中辅助增强信息 SEI 单元、序列参数集单元和图像参数集包含着编码中非常重要的信息,如图像尺寸、熵编码类型、运动矢量分辨率等,这些信息将直接影响能否正确解码,对于这些 NAL 单元也将进行加密处理。

4 视频流加密模块的测试和性能分析

将 SEED 公司的 DaVinci 开发板经由 JTAG 口连接到仿真器，再连接到计算机。使用视频流加密模块对 5 种标准测试序列 (Foreman,Mobile,News,Hall 和 Bus)进行编码和加密[6],考虑到 PC 与 DSP 通过仿真器和 JTAG 口通信速率慢,故将原始码流文件预先放入开发板的存储器中。

分别统计其 I 帧、P 帧和 B 帧中 Partition A 的数据长度，计算了测试序列 Partition A 的平均码率，以及编码、加密的平均时间,见表 2。

从表 2 可以看出，各测试序列中全部 Partition A 的数据量占序列总长度的比例在 23.5%~49.2%之间，从 I,

表 2 H.264 视频码流分析

H.264 视频序列	每帧 Partition A 平均长度/(bit/帧)	序列总长度/bit	Partition A 所占比例/%	H.264 码率/(Kbit/s)	Partition A 平均码率/(Kbit/s)	平均每帧编码时间/ms	平均每帧加密时间/ms	每帧总耗时/ms
Forman	600 789	1 220 444	49.2	308.9	152.0	24.71	4.674	29.38
Mobile	1 118 952	4 768 698	23.5	1 203.0	282.3	22.17	8.681	30.85
News	260 034	766 551	33.9	194.4	66.0	19.36	2.030	21.39
Hall	266 329	719 810	37.0	182.6	67.6	18.06	2.079	20.14
Bus	949 827	3 761 428	25.3	949.5	239.8	21.35	7.374	28.72

P和B帧的Partition A数据量来看，P帧最大，B帧次之，I帧最小，也就是可以通过调整编码格式进一步调整Partition A的平均码率。这意味着使用笔者设计的视频流加密模块进行流加密时，只需要处理不到一半的数据，减少了加密的数据量，显著降低了加密系统的计算复杂度，从每帧的编码和加密时间可以看到，本设计处理每帧的总耗时均在33 ms以下，可以满足CIF格式、帧率为30 f/s(帧/秒)的H.264视频加密的实时性要求。

5 小结

笔者设计了一种基于DM6446的H.264视频流选择加密终端，利用H.264标准的数据分割模式，大大降低了软件设计的复杂度，有效减少了待加密的视频数据量，实现了H.264视频的实时加密，且基本不需对H.264基本编解码的硬件系统进行改动，易于推广。

参考文献：

[1] H.264/ISO/IEC 14 496-10 AVC, Draft ITU-T Recommendation and final draft international standard of joint video specification[S]. 2003.

[2] 廉士国，孙金生，王执铨. 几种典型视频加密算法的性能评价[J]. 中国图象图形学报，2004，9(4)：483-490.

[3] Texas Instruments Incorporated.TMS320DM6446 digital media system on chip[EB/OL]. [2009-01-11].http://focus.ti.com/lit/ds/symlink/tms320dm6446.pdf.

[4] 戚永豪，李式巨，赵民建. 一种基于H.264/AVC的数据自适应不平等保护策略[J]. 电视技术，2005(9):16-18.

[5] WENGER S. H.264/AVC over IP[J]. IEEE Trans. on Circuits and Systems for Video Technology，2003，7(13):645-656.

[6] 代明，张宇，华一满，等. 超混沌迭代同步在数字语音保密通讯中的应用[J]. 南京大学学报:自然科学版，1999，35(1):110-115.

作者简介：

李 丹(1982-)，硕士生，主研多媒体通信和信息安全技术；

王 健(1978-)，讲师，主研视频编码与传输；

季晓勇(1959-)，教授，从事多媒体通信、信息安全方面的研究。

责任编辑：许 盈 **收稿日期：2009-01-27**

(上接第32页)

增强信息完成该行的显示。继续判断是否还有其他的行需要显示直到25行全都结束。

5 小结

图文电视作为一种被广泛接受的服务，在数字电视时代同样得到了很好的支持。笔者提出一种图文处理的软件解决方案，并使用UML对其进行了详细的建模设计，最终完成了通用的图文处理组件。因为采用了面向对象的方法，软件结构更加合理，并为组件功能在今后的进一步扩展奠定了基础。目前该组件的所有设计目标都已实现，可完全满足1.5级别图文的功能要求，其优良的兼容性和可移植性在实际应用中得到了验证，已被集成于各种软硬件平台下的多款数字电视终端产品中。

参考文献：

[1] ETSI EN 300 472,Digital video broadcasting (DVB); specification for conveying ITU-R system B teletext in DVB bitstreams[S].2003.

[2] ISO/IEC 13818-1-1994,Generic coding of moving pictures and associated audio information: systems[S].1994.

[3] ETSI EN 300 706,Enhanced teletext specification[S]. 2003.

[4] BOOCH G,RUMBAUGH J, JACOBSON I. UML用户指南[M].邵维忠，麻志毅，张文鹃，等，译. 北京：机械工业出版社，2001.

[5] 孙亚敏.基于DVB机顶盒的VBI图文接收系统[J].电视技术，2006(8):42-46.

[6] HAMILTON K,MILES R. Learning UML 2.0 [M]. [S.l.]:O′ Reilly, 2006.

[7] LARMAN C. Applying UML and patterns: an introduction to object-oriented analysis and design andIterative development[M]. 3rd ed. [S.l.]:Addison Wesley Professional. 2004.

作者简介：

任郁茁(1977-)，女，硕士，助教，主研电子信息技术；

廉 毅(1977-)，主要研究方向为数字电视、IPTV和移动电视。

责任编辑：许 盈 **收稿日期：2009-02-15**

新书介绍

《视频对象分割提取的原理与应用》一书已由科学出版社出版。该书由我国第一部“数字电视原理”的作者张兆扬教授等编著。自MPEG-4提出基于视频内容和对象的编码以来，视频对象分割除用于提高编码效率以外，已在视频索引/检索、智能视频监控、视频会议与移动通信、虚拟现实与三维电子游戏以及医学、遥感、军事和工农业生产监控检测中得到广泛应用，但是至今尚无一部系统性地从理论到应用详细阐述的专门著作，该书正是为推进这一领域的发展应运而生。

该书分为六章、四大部分，特点是理论与实践紧密结合，集作者十多年之研究、开发经验，在理论阐述上深入浅出、线条清晰，在实验上对不同应用场合的分割提取方法给出了实验手段、过程和结果，除主观评价验证外，还结合客观评价准则，以方便用户判断所采用方法的优劣、按照用户需求及时调整分割参数或选择新的分割方法。书号为ISBN 978-7-03-024185-6。