第 33 卷 第 9 期 计 算 机 工 程 2007 年 5 月
Vol.33 No.9 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)09—0137—03 文献标识码：A 中图分类号：TN918.4

一种加密变长码字并保持视频格式的加密方案

李 伟，徐正全，杨志云，姚 晔
(武汉大学测绘遥感信息工程国家重点实验室多媒体通信工程中心，武汉 430079)

摘 要：视频加密通常要求满足实时性和保持码流格式不变。而直接加密视频码流中的 DCT 系数和 MV 变长码字会产生非法变长码字从而破坏码流格式，不利于视频通信的正常应用。该文提出了一种加密 DCT 系数和 MV 变长码字并保持码流格式不变的方法。此方法同视频码流中定长码字的加密结合起来可以形成一个完整的视频加密方案，试验结果表明该方案满足视频通信实时性的要求并达到较高的保密级别。

关键词：视频加密；变长码字；格式兼容；多媒体安全

A Format-compliant VLC Codewords Video Encryption Scheme

LI Wei, XU Zhengquan, YANG Zhiyun, YAO Ye
(Multimedia Communication Engineering Center, State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430079)

【Abstract】 Efficient encryption in real-time and maintaining compliance to the syntax of video stream is the essential requirement of video security. Direct encryption of VLC codewords will usually not result in valid VLC codewords and so the encrypted video stream is not format-compliant. A scheme is proposed that DCT and MV VLC codewords are encrypted while stream format is preserved. The experimental results show that the proposed scheme combining with the encryption of FLC codewords such as INTRADC, sign bits of DCT and MV using secret key cryptography algorithm can meet the real-time constraint and provide high security level.

【Key words】 Video encryption; VLC codewords; Format-compliant; Multimedia security

由于视频信息具有海量特性，因此传统的把视频作为普通数据全部加密的方法计算量巨大，无法保证视频的实时传输。另一方面，视频加密如果破坏了码流格式，没有解密能力或者使用错误密钥的视频终端会产生解码死机现象。而且在视频点播和付费电视等商业应用场合，为了吸引用户购买，需要非授权用户能顺利解码密文码流来获取一定的视频信息。保持码流格式不变还可以允许直接对密文码流进行视频转码等处理，并有利于保持原始码流的容错性和网络适应性。因此视频加密需要同时满足视频的实时性和保持码流格式不变的要求。

视频压缩编码后码流中的 DCT 系数码字和运动矢量 MV 的码字代表了视频内容的几乎全部信息。而 DCT 系数和 MV 通常采用变长编码，对变长码字直接加密后得到的随机码字很可能是非法码字。例如对于 H.263 标准，如果 DCT 系数 TCOEF 变长码字值 110 加密后变成 011，则解码时在变长码表中搜索不到该码字而造成解码出错，所以如果直接对变长码字进行加密将破坏码流格式。本文针对这种矛盾提出了一种使用合法码字随机置换码流中 DCT 和 MV 变长码字以达到对其加密的保密方法，从而可以在加密变长码字的同时保持码流格式不变。将此方法同加密定长码字结合起来使用可以构成一个完整的视频加密方案。

1 现有保持视频格式的加密方案

Zig-zag置乱算法。用一个随机的置乱序列置乱DCT系数的Zig-Zag扫描顺序，从而达到加密视频图像的效果[1]，它被认为不够安全，另外这种方法显著增加了视频码流大小，减小了视频编码的压缩比。

加密符号位。包括仅加密I帧的DCT符号位的VEA算法[2]；除了I帧还要加密PB帧的DCT符号位和运动矢量MV的符号位的MVEA算法[3]；使用分组密码算法对DCT系数或运动矢量MV符号位进行加密的RVEA算法，它对每个宏块限定最多加密 64 个符号位[4]。加密符号位的方法计算量小，但是仅仅加密上述符号位不够安全，对于加密了上述全部符号位的视频码流，实验表明[5]，如果将帧内块DC符号位全部设置为某个常量(如 128)，即使其它DCT和MV符号位不解密，由于DC含有像素块的主要能量信息，仍可以看出图像的大致轮廓。

文献[6]提出了两种能够保持视频码流格式不变的加密方法：(1)将码表中变长码字与定长序号一一映射，将视频码流中的每个变长码字对应的序号组合起来使用公开密钥算法或者对称密钥算法进行加密，接着将加密后的序号通过码表映射成其它变长码字，然后将这些变长码字代替明文视频中原始码字就得到了被加密后的码流。作者仅给出了运动矢量变长码字加密的具体方法。这种方法采用公开密钥算法或对称密钥算法，保密性较好，但由于序号段数据量较大，其计算复杂度较高；(2)在保持结构信息(如起始码和标志字)不变的前提下，从码流空间位置上置乱压缩后码流的基本数据单

基金项目：湖北省科技攻关计划基金资助项目(2004AA101C18)；武汉市重点科技攻关计划基金资助项目(20031003021)
作者简介：李 伟(1979－)，男，博士生，主研方向：视频编码，多媒体通信与信息安全；徐正全，教授、博导；杨志云、姚 晔，博士生
收稿日期：2006-05-17 **E-mail：**williamlee@126.com

元。置乱单元可以是码字、8×8 块或者宏块。有时一个包可能只有几个宏块，那么以块或宏块为基本单元置乱时，置乱空间将非常有限，不利于安全性。

2 一种加密变长码字并保持格式不变的加密方案

基于现有的视频加密方案，特别是在文献[6]中对运动矢量变长码字序号加密方法的启示下，本文提出了一种计算复杂度较低的变长码字的加密方法。整个方案的基本框架主要由两部分组成：定长码字加密和变长码字加密。定长码字包括帧内块DC码字(INTRADC)、DCT系数符号位(TCOEF sign)和 MV 的符号位(MV sign)。变长码字则包括 DCT 系数码字(TCOEF code)和运动矢量码字(MV code)。其中定长码字加密采用某种分组密码算法(如 AES 或 IDEA)加密。变长码字加密的过程需要定长码字的参与，以利用定长码字的随机性来加密，以下是其加密思路和具体实现方法。

事先对不同长度变长码字预先定义不同的替换表，替换表中都是协议标准中规定的合法码字，用来采用某种方式随机替换码流中的变长码字。假设替换表中有N个码字($2^n = N$)，则表中每个码字可以分配一个长度为n(bit)的定长序号index。替换表中的码字长度需要等于或尽量接近被替换码字的长度，这样可以减少码字替换引起的对增加码流大小的影响。例如可以将所有的 2bits、3bits和 4bits的TCOEF码字组成一个替换表。这样对于码流中所有 2～4bits长度的变长码字code，可以通过查表得到它在该替换表中的序号index。如果改变该序号得到index’，也就在替换表中对应了一个相等或相近长度的变长码字code’。而由于序号是定长的，对其直接加密得到任意一个index’也都是有效的(对应一个符合标准的有效码字)，因此可以通过index’对应的一个任意码字code’来替换码流中的原始变长码字，从而达到加密的目的。

本方案提出的视频加密原理如图 1 所示。

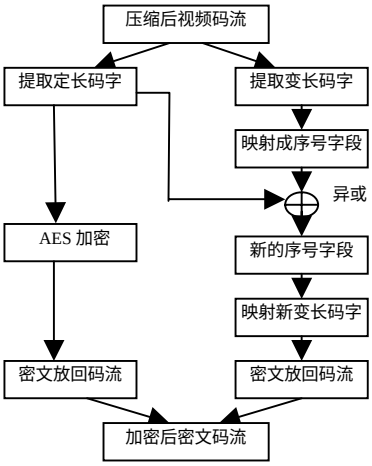


图 1 加密方案原理

加密步骤如下：

(1)从视频码流中逐一提取定长码字组成数据段 F 和变长码字组成数据段 V；

(2)将 V 中变长码字查找替换表一一映射成序号 index 并组合成序号数据段 I；

(3)将序号数据段 I 和定长码字数据段 F 异或，得到序号数据段 I’；当 F 字段长度小于 I 长度时，在 F 后循环连接 F 字段；

(4)将新序号数据段 I’中序号 index’一一映射成变长码字 code’得到数据段 V’；

(5)对定长码字数据段 F 使用分组密码算法(AES/IDEA)加密得到 F’；

(6)将加密后的定长码字和新的变长码字一一放回码流中相应位置即得到密文视频码流。

本加密方案具体的数据流程如图 2 所示。解密则是相反的过程。

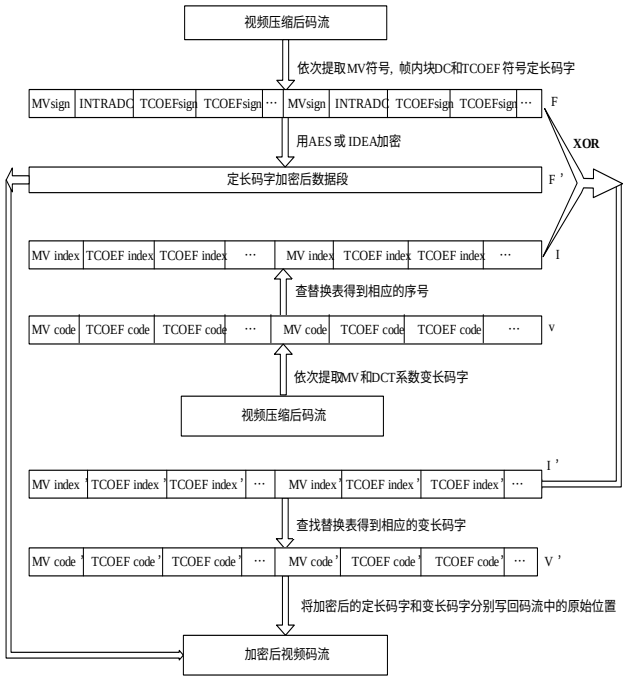


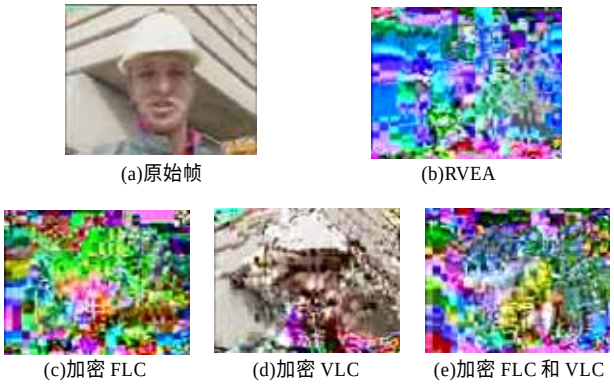
图 2 方案的具体流程

需要说明的是，使用本方案设计替换表时为保证码字替换后码流格式不变需要注意一些实际问题。以H.263 为例，TCOEF的变长码字是一个(LAST, RUN, LEVEL)的组合。LAST为 0 表示这个码字所在块中还有非零系数，为 1 表示这个码字就是所在块中的最后一个非零系数，即为该块的边界。RUN表示该码字前连续零系数的个数，一个块中所有码字的RUN的总和不应该超过 64。LEVEL是该码字表示的非零系数的大小。如果LAST为 1 的码字替换了LAST为 0 的码字，那么解码时会误判为块边界，造成码流格式解码出错。另外，如果将具有不同RUN值的码字相互替换，则会出现一个块中RUN的总和大于 64 的情况，同样会解码出错。因此设计替换表时，需要将不同LAST和RUN的码字放在不同的替换表中。对于LAST为 1 的码字也可以采取忽略的方法，即不予以进行替换加密。对于MV码字则不存在上述问题。另外设计替换表时需要尽量使码表中的码字个数N为 2 的幂($2^n = N$)，如果一些变长码字的某个集合中码字个数N不是 2 的整数次幂，那么可以将该集合划分成几个符合上述要求的替换表。例如可以将一个 6 个码字的集合划分成 2 个替换表，一个含 4 个码字，另一个含 2 个码字。

3 试验与结果分析

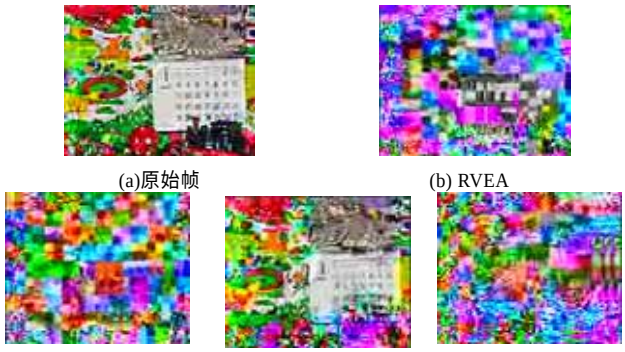
本方案在 H.263 的参考源码 TMN8 上实现了以下 4 种方案：(1)RVEA 方案，即对每个宏块最多加密 64 个 MV 和 TCOEF 符号位；(2)使用本文提出的方法仅加密变长码字(VLC)；(3)仅加密定长码字(FLC)，包括帧内块 DC 码字、TCOEF 和 MV 符号位；(4)本文提出的完整方案即同时加密 VLC 和 FLC。从图 3 和图 4 中可以看出，仅仅加密 VLC 是不足以置乱或加密整个视频图像的；RVEA 和加密 FLC 的加密效果较好；VLC 和 FLC 同时加密可以置乱整个视频图像，看不出任何内容信息。

从加密后视觉效果上看，RVEA 或仅加密 FLC 和本方案差别不大，但实际上由于本方案加密了代表视频内容主要信息的 VLC 码字，因此实质上其保密性相对仅加密 FLC 或 RVEA 要好得多。例如根据 DCT 系数分布的特性，容易找出密文码流中 TCOEF 和 MV 符号的位置。如果攻击者将这些符号位全部设为 0 或 1，如图 5 和图 6 所示，可以看出同时加密 FLC 和 VLC 按上述方法被攻击后的视频图像比仅加密 FLC 被攻击后的视频显露的信息要少。也就是说从攻击者的角度而言，本加密方案比仅加密 FLC 和 RVEA 加密或屏蔽了更多的信息。



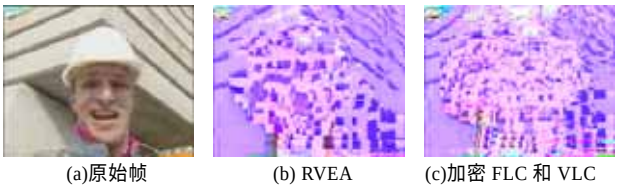
(a)原始帧　(b)RVEA　(c)加密 FLC　(d)加密 VLC　(e)加密 FLC 和 VLC

图 3 对 foreman 序列加密后第 17 帧效果



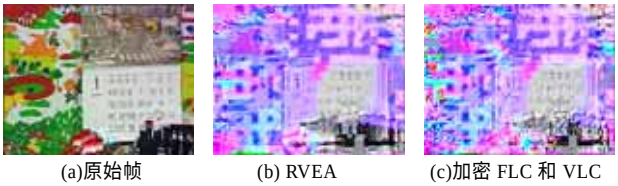
(a)原始帧　(b) RVEA　(c)加密FLC　(d)加密VLC　(e)加密FLC和VLC

图 4 对 mobile 序列加密后第 17 帧效果



(a)原始帧　(b) RVEA　(c)加密 FLC 和 VLC

图 5 视频码流 TCOEF 和 MV 符号位全置 0 后第 7 帧效果



(a)原始帧　(b) RVEA　(c)加密 FLC 和 VLC

图 6 视频码流 TCOEF 和 MV 符号位全置 0 后第 7 帧效果

除观察加密后的视频视觉效果外，衡量视频加密方案性能的 3 个主要尺度是：保密性，加密速度和对码流大小的影响。在保密性方面，首先由于对定长码字和变长码字都加密了，因此无论从加密的视频显示上还是视频内容的安全性上都具有较高的保密性。另一方面从攻击者的角度来看，本加密算法的保密性主要跟针对关键信息采用的密码算法的保密强度有关。如果采用国际标准的分组加密算法 AES，破解视频加密算法同破解 AES 算法的难度相当，而 AES 目前被公认是难以破解的。另外，要正确解密一帧视频图像需要对重建图像内容参与主观判断和分析，这也大大增加了攻击时间和难度。

对于加密速度，变长码字加密主要使用异或操作，计算量非常小，主要计算量集中在定长码字的分组加密上，而由于定长码字总共占码流的比例通常为 10%左右，本方案的计算量仅相当于全部加密的约 10%。表 1 列出了加密耗时与编码耗时比例和解密耗时与解码耗时比例，可以看出其加解密计算比重是比较小的，能够保证视频实时处理。

表 1 加解密与编解码耗时比

Sequence	Format	Time Ratio (encryption/encoding)	Time Ratio decryption/decoding
foreman	QCIF	1.07%	5.83%
mobile	QCIF	1.19%	6.76%
foreman	CIF	1.07%	7.21%
mobile	CIF	1.23%	7.85%

对于增加码流大小的影响，一方面加密定长码字不会影响码流大小，因为分组加密算法不改变加密数据的长度。另一方面对于加密变长码字，如果变长码字替换表内码字都是等长的则不会增加码流大小；如果替换表内码字不等长则会增加码流。因为根据变长编码的原理，实际码流短码字出现的频率较高，所以替换时变长码字大部分时候是被一个相对较长的码字替换。在 TMN8 的测试表明，对不同的序列码流大小增加的比例是变化的，但是如果设计替换表合理，增加的比例通常不会超过 25%。

4 结论

提出了一种能够保持码流格式不变的方法解决了视频码流中变长码字加密的问题，本方法结合加密码流中帧内块 DC、DCT 和 MV 符号位的加密方案，可以在保密性、计算复杂度和对码流大小影响 3 个方面到达一种平衡。本方案保持了码流格式不变，密文码流仍然可以被普通解码器顺利解码。本加密方案的软件实现仅有不到 2ms 的附加延时，完全可以满足视频编解码的实时性要求。

参考文献

1 Tang L. Methods for Encrypting and Decrypting MPEG Video Data Efficiently[C]//Proceedings of the 4th ACM International Multimedia Conference, Boston, MA. 1996: 219-230.

2 Shi C, Bhargava B. A Fast MPEG Video Encryption Algorithm[C]//Proceedings of the 6th ACM International Multimedia Conference. 1998: 81-8.

3 Shi C, Bhargava B. An Efficient MPEG Video Encryption Algorithm[C]//Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems. 1998: 381-386.

4 Shi C, Wang S Y. MPEG Video Encryption in Real-time Using Secret Key Cryptography[C]//Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, Las Vegas, Nevada, USA. 1999: 2822-2828.

5 Wu CP, Kuo C C J. Efficient Multimedia Encryption via Entropy Codec Design[C]//Proceedings of SPIE Security and Watermarking of Multimedia Content III. 1999.

6 Wen J, Severa M. A Format Compliant Configurable Encryption Framework for Access Control of Video[J]. IEEE Trans. on Circuits & Systems for Video Technology, 2002, 12(6): 545-557.