基于改进型 OFB 模式的视频流加密方法

范 晶，贾旭光
（华北计算机系统工程研究所，北京 100083）

摘 要：介绍了一种新型的视频流加密系统设计方法，并结合无线通信中常用的交织技术，提出了一种新型的密钥分发管理机制和改进型 OFB 加密工作模式。提出的加密方法保留了 TS 包结构，硬件实现简单，协议开销小，安全性高，适用于 AES 和 SM4 等加密算法，可以广泛应用于无线图像传输及数字电视广播系统中。

关键词：OFB；TS 流；加密；密钥分发
中图分类号：TN918 **文献标识码**：A DOI：10.16157/j.issn.0258-7998.191345

中文引用格式：范晶，贾旭光. 基于改进型 OFB 模式的视频流加密方法[J].电子技术应用，2021，47(2)：63-66.
英文引用格式：Fan Jing，Jia Xuguang. A new video encryption method based on modified OFB mode[J]. Application of Electronic Technique，2021，47(2)：63-66.

A new video encryption method based on modified OFB mode

Fan Jing，Jia Xuguang
(National Computer System Engineering Research Institute of China，Beijing 100083，China)

Abstract：A new design of video stream encryption system is introduced，combined with the interleave technology，which is widely used in wireless communication. This paper provided a new key distribution and management system and a modified Output-Feedback encryption operate mode. The provided method keeps the structure of the transport steam packet，has a low protocol cost and a high level of security，compatible with the AES and SM4 encryption algorithm，thus can be easily implemented in hardware and widely used in wireless image transmission and digital video broadcasting system.

Key words：OFB；transport stream(TS)；encryption；key distribution

0 引言

目前，在地面数字电视广播、网络视频监控及无线图像传输等多个领域，视频图像往往采用明文的方式进行传播，并且现有大部分视频传输标准均为公开标准，一旦传输信号被截获，很容易将视频信号解调出来，存在严重的泄密隐患。针对此现状，本文提出了一种视频流加密方法，该方法不破坏视频流原有的传输流(Transport Stream，TS)包结构，兼容现有传输系统。同时，结合现在的 AES 和 SM4 等对称加密算法的特点，引入无线通信中常用的交织技术，提出了新型的密钥分发管理机制和改进型 OFB 加密工作模式。密钥分发和加密单元中交织器的引入，以较低的硬件成本大大提升了加密强度。本文提出的视频流加密方法，具有简单高效、无需填充、协议开销小、易于 FPGA、ARM 等硬件实现等诸多优点，可广泛用于上述视频传输系统中。

本文提出了改进型 OFB 工作模式，介绍了新型密钥分发机制的实现方式，然后以地面数字多媒体广播(Digital Terrestrial Multimedia Broadcast，DTMB)系统为例，详细描述了视频流加密方法的具体实施过程，最后与普通模式进行了性能对比。

1 背景技术介绍

地面数字电视和网络视频传输视频图像多采用以 MPEG-2 或 H.264 编码的 TS 流。常用的商用对称加密算法为高级加密标准(Advanced Encryption Standard，AES)和我国提出的 SM4。为解决视频流明文传输的缺陷，已有不少研究人员提出了自己的视频流加密方案。如在一专利中提出，将 TS 流切割成 n 个视频块，每个视频块长度固定为 188 B 和长度值的最小公倍数，各个视频块独立并行加密[1]。该专利提出的方案破坏了 TS 流原有每个包 188 B 结构，加密后的密文不适用于现有的数字视频广播(Digital Video Broadcasting，DVB)、DTMB 等地面数字电视传输系统，并且对不满足长度部分进行填充，降低了传输效率。针对流加密，也有提出使用线性反馈移位寄存器(Linear Feedback Shift Register，LFSR)进行加解密的系统[2]，LFSR 受限于 M 序列本原多项式，生成的密码流虽然随机性强，但模式不多，相比 AES 和 SM4 加密算法极易破解。本文充分分析了 TS 包的结构特点，结合现有加密算法，在不破坏原有结构的基础上进行加密，加密

后的密文仍适用于复用器及数字电视等传输系统。

1.1 TS 包格式介绍

TS 流(传输流)是一种用于存储和传输音视频数据的标准格式,被广泛应用于数字电视广播系统 DVB、DTMB 中。现有无线图像传输系统大多采用 TS 流作为传输单元。TS 包为 TS 流的基本单元,每包包含 188 B,由 4 B 的包头和 184 B 的数据负荷组成。包头包含 1 个同步字节的头十六进制 47、13 bit 的包标记符(Packet IDentifier,PID)、4 bit 的包连续计数等字段[3]。同步头用于同步 TS 流,PID 用于区分 TS 流中不同类型的数据包(如视频音频包),TS 流中同类型包,PID 相同,但包连续计数域数值会依次从 0 到 15 累加。本文设计的加密系统利用 PID 和包连续计数作为地址对不同的密钥进行索引,实现不同的 TS 包采用不同的密钥加密,相同类型的 TS 包采用 16 个密钥进行轮换加密,增加加密的可靠性。

1.2 常用加密算法及工作模式

现代密码根据加解密所用密钥分为非对称加密算法和对称加密算法两类。非对称加密算法加解密使用不同的密钥,多采用椭圆曲线算法,加密结构复杂,常用于数字签名和用户认证;对称加密算法加解密使用同样的密钥,具有计算量小、加密运算单元简单易于硬件实现等优点,常用于加密高速数据流。常见的对称加密算法为 AES 和 SM4,针对高带宽、高性能等应用场景,可以方便地引入采用流水线架构提高吞吐率[4],针对低速率、低功耗(如物联网等)领域,也有轻量级处理架构设计方案[5]。

加密算法在现实应用中有多种工作模式,常用的工作模式有电子密码本(Electronic CodeBook,ECB)、密码分组链接(Cipher-Block Chaining,CBC)、计算器模式(Counter,CTR)、密文反馈(Cipher FeedBack,CFB)和输出反馈(Output FeedBack,OFB)模式共 5 种。ECB 模式加密解密使用不同的硬件架构,而其余 4 种模式加密采用密码流与明文异或的方式生成密文,解密只需同样的密码流与密文再次异或即可得到明文,因此只需用一种结构即可完成加解密,减少硬件复杂度。同时,ECB 模式对传输错误非常敏感,一个比特错误造成的解密失败会扩散到整个分组单元,而其余 4 种模式采用异或方式,错误仅局限于自身,不扩散。这 4 种模式中,OFB 模式最为常用。为了进一步增强 OFB 模式的安全性,本文结合无线通信中常用的交织技术提出了改进型 OFB 工作模式。

1.3 交织技术及改进型 OFB 工作模式

无线通信的信道环境复杂多变,深衰落会造成大面积的块传输错误。采用交织技术可以实现将整块打散分别传输,接收端进行解交织还原。大面积错误分散到各个信号帧中,增大解码成功的可能,从而提高传输系统的鲁棒性[6]。信息论鼻祖香农指出,一次一密且密钥随机性越大,加密强度越高[7]。交织技术具有随机性的特点,因此可用于改进加密的工作模式,提升加密系统的性能。

传统的 OFB 工作模式加密单元以初始向量和密钥作为输入,加密单元的输出作为后级加密单元的输入并使用同样的密钥得到输出,按照此模式依次向后级联。由各个加密单元的输出得到密码流,将密码流与明文异或实现加解密,如图 1 所示。

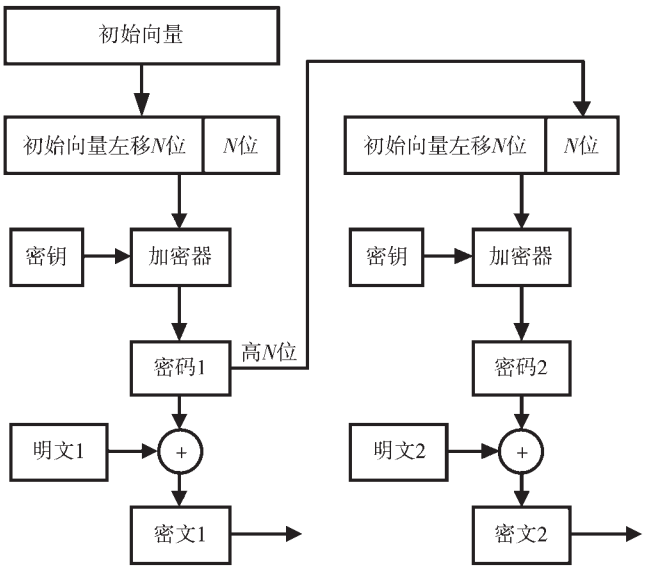

图 1 OFB 工作模式结构框图

本文提出的改进型的 OFB 模式在各个加密器的输入端引入交织器,将待加密数据打散乱序输出,增加随机性,提升加密强度。交织器的输入位宽为初始向量位宽,输出位宽为加密器的分组长度,如图 2 所示。

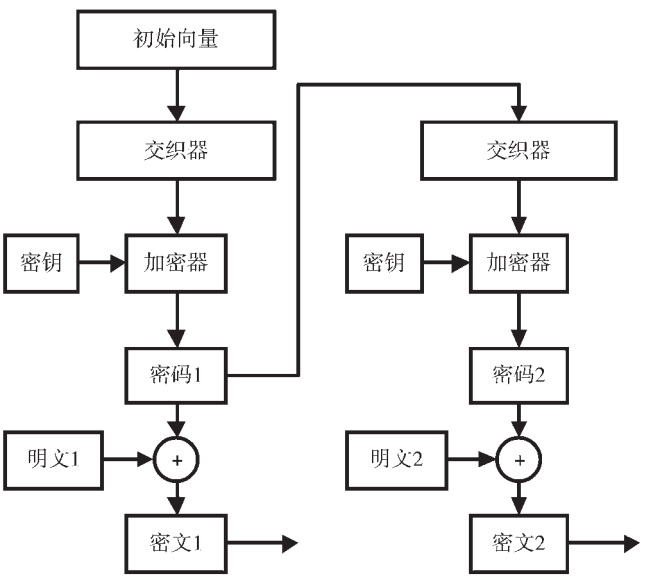

图 2 改进型 OFB 工作模式结构框图

2 基于改进型 OFB 模式的加密方法

现代密码体制往往采用算法公开、保护密钥的方式

进行加密。该方式对密钥的分发管理机制有较高的要求，对称加密系统初始化时，常常将密钥存入存储器中，存储密钥的常常为 EEPROM 等掉电不丢失的器件，一旦存储器被非法读取，会造成密钥泄露，导致泄密。为解决上述问题，本文将结合上文提到的交织技术提出一种新的密钥分发管理机制，然后以 DTMB 传输系统为例，详细介绍基于改进型 OFB 工作模式的加密方法的具体实施过程。

2.1 密钥分发管理机制

初始密钥和初始向量的生成依赖物理热噪声源，初始密钥根据所选择的加密算法长度不同，如 AES128 和 SM4 长度为 128 bit，AES256 长度为 256 bit。提取多组初始密钥和初始向量存放于存储器中，形成查找表。取出 TS 包中的 PID 和包连续计数字段共 17 bit 数据作为地址访问存储器，如果地址和存储器输出数据不做处理，存储器内信息一旦被读取，存在严重的泄密风险。本文提出的新型密钥分发管理机制充分利用交织器的随机性分别对输入地址和输出数据进行处理，需要两个交织器分别连接存储器的输入和输出。存储器前的交织器 A 的输入位数为固定 17 bit，输出位数可根据存储器的深度灵活变化，实现一对一映射或多对一映射。多对一映射节省了存储器，但因为多个 TS 包均采用同一个初始向量和密钥加密，牺牲了安全性，存储器后的交织器 B 输入位数为存储器的位宽，输出位数为初始向量和密钥位宽之和，密钥分发管理体制框图如图 3 所示。

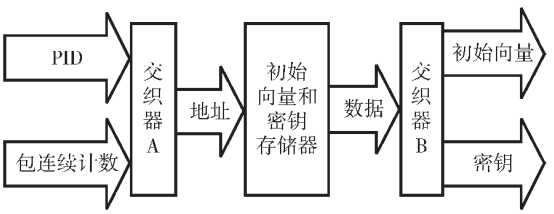

图 3 密钥分发管理体制框图

交织图样可以采用固定单一模式，如固定使用输入比特倒序输出模式，也可以采用动态轮换模式，按照一定的模式更换。交织图样保密不公开，存储器的输入与输出均被交织器打乱。因此，即使存储器中的数据全被窃取，密钥也不会丢失。

2.2 加密流程

视频传输常应用于无线图像传输和数字电视广播等领域。常见的数字电视标准有 DVB、DTMB 和 ATSC 等。其中，DTMB 是我国具有自主知识产权的地面数字电视标准。DTMB 以 TS 包作为传输单元，实现视频信号到射频调制信号的相互转换[8]。下面以 DTMB 系统为例，讲述基于改进型 OFB 工作模式的视频流加密的具体实施流程。

首先，系统上电初始化，从噪声码芯片或其他物理噪声源读取伪随机信号生成初始向量和密钥，并存放于存储器中。接着，对待传输的 TS 流进行同步，锁定同步包头。采用二次同步的方式对 TS 流进行同步，具体实现过程为检测接收的 TS 流，收到数据为十六进制 47 则进入预同步状态，计数器清零并开始计数，当计数到 187 时检测收到的数字是否仍为 47，是 47 则进入二次同步状态，不是则跳回预同步状态。在二次同步状态再次清零计数器并继续计数，计数器再次累加到 187 时，如果收到数据为 47 则同步完成，否则跳转到预同步，重新开始同步过程，二次同步流程图如图 4 所示。码流同步完成后，提取 TS 包中的 PID 和包连续计数信息，PID 为 47 同步字节后两个字节拼接后的低 13 位，包连续计数为 47 同步字节后第三个字节的低 4 位。根据 PID 和包连续计数确定初始向量和密钥。将 PID 和包连续计数共 17 bit 数据输入交织器，交织器 A 实现将数据线 17 打乱重新排序功能，交织器 A 的输出作为地址信息对初始向量和密钥存储器进行寻址，存储器的输出连接另外一个交织器 B，交织器 B 实现存储器输出数据的进一步打散，最后，将交织器 B 的输出的低部分作为初始向量，高部分作为密钥。生成密钥和初始向量后，采用改进型 OFB 工作模式得到与明文长度相同的密码流。本文提出的加密系统需要加密的明文长度为 184 B 共 1 472 bit。AES 和 SM4 加密模块的分组长度均为 128 bit，1 472 除以 128 向上取整为 12，因此需要 12 个密码块的拼接形成密码流。改进型 OFB 模式与普通 OFB 模式一样，密码流的生成不依赖于明文的输入，因此可以提前工作，等明文到来时直接加密输出，减小加密延迟。最后，将密码流与 TS 包除包头 4 B 外的 184 B 进行异或得到密文输出。加密流程图如图 5 所示。

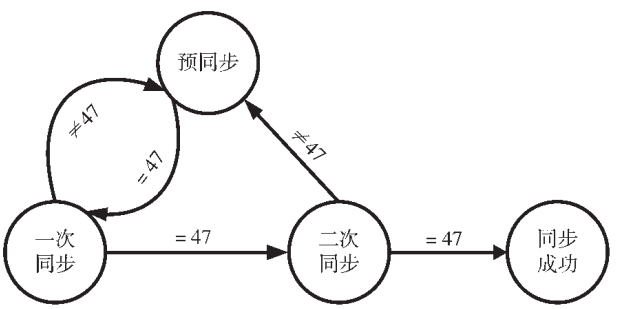

图 4 二次同步流程图

上述加密方法可以直接运用到 DTMB 系统中实现电视节目的加密传输。复用器或其他信源输出的 TS 流经过加密单元处理，处理后的加密数据不改变 TS 包结构，可以直接接入 DTMB 发射机中变成射频信号发出，射频信号经过 DTMB 接收机解调为加密数据，再经过解密单元还原成 TS 流。解密流程与加密流程一致，可硬件复用。信道传播过程中造成的错误不扩散，不会造成大面积解密失败。DTMB 系统加密传输的流程如图 6 所示。

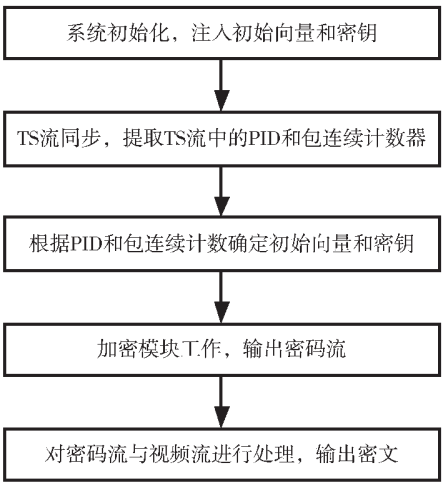

图 5 加密流程图

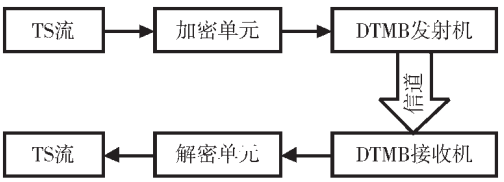

图 6 DTMB 系统加密传输流程图

2.3 性能对比

密码系统中，加密单元使用的密钥数量越多，随机性越强，加密强度越高。为了描述加密系统的性能，引入随机性因子的概念。将随机性因子定义为对密钥的变化处理从而生成的新的密钥数量。一个加密系统对密钥多级处理，会产生多个随机性因子，总的随机性因子为各级处理的随机性因子的乘积。在经过多次处理流程后，同一密钥可能会产生相同的输出，造成碰撞，故随机性因子往往大于密钥的实际数量。随机性因子可用来描述密钥的随机性，进而量化加密系统的性能。

以初始向量和密钥长度均为 128 bit，密钥存储器地址位宽 17 为例，TS 包中 184 B 可分成 12 个 128 bit 的分组单元。使用 ECB 加密模式，一个 TS 包可分配 12 个不同的密钥，后期不对密钥做任何处理，故随机性因子为 12。新型密钥分发机制和改进型 OFB 模式都对密钥进行二次处理，新型密钥分发机制中的交织器输入端会产生 2^{17} 种变化，输出端也会产生 2^{128} 种变化，随机性因子为 $2^{17}\times2^{128}$。同样，改进型的 OFB 模型也会增加 2^{128} 种变化，随机性因子为 2^{128}。各个不同组合模式的随机性因子对比如表 1 所示。

表 1 各种加密模式随机性因子对比

加密模式	随机性因子
普通 ECB 模式	12
新型密钥分发+OFB 模式	$2^{17}\times2^{128}$
新型密钥分发+改进型 OFB 模式	$2^{17}\times2^{128}\times2^{128}$

从表 1 中可以看出，基于新型密钥分发机制和改进型OFB 模式的加密方法相对于传统电子密码本 ECB 加密模式，在牺牲很小的硬件代价下，极大地增加了密钥随机性，大大提升了破解难度，具有很高的实用价值。

3 结论

本文提出的视频流加密方法创新性地引入了无线通信中常用的交织技术，提出了新的密钥分发管理机制和改进型 OFB 工作模式。相比传统加密方法，通过在多个环节引入交织器，极大地增加了随机性，最大程度实现一次一密原则，有效提升加密强度。同时，结合 TS 包结构自身特点，不破坏原有包结构，加密后的视频流能够无缝接入现有的无线图像和数字电视广播等传输系统中。本文的解密系统与加密系统架构一致，在某些场合可分时复用，节省硬件开支，密文在传播过程中的差错仅局限于自身，无扩散，不会造成大面积解密失败，具有很高的实用性。另外，本文提出的加密系统可以方便地引入并行结构，提高加密模块的吞吐量，解决目前人们对 4K、8K 等超高清视频的实时加密需求。

随着互联网和移动通信技术的发展，人们对视频等多媒体的需求越来越高，视频传输的安全性越来越成为一个严峻的问题。本文提出的视频流加密方法结构简单，加密强度高，兼容性广，在现实中有很高的实用价值，可被广泛应用于无线图像传输、网络监控和数字电视广播领域中。

参考文献

[1] 郑铸东.通过 aes-cbc 算法进行并行加密的方法及系统：中国，CN104284208A[P].2015-01-14.
[2] 潘必韬，聂小龙，王祖强.基于 FPGA 的 LFSR 异步加解密系统[J].电子技术应用，2016，42(6)：56-58.
[3] 王玉欣.MPEG-2 传输流复用器的 FPGA 实现[D].福州：福州大学，2010.
[4] 江磊，魏震楠，刘明.基于内外混合流水线的高吞吐率 AES 结构[J].电子技术应用，2015，41(6)：114-117.
[5] 朱坤崧，戴紫彬，张立朝，等.面向物联网的 SM4 算法轻量级实现[J].电子技术应用，2016，42(12)：27-30.
[6] 宋林琦，王军，潘长勇.DTMB 系统中解卷积交织的设计和实现[J].电视技术，2008(1)：33-35.
[7] SHANNON C E.Communication theory of secrecy systems. 1945[J].M.D.Computing：Computers in Medical Practice，1998，15(1)：57-64.
[8] 杨知行.地面数字电视国家标准 DTMB 技术解读[J].中国数字电视，2006(11)：30-33.

(收稿日期：2019-12-09)

作者简介：
范晶(1987-)，男，硕士研究生，工程师，主要研究方向：网络与信息安全。
贾旭光(1987-)，男，本科，工程师，主要研究方向：数字通信、信息安全。

版权声明