几种典型视频加密算法的性能评价

廉士国 孙金生 王执铨

(南京理工大学自动化系,南京 210094)

摘 要 视频加密对于保护视频数据的安全具有重要作用。将已有的几种典型 MPEG 视频加密算法,根据加密过程与压缩编码过程的关系不同,分为 4 类:完全加密算法,部分加密算法,DCT 系数加密算法和熵编码过程加密算法,并从算法的安全性、压缩比、计算复杂度和可操作性几个方面对算法的性能分别做了评价,给出了理论分析和实验结果;结合各类算法的特点,指出了它们各自适应的应用场合。

关键词 视频加密 MPEG 编码 密码 信息安全 密码分析

中图法分类号: TP309.7 TP391.41 **文献标识码**: A **文章编号**: 1006-8961(2004)04-0483-08

Quality Analysis of Several Typical MPEG Video Encryption Algorithms

LIAN Shi-guo, SUN Jin-sheng, Wang Zhi-quan

(*Department of Automation, Nanjing University of Science and Technology, Nanjing* 210094)

Abstract Video encryption is a suitable method to protect video data. In this paper, the existed MPEG video encryption algorithms are classified into four types according to the relationship between encryption process and compression process. They are complete-encryption algorithm, partial-encryption algorithm, DCT coefficient encryption algorithm and entropy encoding encryption algorithm. Each of them is evaluated from the four aspects: security, compression ratio, computing complexity and operationality. Theoretical analyses and experimental results are presented to compare these algorithms. And their application fields are given, which are consistent with their properties. According to the development direction of video application, the encryption algorithms combining with encoding process will be studied deeply in the future, such as DCT coefficient encryption algorithm, entropy encoding encryption algorithm or novel algorithm combining with error-correcting code and so on.

Keywords video encryption, MPEG encoding, cryptography, information security, cryptanalysis

1 引 言

随着计算机和网络技术的发展,图像、音频、视频等多媒体信息的应用也越来越广泛。尤其是分布式多媒体在视频点播系统、视频广播系统、视频会议系统和监视系统等方面的应用提出了对多媒体信息安全进行研究的要求。早期的安全方法主要依赖于权限控制,多媒体数据本身没有被加密,因此,在传输过程中很容易被窃取。针对这种情况,尤其是关系到军事、经济和政治敏感性的视频数据的保护,更有必要研究多媒体数据的加密算法。由于多媒体数据具有编码结构特殊、数据量大、实时性要求高等特点,传统的数据加密算法直接应用于多媒体数据,很难满足实时性要求,而且还会改变数据格式等,这就要求对多媒体数据采用特殊的加密算法。在近 10 年中,出现了许多视频加密算法。它们具有不同的安全性能,能够不同程度地达到实时性、保持压缩比不变、保持数据格式不变等要求。

目前常用的视频编码压缩算法有 MPEG[1]、H.26x[2]等,它们都是基于图像压缩方法 JPEG[3]的,压缩过程都是利用 8×8 DCT 变换或者小波变换来减小空间冗余度,并结合运动补偿来减小视频信号的时间冗余度,同时还会利用人类视觉特性将空间域数据变换到合适的颜色空间以降低冗余度。考虑到 H.26x 与 MPEG 在基本编码方法上有相似

基金项目:博士点基金(20020288025);江苏省自然科学基金(BK2001054)
收稿日期:2003-09-01;改回日期:2003-12-19

之处，仅以 MPEG-2 为例，简要介绍它们的编码格式。MPEG-2 视频由图像组(GOP)序列组成，每个 GOP 由一系列 I、P 和 B 图像帧组成。I 帧进行帧内编码，不依赖于其他帧；P 帧是通过前一个 I 帧或者 P 帧进行预测编码；B 帧是通过前面或者后面相邻的 I 帧或 P 帧进行双向预测编码。I 帧、P 帧和 B 帧间的预测依赖关系可参见文献[1]。其中，每一帧又被分为许多 16×16 点阵的宏块，I 帧中的宏块采用空间域编码方法，P 帧和 B 帧中的宏块根据相应的索引帧进行时间域互操作，即编码当前值和索引值之间的差值。不管帧的类型如何，每一宏块又被分为 4 个 8×8 的亮度块和 2 个 8×8 的色度块。空间域编码的每一个 8×8 块都要进行 DCT 变换、量化、行程编码和熵编码等操作，同 JPEG 中的变换域编码过程。而 I 帧中的宏块的 DC 系数和 B 帧、P 帧中的运动向量都要进行差分编码。最后通过熵编码(Huffman 编码或算术编码)，进一步压缩数据。整个编码过程如图 1 所示。

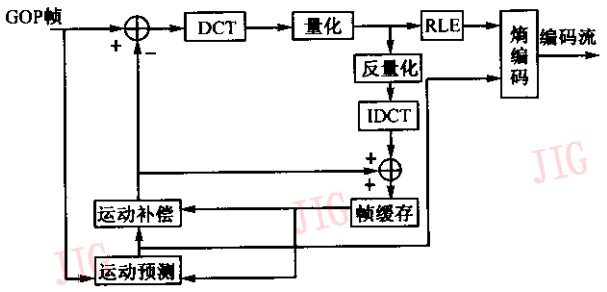

图 1 MPEG-2 编码过程

2 算法分类

根据加密过程与压缩编码过程关系的不同，如图 2 所示，MPEG 视频加密算法主要分为 4 类。其中 M 表示视频数据，E 表示编码加密后的视频数据，K 表示密钥。第 1 类，如图 2(a)所示，采用传统密码完全加密压缩过的码流，称其为完全加密算法，其中，加密过程与编码过程相互独立；第 2 类，如图 2(b)所示，采用传统加密算法对压缩过的码流部分加密，包括分层加密和分块加密等，称其为部分加密算法，其中，加密过程对压缩过的码流进行部分加密；第 3 类，如图 2(c)所示，在压缩编码过程中，加密敏感数据，常用的是加密 DCT 系数，称其为 DCT 系数加密算法，其中，加密过程位于压缩编码过程之中；第 4 类，如图 2(d)所示，将编码过程和加密过程

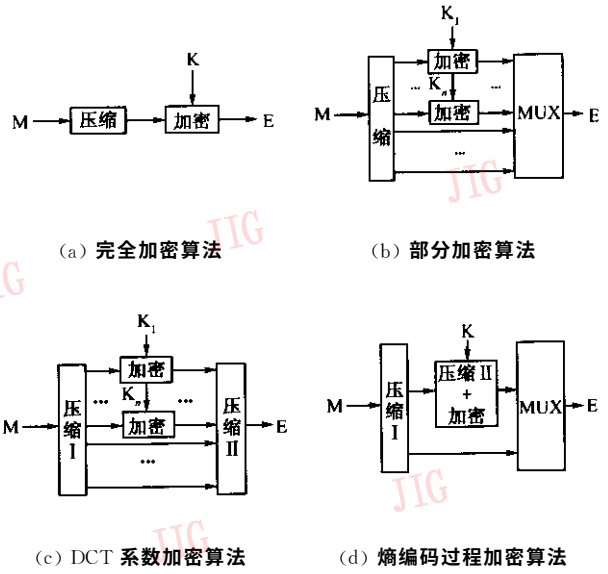

图 2 视频加密算法分类

结合，使用具有加密功能的压缩算法，在压缩的同时实现加密，通常是在熵编码过程中实现加密，称其为熵编码过程加密算法，其中，采用具有加密功能的压缩算法，将加密和压缩过程同步进行。

2.1 完全加密算法

完全加密算法不必考虑视频编码格式，将视频数据看作普通的二进制数据加密。最常用的完全加密算法是 VEA[4]视频加密方法，其是将明文块分成 $Odd=a_1a_3\cdots a_{127}$ 和 $Even=a_2a_4\cdots a_{128}$ 两半部分，将奇数部分 $Even$ 用 DES[5]算法加密得到密文的一半 $E(Even)$，同时另一半为明文块偶数部分 Odd 和奇数部分 $Even$ 按位异或的结果，即 $C=Odd\oplus Even=c_1c_2\cdots c_{64}$。这样，加密后的密文为这两半的拼结，即 $CE(Even)$。这种算法将加密复杂度降为接近原来的一半，同时保持了较高的安全性。将此方法作进一步扩展[6]，即将奇数部分 $Even$ 再分半，这样加密复杂度降为接近原来的四分之一。

一种混沌加密算法[7]，称其为 CSC 算法，采用斜帐篷映射、Logistic 映射、λ 映射等 3 种混沌映射构造混沌整数序列产生器，并将产生的序列与视频数据做异或运算，产生的结果即为加密的密文。此算法比传统的采用单一混沌映射的混沌流密码更安全，比 DES、IDEA 等块密码更快速。

2.2 部分加密算法

部分加密算法要考虑编码过程，选择较敏感的部分加密，常用的加密算法有分层加密算法和基于帧结构的选择性加密算法。一种适用于流格式视频

数据的分层加密方法[8,9],即使用传统的流密码加密视频数据的不同数据层,称其为 MSE 算法。可以采用密文反馈方式加密,以增强密码系统安全强度。

最基本的分块加密方法是基于 MPEG 的 IPB 帧结构的,即仅加密其中的 I 帧,因为从概念上讲,如果不知道相应的 I 帧,仅有 P 帧和 B 帧是没有用的,称这类算法为 MPE 算法。但是文献[10]中的实验表明,由于帧间的相关性和 P 帧、B 帧中有未加密的 I 块,所以仅仅加密 I 帧不能达到足够高的安全性。Tang 提出一种改进方法[11],此算法产生一种新的 MPEG 流,称作 SECMPEG,它将选择性加密和附加头信息结合到一起,可以使用两种传统的加密方法 DES 和 RSA 实现 4 个级别的安全性:(1)加密所有格式头信息;(2)加密所有的格式头信息和 DCT 的 DC 系数和较低层的 AC 系数;(3)加密 I 帧和 P 帧、B 帧中所有的 I 块;(4)加密所有数据。可见,这 4 个级别的安全性是由低到高递增的,但是 SECMPEG 并不能与标准 MPEG 相容。

2.3　DCT 系数加密算法

Tang[11]提出对 DCT 数据置乱的方法。MPEG 编码中使用二维 DCT 变换将空间域数据变换到频率域,减小数据的相关性,以实现压缩目的。置乱变换后的 DCT 系数方法,实现了加密的目的,称其为 DCW 算法。该算法包含以下几种方法:(1)保持直流系数(第 1 个系数)位置不变,其他系数间置乱;(2)置乱所有的系数;(3)将直流系数拆开,然后置乱所有的系数;(4)将许多块的直流系数一起加密,然后将直流系数拆开,并置乱所有的系数。这几种方法获得的安全性逐渐增加。但是能量的集中性并不等价于信息可理解性的集中性,因此,仅加密直流系数,并不能保证密文的不可理解性;而将 64 个 DCT 系数完全置乱,就违背了"之"形扫描的能量大小排列顺序,因此这会使得熵编码后的压缩比降低。

Tosum 等对其作了改进[12],将 64 个 DCT 系数按照频带划分为 3 段,可以根据安全性和压缩比要求的不同,对不同的段置乱加密,称其为 DCF 算法。因此,从安全性角度讲,每一段对应一种安全层或安全级:基础层、中间层和增强层。分层方法为(4,19),即第 1 层为 1～4 点,第 2 层为 5～18 点,第 3 层为 19～64 点。

加密 DCT 系数符号的方法[13],称其为 SE 算法,是将符号("0"表示正数,"1"表示负数)拼成比特流或数据段,然后使用随机产生的密钥流与其作按位的异或运算,将加密后的符号相应地赋回原数据中。加密 DCT 系数的符号和运动补偿向量的符号的方法[14],是将符号("0"表示正数,"1"表示负数)拼成比特流或数据段,然后使用私钥密码加密,将加密后的符号相应地赋回原数据。可以用 DES 或 IDEA 算法加密符号,这两种算法要求明文为 64 位,所以每次要获取 64 个符号。

2.4　熵编码过程加密算法

Wu 和 Jay Kuo[15,16]指出选择性加密不能保持压缩比不变,并提出了采用多种 Huffman 树的加密方法(MHT)。在使用熵编码的视频编码格式中,可以采用多种熵编码的统计模型,通过密钥控制模型的选择来实现视频编码过程中的加密。例如,MPEG 格式中使用了 Huffman 编码,标准格式中使用的是通过统计测试获得的标准的 Huffman 编码表。为了实现加密,可以选择其他不同的 n 个 Huffman 编码表作为基本的编码表,当然每个编码表与标准码表相比,不能造成太大的降质。对于一棵 Huffman 树,它的每个节点的 2 个子节点都可以置为"0"节点或"1"节点,这样,每个基本码表(Huffman 树)能够有 2^{m-1}(令 m 为树的叶子节点的个数,则树的内部节点的个数为 $m-1$)种变异树。这样总共有 $2^{(m-1)(n+1)}$ 种 Huffman 树可供选择。编码过程中可以通过密钥控制采用哪一种 Huffman 树,从而实现加密。

对于另外一种熵编码方法——自适应算术编码 QM,采用了编码与加密相结合的方法,称作多状态索引(MSI)方法。在 QM 编码过程中,二进制符号的统计概率是随着待编码的符号增加而动态改变的,并且最终通过查表方式获得。在算术编码中,每个状态都对应一个分段。MSI 方法通过随机选择多个状态的分段索引来实现加密[15,16]。这种算法的安全性以及改进方法已经得到很好的研究[17,18]。

3　算法性能要求

视频数据具有数据量大、冗余度高、实时性要求高等特点,为了满足视频的应用要求,视频加密算法在安全性、压缩比、计算复杂度和数据可操作性方面都要有一定的要求。

(1)安全性　安全性是数据加密的首要要求。对于视频加密,一般认为,当破译密码所需付出的代价大于直接购买视频版权所需的代价时,密码系统是安全的。因为视频数据也可以看作普通的二进制数

据，因此，传统的密码可以用在视频加密中。又因为视频数据具有数据量大的特点，破译者难免要对数据进行大量的解码操作，这将大大增加破译难度。因此，在保证安全性的情况下，一些特殊的、快速的加密算法也可以使用。

(2)压缩比　能够保持加、解密前后的数据量不变的算法，被称为具有压缩比不变性的算法。使用具有压缩比不变性的算法加密过的数据，在存储过程中不改变占用的空间，在传输过程中保持传输速度不变。因此，理想的视频加密算法应该具有压缩比不变性。但是，考虑到安全性、计算复杂度和数据可操作性等方面的要求，压缩比不变性一般不能够完全满足。

(3)计算复杂度　由于视频数据实时编解码、实时传输和存取的要求，加、解密算法的使用不能给编解码、传输和存取带来过大的延迟。因此，要求加、解密算法的计算复杂度低，以保持较高的加、解密速度，这样可以满足视频数据应用的实时性要求。

(4)数据可操作性　压缩编码后的视频数据，通常要求能够进行某些操作，如图像帧的定位、图像数据的剪贴和增删、视频数据的解码和播放、编码数据的码率控制等。如果某种加密算法加密后的视频数据，仍然支持某种数据操作，则称这种算法具有数据可操作性。其中，要保持图像帧的定位、图像数据的剪贴和增删，就要要求加密算法保持帧同步信息不变；要保持视频数据的解码和播放功能，就要要求加密算法保持所有的格式信息不变；要保持编码数据的码率控制功能，就要要求加密算法除了保持所有格式信息不变之外，还要支持码率控制功能。

4　算法性能评价

4.1 安全性

由于采用的加密原理不同，4 类算法分别具有不同的安全性。其中，完全加密算法 VEA 利用传统高强度块密码 DES 加密，DES 算法针对穷举攻击、只知密文、已知明文攻击和选择明文攻击的安全性使得视频加密系统具有较高的安全性。CSC 算法利用混沌流密码加密视频数据，其中的混沌流密码针对各种攻击具有较高的安全性，这种安全性保证了视频加密系统具有很高的安全性。

在部分加密算法中，分层加密算法(MSE)和分块加密算法(MPE)均采用传统高强度密码选择性加密压缩编码后的视频数据。其中的传统高强度密码是指通常应用于文本数据和二进制数据加密的密码，包括块密码(DES、IDEA、RSA 等)、流密码(直接加密方式、密文反馈方式)等，这些密码算法针对各种密码攻击均具有较高的安全性。但是，由于这类视频加密系统中，数据被部分加密，保持某些格式信息不变，这给利用数据编码原理进行攻击者提供了方便。因此，这类视频加密系统的安全性比完全加密算法低；与其他两类算法相比，其安全性较高。

DCT 系数加密算法是在视频压缩编码过程中加密 DCT 系数，利用解码过程导致的图像混乱实现加密。常用的方法是置乱 DCT 系数的位置和加密 DCT 系数的符号，如完全置乱算法(DCW)、分段置乱算法(DCF)和符号加密算法(SE)。对于穷举攻击和统计攻击，它们的安全性不同。首先，对于穷举攻击，这 3 种算法具有不同的加密空间。对于 DCT 系数置乱算法，令被置乱的系数总数为 $N(N\leqslant 64)$；对于分段置乱，令各分段为 $N_1,N_2,\cdots,N_m$，且 $N_i\neq 0(i=1,2,\cdots,m)$，$N_1+N_2+\cdots+N_m=N$；对于系数符号加密，令被加密的系数符号个数为 N，与置乱系数总数相同。则这 3 种算法的加密空间分别如表 1 所示(不考虑零系数)。

表 1　算法加密空间比较

加密算法	加密空间(不考虑零系数)
DCT 系数完全置乱	$N!$
DCT 系数分段置乱	$(N_1!)\cdot(N_2!)\cdot\cdots\cdot(N_m!)$
DCT 系数符号加密	2^N

其中，DCT 系数完全置乱的置乱空间大于分段置乱的置乱空间；DCT 系数分段置乱的置乱空间大于符号加密的加密空间。因此，对于穷举攻击，DCT 系数完全置乱算法的安全性最高，符号加密算法的安全性最低。对于统计攻击，由于 DCT 变换的能量集中特性，DCT 系数中低频系数的幅值通常大于高频系数的幅值，这给统计攻击提供了方便。尤其是完全置乱算法(DCW)和分段置乱算法(DCF)，在统计攻击情况下，安全性较低。对于符号加密算法(SE)，由于能量集中于低频的统计特点，可以通过破译少量低频系数的符号实现整个 DCT 块的破译。可见，与完全加密算法和部分加密算法相比较，DCT 系数加密算法安全性较低。

熵编码过程加密算法(MHT 和 MSI)，通过对编码模型的参数加密实现编码过程加密，它们的安全性依赖于模型参数的参数空间。其中，MHT 算法

通过增加原始的 Huffman 编码树来增加密钥空间，从而增加密码系统的强度。例如，对于 n 个 Huffman 基本编码表，每个基本码表（Huffman 树）能够有 2^{m-1}（m 为树的叶子节点的个数）种变异树，这样 Huffman 树的穷举空间为 $2^{(m-1)(n+1)}$。同理，MSI 算法通过增加算术编码的状态分段的随机选择空间来增加穷举空间，从而增加系统安全性。在已知明文攻击情况下，这类算法是不安全的。通过某些措施（如在密文中插入比特位、分段采用不同密钥等）能够增加其安全性，但它们仍然没有完全加密和部分加密算法的安全性高。

完全加密算法和部分加密算法不支持对密文直接进行解码和播放，图 3 所示仅给出了 DCT 系数加密算法和熵编码过程加密算法对视频片断的加密结果。可见，加密过的视频图像都混乱不可理解，这些加密算法都可以实现视频数据的安全保密功能。

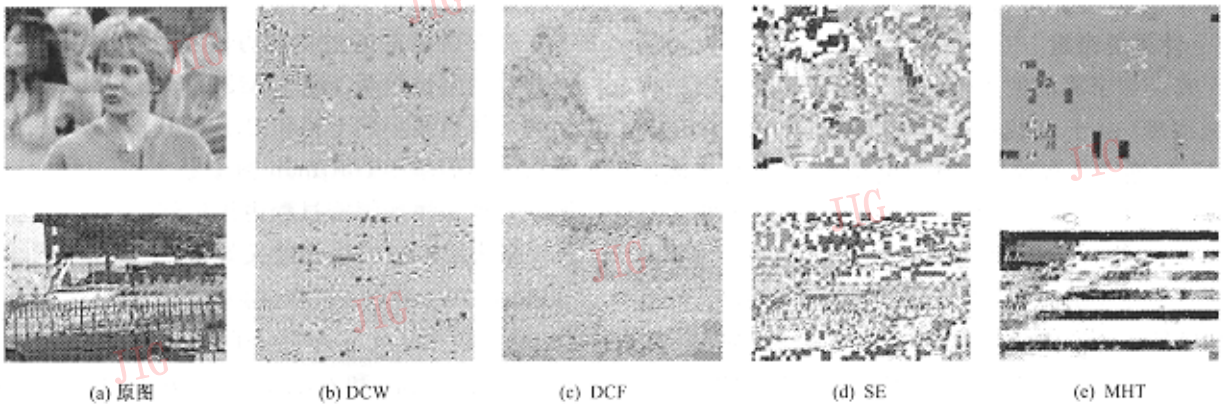

图 3　不同算法的加密结果

4.2　压缩比

4 类算法对压缩比具有不同的影响。其中，完全加密算法和部分加密算法是对压缩后的码流进行加密操作，因为采用的加密算法通常保持加密后数据量不变，因此，这两类算法不改变视频压缩过程的压缩比。

熵编码过程加密，是采用具有加密功能的熵编码方法，将编码过程与加密过程结合在一起，即在压缩过程中实现加密操作。这类算法因为要实现压缩功能，对压缩比的降质很小。例如，MHT 算法中，一般采用与最优 Huffman 树相近的多棵 Huffman 树以及它们的变异树作为基本码表。其中，每棵原始树和它的多棵变异树，对于相同的视频数据具有相同的压缩比；不同的原始树间，对于相同的视频数据具有不同的压缩比，但通过选择结构相近的 Huffman 树，可以尽量降低压缩比的差异。因此，整个 MHT 加密过程对压缩比的影响很小。对于 MSI 算法，通过减少随机状态分段的个数和分段的变化范围，也可以获得尽量小的压缩比改变。总之，熵编码过程对压缩比的影响很小。

DCT 系数加密算法，因为改变了 DCT 系数分布的统计特性，使得利用其统计特性进行压缩的压缩过程获得的压缩比有较大改变。其中，完全置乱算法（DCW）将 64 个系数在整个 DCT 块内置乱，从而会带来高频系数与低频系数的位置置换，会导致压缩比较大改变；分段置乱算法（DCF）利用系数幅值随着频率有规律变化的统计特点，将 64 个系数分成多个频率段，将系数分别在相应的分段内置乱，可以避免大系数与小系数的位置置乱，从而降低对压缩比的影响；符号加密算法（SE）仅改变系数的符号，而不改变其幅值，由于 MPEG 编码中 DCT 系数符号单独编码，因此，符号加密算法对压缩比的影响很小。

完全加密算法和部分加密算法不改变压缩比，DCT 系数加密算法和熵编码过程加密算法的压缩比变化率测试结果，如表 2 所示。

表 2　压缩比测试

单位：%

视频片断（I：P：B）	DCW	DCF	SE	MHT
bus(10：40：100)	35.7	20.6	5.5	3.7
bundy(8：35：81)	38.2	23.3	4.3	3.2
hulla(10：30：0)	32.4	17.5	6.1	3.3
car34(6：6：22)	30.1	15.7	5.6	3.9
flower(8：38：96)	34.3	20.7	5.8	3.8

表 2 中，DCF 算法的分段方式为（4，19），MHT 算法中基本 Huffman 树的个数为 $n=4$。并且，压缩比变化率 r 定义为

$$r=\frac{|r_{\text{compress}}-r_{\text{compress\_encrypt}}|}{r_{\text{compress}}}\times 100\%$$

其中，r_{compress} 表示仅仅进行压缩操作后的视频数据量，$r_{\text{compress\_encrypt}}$ 表示进行压缩和加密操作后的视频数据量。因此，r 反应了加密过程导致的压缩比改变量。从表 2 可见，DCT 系数完全置乱算法(DCW)和分段置乱算法(DCF)对压缩比的影响比较大，而 DCT 系数符号加密算法(SE)和多 Huffman 树加密算法(MHT)对压缩比的影响很小。

4.3 计算复杂度

完全加密算法使用传统高强度密码对视频数据完全加密，由于传统高强度密码(如 DES、IDEA、RSA 等)通常具有较高的计算复杂度，并且视频数据的数据量通常很大，因此，完全加密算法的计算复杂度很高。与完全加密算法相比较，部分加密算法选择加密部分视频数据，从而降低了加密的数据量，提高了加密系统的计算复杂度，具有较快的加、解密速度。

DCT 系数加密算法，采用置乱方法加密 DCT 系数，或者采用传统高强度密码加密 DCT 系数的符号。由于视频编码中，只有部分宏块进行 DCT 变换编码，其他宏块采用运动估计和运动补偿方式编码，因此，加密的数据量相对较少，尤其是符号加密算法，每个系数只加密一个符号位，并且，系数置乱算法的计算复杂度远比传统高强度加密算法的计算复杂度低。如果一个视频帧，含有的宏块总数为 C，进行帧内编码的宏块个数为 M，则进行 DCT 系数置乱和 DCT 系数符号加密时，加密操作的数据量占整帧数据的比例分别为 $\frac{M}{C}$ 和 $\frac{M}{8C}$。可见，DCT 系数符号加密方法加密的数据量比 DCT 系数置乱方法加密的数据量小。例如，对于 240×352 的视频图像，每一帧的宏块个数为 $C=330$，则帧内编码的宏块个数 M 的取值范围为 $[0,330]$。则可得，采用系数置乱方法时，平均每帧中被加密的数据量与原始数据量的比例 R 的取值范围为 $0\leqslant R\leqslant 1$；采用符号加密方法时，平均每帧中被加密的数据量与原始数据量的比例 R 的取值范围为 $0\leqslant R\leqslant 0.125$。即，当帧内宏块均采用帧间编码时($M=0$)，没有进行 DCT 系数加密的宏块；当帧内宏块均采用帧内编码时($M=330$，即为 I 帧)，加密的数据量比例最大，且分别为 1(系数置乱方法)和 0.125(符号加密方法)。在 MPEG-2 编码中，一般地，I 帧的数目远远小于 P 帧和 B 帧的数目，加密的数据量比例很小。可见，加密操作的数据量很小，整个密码系统的计算复杂度相对较低。因此，DCT 系数加密算法计算复杂度低，具有较高的加解密速度。

熵编码过程加密算法，通过密钥控制编码表的选择，它的计算复杂度等同于查表过程，其时间损耗主要是密钥的控制，其计算复杂度很低，因此，与其他算法相比较，它的计算复杂度最低。并且，此加密过程与压缩过程相结合，同步完成，这保证了算法的实时性。

表 3 所示是通过实验方法得到的各类算法加、解密速度测试结果。其中，MPE 算法采用 DES 密码加密视频数据中的 I 帧和 P、B 帧中的 I 宏块，MHT 算法采用的基本 Huffman 树个数为 $n=4$。并且，加、解密速度采用加解密过程占用编解码过程的时间比例 τ 来表示。时间比例定义如下：

$$\tau=\frac{|t_{\text{compress\_encrypt}}+t_{\text{decompress\_decrypt}}-t_{\text{compress}}-t_{\text{decompress}}|}{t_{\text{compress\_encrypt}}+t_{\text{decompress\_decrypt}}}\times 100\%$$

其中，$t_{\text{compress\_encrypt}}$ 和 $t_{\text{decompress\_decrypt}}$ 分别为加入加解密过程的编解码过程的时间消耗，而 t_{compress} 和 $t_{\text{decompress}}$ 分别为不含有加解密过程的编解码过程的时间消耗。可见，时间比例 τ 反应了加解密过程占用整个编解码过程的时间比例。τ 越大，说明编解码过程的计算复杂度越高；反之，越低。由表 3 可见，VEA 和 MPE 的加解密时间比例比较高，算法的计算复杂度高；而 DCW、SE 和 MHT 的加解密时间比例较小，算法的计算复杂度低。

表 3 加解密速度测试

单位：%

视频片断 (I：P：B)	VEA	MPE	DCW	SE	MHT
bus(10：40：100)	34.6	16.3	5.8	3.3	1.8
bundy(8：35：81)	29.7	13.5	4.9	3.1	2.1
hulla(10：30：0)	30.2	15.2	5.4	3.8	1.6
car34(6：6：22)	27.4	12.1	4.4	2.9	1.3
flower(8：38：96)	31.8	14.5	5.2	3.5	1.7

4.4 数据可操作性

将数据可操作性分为 3 类：位置索引、裁减、粘贴(保留帧同步信息)；解码、播放(保留所有格式信息)；编码率变换(保留所有格式信息，并且利于编码率控制)。可见，它们分别对应于数据格式的不同保持程度，这与算法的性质相关。

完全加密算法，因为将视频数据当作一般的二进制数据进行加密，没有考虑视频数据的数据格式问题，所以，其加密过的数据不支持以上任何操作。

完全加密算法不具有数据可操作性。

部分加密算法，包括分层加密算法和分块加密算法，一般考虑了视频数据的数据格式。例如，分层加密算法(MLE)按照视频编码的分层累进编码的特点，选择加密适当的数据层，因此，分层加密算法保持了数据编码的分层信息不变；分块加密算法(MPE)按照视频编码中以宏块、块组、帧、图像组为编码单位的特点，选择加密部分宏块或部分帧，能够保持视频数据的帧同步信息不变。这一特点决定了它们具有一定的数据可操作性：分层加密算法支持数据的编码率控制，分块加密算法支持数据的位置索引、粘贴、裁减等操作。

DCT 系数加密算法，仅仅置乱 DCT 系数和加密 DCT 系数的符号，不改变任何数据格式信息。因此，除了支持视频数据的位置索引、粘贴、裁减等操作外，还支持数据的解码、播放等操作，而且，置乱 DCT 系数的加密算法，仅仅改变系数的位置而保持其幅值不变，因此支持直接进行编码率控制。DCT 系数符号加密算法，如果采用的是直接加密方式的流密码，则支持直接进行编码率控制；如果采用的是块密码或密文反馈方式的流密码，则不支持直接编码率控制。

熵编码过程加密算法，仅仅加密 DCT 系数和运动信息，而保持所有的数据格式信息不变。因此，它支持数据的位置索引、粘贴、裁减等操作，但不支持编码率控制功能。

5　结　论

根据以上分析与比较，给出了各类算法的安全性、压缩比、计算复杂度和可操作性的评价，并给出其各自适应的应用范围，如表 4 所示。

表 4　视频加密算法性能比较

算法分类	算法举例	安全性	压缩比改变	计算复杂度	可操作性			应用范围
					位置索引、粘贴、裁减	解码、播放	编码率控制	
完全加密	VEA	高	不变	高	否	否	否	存储、高安
	CSC	高	不变	较高	否	否	否	全性传输
部分加密	MSE	较高	不变	较高	是	否	是	存储、实时
	MPE	较高	不变	较高	是	否	是	安全传输
DCT 系数加密	DCW	低	大	低	是	是	是	实时传输、
	DCF	低	较大	低	是	是	是	实时编解码、
	SE	低	小	低	是	是	是	窄带传输
熵编码过程加密	MHT	一般	很小	低	是	是	否	存储、
	MSI	一般	很小	低	是	是	否	实时传输

可见，各类算法因为其特点，而具有相应的适用范围。例如，完全加密算法因为其高安全性，很适合用于视频数据的安全存储；DCT 系数加密算法，由于支持编解码操作和编码率控制，而适合用于要求实时编解码的网络传输、窄带传输等。由于视频数据的大数据量特点，其安全性要求一般是攻击代价大于购买版权的代价，这种安全性要求使得与视频编码格式相结合的数据加密方法具有研究价值，并且，这类算法通常具有较低的计算复杂度，具有较强的数据可操作性，适合更广泛的应用。因此，这类算法将是未来研究的热点。

参 考 文 献

1　Committee Draft Standard ISO11172：ISO/MPEG90/176. Coding of moving pictures and associated audio[S].

2　ITU-T Rec. H. 263，Videocoding for narrow telecommunication channels at＜64kbit/s[S].

3　Wallace Gregory K. The JPEG still image compression standard [J]. Communisations of the ACM，1991，**34**(4)：30～34.

4　Qao L，Nahrstedt K. A new algorithm for MPEG video encryption [A]. In：Proceeding of the First International Conference on Imaging Science，Systems and Technology (CISST'97)[C]，Las Vegas，Nevada，1997：21～29.

5　NIST，Data encryption standard [S]. FIPS Publication 46-2，1993.

6　Tosun A S，Feng Wu-Chi. Lightweight security mechanisms for wireless video transmission [A]. In：Proceedings. International Conference on Information Technology：Coding and Computing [C]，Las Vegas，NV，2001：157～161.

7　Franco Chiaraluce，Lorenzo Ciccarelli，Ennio Gambi，*et al*. A new chaotic algorithm for video encryption [J]. IEEE Transactions on Consumer Electronics，2002，**48**(4)：838～844.

8　Wee S J，Apostolopoulos J G. Secure scalable video streaming for wireless networks [A]. In：Proceedings of the IEEE

International Conference on Acoustics, Speech, and Signal Processing[C], Salt Lake City UT, 2001,**4**:2049～2052.

9 Wee S J, Apostolopoulos J G. Secure scalable streaming enabling transcoding without decryption[A]. In:Proceedings of the IEEE International Conference on Image Processing[C], Thessaloniki, Greece, 2001,**1**:437～440.

10 Agi I, Gong L. An empirical study of MPEG video transmissions [A]. In: Proceedings of the Internet Society Symposium on Network and Distributed System Security[C], San Diego, CA, 1996:137～144.

11 Tang L. Methods for encrypting and decrypting MPEG video data efficiently[A]. In: Proceedings of the Fourth ACM International Multimedia Conference(ACM Multimedia'96)[C], Boston, MA, 1996:219～230.

12 Tosum A S, Feng Wu-Chi. Efficient multi-layer coding and encryption of MPEG video streams[A]. In:IEEE International Conference on Multimedia and Expo[C], New York, 2000,**1**: 119～122.

13 Shi Changgui, Bhargava Bharat. A fast MPEG video encryption algorithm[A]. In: Proceedings of the 6th ACM International Multimedia Conference[C], Bristol, UK, 1998:81～88.

14 Shi Changgui, Wang Shangyin, Bhargava Bharat. MPEG video encryption in real-time using secret key cryptography[A]. In: Proceedings of International Conference Parallel and Distributed Processing Techniques and Application [C]. Las Vegas, Nevada, 1999.

15 Wu Chunping, Jay Kuo C C. Fast encryption methods for audiovisual data confidentiality[A]. In: SPIE International Symposia on Information Technologies 2000[C], Boston, MA, USA, 2000,**4209**:284～295.

16 Wu Chunping, Jay Kuo C C. Efficient multimedia encryption via entropy codec design[A]. In:SPIE International Symposium on Electronic Imaging 2001[C], San Jose, CA, USA, 2001,**4314**: 128～138.

17 Lim J, Boyd C, Dawson E. Cryptanalysis of adaptive arithmetic coding encryption scheme[A]. In: Information Security and Privacy, Second Australasian Conference, ACISP'97[C]. Sydney, NSW, Australia, 1997:216～227.

18 Cleary J G, Irvine S A, Rinsma-Melchert I. On the insecurity of arithmetic coding[J]. Computers and Security, 1995,**14**:167～180.

廉士国 1978 年生，博士研究生。2000 年获南京理工大学信息工程专业学士学位，现于南京理工大学攻读博士学位。现主要研究方向为混沌密码学及多媒体加密。

孙金生 1967 年生，博士，副教授。1995 年毕业于南京理工大学。当前感兴趣的领域为容错控制理论与应用、网络拥塞控制、信息安全等。

王执铨 1939 年生，教授，博士生导师。1962 年毕业于哈尔滨军事工程学院。当前感兴趣的领域为信息安全技术、混沌控制与应用、大系统的容错控制理论与应用等。