精细粒度可扩展编码中基于 VOP 的基本层加密算法

文振[1], 袁 春[2], 张基宏[1]
(1. 深圳大学信息工程学院, 广东深圳 518060; 2. 清华大学计算机系, 北京 100084)

摘 要: 本文提出的细粒度可扩展编码中基于 VOP(video object plane)的基本层加密算法, 是利用 FGS(fine granularity scalable)压缩视频流的分层特点和 MPEG4 视频对象 VO(video object)编码原则, 结合改进的 C&S(chain and sum)加密算法, 通过提取并加密基本层 VOP 的关键数据, 包括形状、纹理、运动和全局背景等, 实现 FGS 整体流的加密. 本加密算法使加密数据流无需解密和加密操作就可支持网络节点的变换编码以适应带宽变化. 以 VOP 为单位的加密策略和改进的 C&S 加密算法的采用, 使媒体流丢包、位错等传输错误受到限制, 加密后的媒体流没有任何比特增加, 加密密钥的相应变化, 抵御了已知明文攻击. 通过对 MPEG 提供的三个序列 forman、akyio 和 carphone 以采样率为 3、处理帧数为 300 帧的测试, 测得 C&S, RC4 和 RC5 的处理速度分别约为 23.5, 64.5 和 42.7M 字节/每秒, 加密安全特性和混乱视觉效果十分理想.

关键词: FGS; 可扩展编码; 视频加密; 数字权力管理 DRM
中图分类号: TN919 文献标识码: A 文章编号: 0372-2112 (2008) 08-1547-05

VOP Based Base Layer Encryption Algorithm in Fine Granular Scalable Coding

WEN Zhen-kun[1], YUAN Chun[2], ZHANG Ji-hong[1]
(1. *College of Information Engineering, Shenzhen University, Shenzhen, Guangdong* 518060, *China*;
2. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: By using the leveled characteristics of fine granularity scalable (FGS) compressed video, the MPEG4 video object coding rules and the improved C&S(chain and sum), the base-level encryption algorithm, which is based on Video object plane (VOP) in Fine-grain extensible coding, retrieve and encrypt the key data, including shape, texture, motion and global background, of the base-level VOP to encrypt the FGS steaming. The algorithm supports the transform coding of the network node to adapt to the variation of the bandwidth without any encryption and decryption operations. The use of encryption in VOP unit and C&S algorithm effectively reduce the media stream package loss and transport errors. There is no size increment in the encrypted data steam and the variation of the encrypted key withstands the Known-plaintext attack. By the experiments on three series forman, akyio and carphone provided by Moving Pictures Experts Group (MPEG) in a sampling rate of 3 of 300 processing frames, the processing speed of C&S, RC4 and RC5 are 23.5, 64.5 and 42.7M b/s. The results also show a satisfying encrypted security and descrambled visual effect.

Key words: fine granularity scalable; scalable coding; video encryption; DRM

1 引言

MPEG-4 于 1998 年开始征集细粒度可扩展的视频编码方案, 用于流式服务中的编码标准 (MPEG-4: Streaming Profile), 它的基本思想是将视频编码成一个可以单独解码的基本层码流(Base Layer Bit-stream)和一个可以在任何时间点截断的增强层码流(Enhancement Layer Bit-stream), 其中基本层码流能够适应最低的网络带宽, 提供一个基本的图像质量, 增强层码流能够覆盖一定网络带宽变化的动态范围, 提供从基本层图像到无损失图像质量的细粒度增强. 经过 MPEG 测试和评比, 从编码效率和复杂性两方面的考虑, 从众多的方案中最终

收稿日期: 2007-11-19; 修回日期: 2008-03-26
基金项目: 国家自然科学基金(No. 60573132), 国家自然科学基金(No. 60503063). 深圳市项目(No. 200507)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

采纳了 W. Li[1] 等人提出的基于 DCT 变换系数的 FGS (Fine Granularity Scalable, 精细可伸缩性) 方案[2,3], 并于 2001 年成为精细粒度可扩展的视频编码标准: MPEG-4 FGS (Fine Granularity Scalability). [4]

随着扩展编码算法 MPEG-4 FGS 的出现, 给视频加密提出了新的要求, 在对 FGS 进行加密时, 要使码率控制操作能直接在加密的视频流上进行, 而无需进行解密/加密的操作以减轻中间阶段的处理负担, 并保证 FGS 加密后的细粒度性, 防止明文传输过程中的错位, 减少由于加密错误或包丢失所引起的 FGS 流恢复处理造成的负面影响, 都给 FGS 加密提出了全新的要求. Wee 针对 FGS 的安全性, 提出了一种可扩展流 SSS(Secure scalable stream)的加密算法[5], SSS 支持无需解密的变换编码, 通过简单切割或丢弃包来实现中间阶段的变换编码. 该算法对 FGS 除了头信息以外的基本层和增强层信息都进行加密, 用于指示扭曲率优化分割点的提示信息必须加入未加密的头信息中, 以便于传输的中间阶段在进行扭曲率优化下的码率剪裁处理. 其缺点是加密的粒度大小取决于视频打包的方式, 这就是说, 当 SSS 算法实施时, 包的大小必须事先知道, 一旦加密完成, 不允许进行包大小的变化.

Grosbois 等在文[6]中提出了一种针对 JPEG2000 图像压缩标准的可扩展的认证和访问控制机制. 算法首先计算基于块位流(code-blocks bit stream) 的哈希值, 加密后插入到视频流中, 这个哈希值作为密钥, 控制线性同余模运算, 生成伪随机序列, 根据随机序列的'0', '1'状态, 来决定对小波变换系数的高频子带部分的符号位进行翻转, 该方法采用分层加密策略以适应不同的需求, 还可利用 JPEG2000 的结构适应变换编码. 但是, 该算法必须在加密流中增加辅助的信息位来实现认证和访问控制, 同时加密方法中的同余模伪随机序列发生器的安全性不高.

2 精细粒度可扩展编码中基于 VOP 的基本层加密算法

由于 FGS 结构的特殊性, 增强层数据是由原始图象和重构图象的基本层中 DCT 参数的差值获得的, 如果基本层的图象数据不能重构, 增强层数据也就必然失去意义, 于是, 对整个流的加密可以简化到主要针对基本层的加密.

2.1 基本层加密算法信息结构

对于 MPEG4 基本层的加密, 必须考虑其视频对象模板 VOP(Video object plane) 的特性, 在 MPEG4 中, 一个景物被视为多个视频对象和其内在特性如形状、运动和纹理等信息的结合[7]. 这种基于内容信息的表达方式, 可以被利用作为选择合适的、并且是可操作的位流中码字的基础. 对这些信息的加密可以达到对整个 VOP 的安全保证[8,9]. 采用选择部分关键信息进行加密时, 被选择的压缩流内的 VLC 码字必须满足二个条件: 一是对图象的重构具有重要意义, 二是具有可确定的位置和长度. 基于 VOP 的基本层加密算法中的信息结构如图 1 所示.

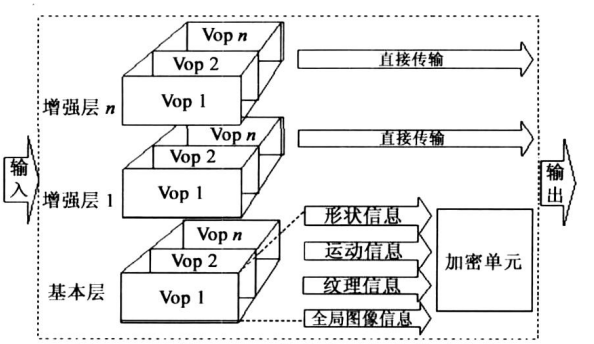


图 1 FGS 基于 VOP 的基本层加密算法结构

(1) 形状信息

形状信息用于构造一个视频对象, 实际上是构造一个 ALPHA 平面. 二值 ALPHA 平面是通过基于内容的算术编码构成的, 而灰度 ALPHA 平面是由 DCT 运动补偿编码的. ALPHA 平面是用一个矩形作为边界, 包含了视频对象模板的形状. 形状信息值包括矩形框的水平、垂直方向的象素个数和边角位置等信息.

(2) 运动信息

为了对每个 VOP 进行运动预测, 对于 VOP 边界上的块的运动估计必须由普通的块匹配变为多边形匹配. 这样就需要进行 VOP 尺寸变换和填充. 运动信息的放置有两种方式: 数据分割方式和混合方式, 前者每个宏块数据中的运动信息和纹理信息分开放置, 而后者的运动信息和纹理信息以每个宏块为单位混合放置.

(3) 纹理信息

纹理信息是图像的空间信息, 它反映了图像的灰度性质及其空间关系. 帧内 VOP 和运动补偿后的残差数据使用相同的 8×8 块 DCT 方法处理, 对于每个亮度和色度模板分别进行 DCT 变换. 当 VOP 为二值信息, 在对属于 VOP 形状的所有宏块进行处理时, 对于完全处在 VOP 内部的, 使用和 H263 完全相同的技术, 对于处于形状边界上的, 先要进行填充处理.

(4) 全局信息

全局信息是指视频片断中属于一个视频对象的所有可见象素的合成图象. 例如, 当摇动镜头时, 全局信息就包括整个序列中的前景和背景的可见象素. 背景的一部分也许在某帧图象中因为前景物体的遮挡而不可见, 全局信息可以用于直接重构背景的视频对象, 或者是背景视频对象的预测编码. 在某些文献中, 全局信息也被称为背景镶嵌.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2.2 基本层加密算法

算法的实现是基于 MPEG-4 校验模型版本 17 和 W3515 标准说明文档, 基于 VOP 的基本层加密算法系统是结合 C&S 算法理论, 有效地应用在 MPEG-4 FGS 基本层加密系统中. 基于 VOP 的基本层加密算法如图 2 所示.

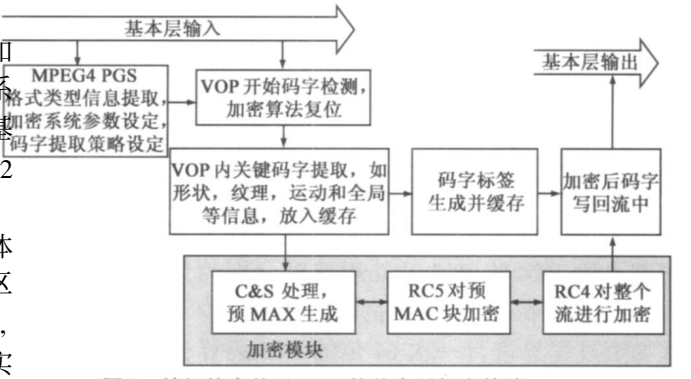


图 2　精细粒度基于 VOP 的基本层加密算法

算法首先会在 MPEG4 FGS 流的开始部分提取总体的格式信息, 以进行算法的初始化, 如参数设定, 存储区设定等, 然后, 以 VOP 为加密算法周期, 进行选择码字, 缓存标签, C&S 加密操作, 写回码率和系统复位. 具体实现时, 当一个 VOP_ start_ code 被检测到时, 相应的码字就开始被提取并依次放入到加密缓存中, 同时生成码字标签以记录被提取的码字长度和流中位置, 直到下一个 VOP_ start_ code 被检测到, 就开始对加密缓存中的数据进行 C&S 加密操作, 最后将加密后码字根据码字标签的信息逐个写回流中, 以保持流的格式兼容性. 对一个 VOP 的加密操作完成后, 算法复位, 开始下一个 VOP 加密周期的操作.

解密部分的实施, 除了加密模块部分被解密模块替代以外, 其它模块完全一致, 保证了加解密的对称性.

当整个帧被认为是一个 VOP 时, 对于 FGS 基本层的加密就和 MPEG1、MPEG2 格式兼容流的加密具有类似的特性, 也就是说该方法可以不做修改就可以扩展到 MPEG 兼容格式流的加密中, 对于每个 VOP 的加密是采用 C&S(chain & sum) 运算.

(1) C&S 加密运算

C&S(chain & sum) 加密运算由 Jakubowski 和 Venkatesan[10]最近提出, 主要是基于 CBC-MAC(块加密链_ 消息提取码) 的加密算法, 用于加密单元的加密运算. 根据安全和密钥的灵活性要求, 将预消息认证码 MAC 的加密算法由原来的 DES 变为 RC5. 该加密运算的关键思想是采用可逆的消息认证码来替代数据中的一部分, 然后将该消息认证码和服务密钥结合作为密钥, 对数据中的其它部分进行流加密, 如 RC4[11]. 由于消息认证码是可逆的, 加密处理后的数据如果没有比特错误, 可以通过逆运算得到原始的明文. 由于流加密的密钥取决于加密单元的服务密钥和被加密数据的哈希值, 使得加密的安全得到保证, 每个加密单元的安全性达到 2^{62}. 具体实现算法时, 采用 $Z_{2^{32}-1}$的有限域运算使其速度更快.

(2) 帧中的 VOP 加密

对于帧中的每一个 VOP, 根据上节的方法, 选择适当的码字, 放入加密存储区, 同时记录其在流中的位置和位长, 然后开始处理. 加密存储区的数据构成 n 个 l 位长的明文序列 $X=x_0, x_1, \cdots, x_n$, 其算法如图 3 所示.

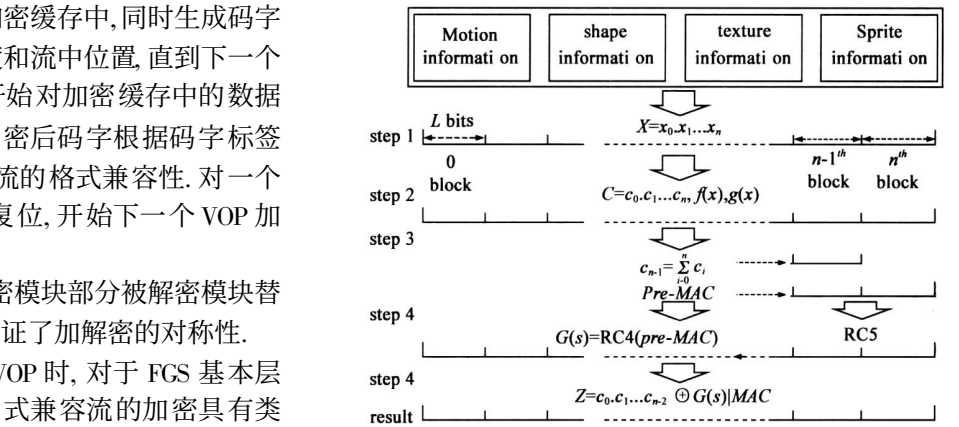


图 3　C&S 算法对于 VOP 的处理过程

算法过程:

(1) 计算 $C=c_0, c_1, \cdots, c_n$, 其中, $c_0=f(ex_0)$;

当 i 为偶数, 且 $i>1$ 时, $c_i=f(c_{i-1}+ex_i)$;

当 i 为奇数, 且 $i\geq 1$ 时, $c_i=g(c_{i-1}+e'x_i)$;

$$f(x)=ax+b,\ g(x)=cx+d.$$

(2) 替代 $c_{n-1}=\sum_{k=0}^{n} c_k$, 并且令 let $s=c_{n-1}c_n$, 称为预 MAC.

(3) 计算 $h(s)=RC5(s)$, 用 $h(s)$ 替代 $c_{n-1}c_n$.

(4) 计算 $Z=c_0, c_1, \cdots, c_{n-2} \oplus G(s)$, $G(s)$ 是一个伪随机序列, 由 RC4 产生, 密钥为预 MAC 值和全局密钥的哈希值.

(5) 将加密后的位流 Z 和 $h(s)$ 根据获取时的信息放回压缩流中.

(3) RC5 和 RC4 的安全性分析

这里, RC5-32/12/16 算法用来对预 MAC 进行加密, 在差分攻击下, 它的 2^{44}选择明文或 DES 的 2^{43}已知明文的攻击具有相同的安全性. RC5 的最大优点在于其参数化的运算, 具有可变的块大小, 可变的运算轮数和可变长度的密钥. 这就为实际使用提供了性能上和安全等级上的灵活选择.

RC4 是一种二进制加法流密码算法, 它使用可变长度密钥, 从 8 到 2048 位. 算法的核心部分是一个密钥流

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

的发生函数,产生的流序列和明文进行异或运算以获得密文.

3 实验结果

(1) 复杂度分析

实验采用了 MPEG 提供的三个测试序列, forman, akyio 和 carphone, 采样率为 3, 处理帧数为 300 帧. 实验得到 C&S, RC4 和 RC5 的处理速度分别约为 23.5, 64.5 和 42.7M 字节/每秒. RC5 的时间开销最少,这是由于每次加密过程只进行一次 64 位的 RC5 运算; RC4 也基本保持一致,这是由于其加密过程中除了初始化阶段,其他只对 C&S 处理后的数据进行异或运算; 而 C&S 运算的时间与明文数据大小(选择的码字位数总和) 成比例.

(2) 和其它视频加密方法的比较

表 1 是 MPEG4 FGS 基本层加密的位数和时间统计. 表 2 将本算法和其他三个典型的视频流加密算法进行了关键性能的比较.

表 1 MPEG4 FGS 基本层加密的位数和时间统计

流序列名称	全部加密时间(μsec)	加密位数	流的总长度(bits)	处理的位数(%)	平均处理时间(μsec/frame)
Foreman_qcif	8557.3	139026	1112475*8	0.0156	85.57
Akyio_qcif	7050.1	97485	1086527*8	0.0112	70.50
Carphone_qcif	2409	10155	1110016*8	0.00114	24.09

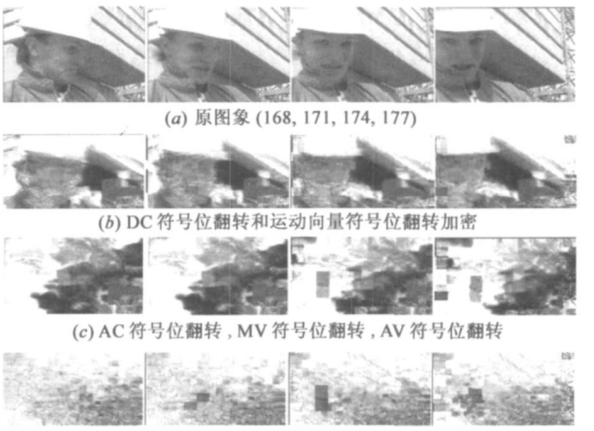
表 2 不同加密算法关键性能比较

性能参数	频域选择加密算法	VEA 视频加密算法	格式兼容加密算法	基本层加密算法
加密后比特增加	16% – 55%	Not entioned	8% – 17% (qcif)	0
对变换编码的支持	不支持	不支持	不支持	很好地支持
选择加密内容	MV 等重要码字的符号位, 同一片层下 DC, AC 的混排	除了同步码字以外的几乎所有数据	DCT 符号, 量化信息, 帧内编码的 DC, 和帧间的 MV	基本层中基于 VOP 的关键信息, 约占 0.01%
错误保护	支持	不支持	不支持	支持
加密算法	块混排, 随机符号位翻转	DES, IDEA	DES	C&S, RC4, RC5
安全性	中	高	中	高

(3) MPEG4 基本层加密的视觉效果

在 MPEG4 FGS 基本层加密算法中,采用了层次性加密策略,根据不同的安全性等级和接收端处理能力,加密的数据量不同. 加密的效果如图 4(*a*. *b*, *c*, *d*) 所示.

图 4(*a*) 是流序列 foramen 的第 168, 171, 174 和 177 帧原图象; 当 DC 进行翻转加密时, 图象的亮度和色度信号呈现混乱的视觉效果, 运动信息也出现混乱的运动效果, 但是宏块的纹理仍然明显, 如图 4(*b*) 所示; 当 AC 系数的符号位进行翻转加密时, 纹理变得模糊, 但是宏块间颜色差异明显, 运动信息也有少许暴露如图 4(*c*) 所示. 图 4(*d*) 显示经过 DC 和 MV 值加密和 AC 的符合位翻转加密, 获得了较平滑的模糊图象.



(*a*) 原图象 (168, 171, 174, 177)

(*b*) DC 符号位翻转和运动向量符号位翻转加密

(*c*) AC 符号位翻转, MV 符号位翻转, AV 符号位翻转

(*d*) DC 值、MV 值加密和 AC 符号位翻转

图 4 MPGE-4 FGS 基于 VOP 的基本层加密算法效果图

4 结论

针对目前相关方法存在的问题如: 加密运算复杂, 安全性具有缺陷, 尤其是在支持异构网络环境下的变换编码技术方面存在诸多不足, 本文提出的"精细粒度可扩展编码中基于 VOP 的基本层加密算法" 很好地解决了这些问题.

该算法充分利用 MPEG4 FGS 的压缩视频流的特点, 采用了改进的 C&S 综合加密技术, 将 RC4 和 RC5 结合到算法中, 实现基于 VOP 的加密运算. 该方法的优点在于加密后的压缩视频流无需任何附加的比特信息, 很好地支持异构网络节点的变换编码操作, 只需要加密很少的视频数据就可以达到很好的加密安全特性和混乱的视觉效果, 基于 VOP 的加密单元使错误受到限制, 防止了错误扩散, 综合的加密算法保证了整个系统的安全性.

参考文献:

[1] Weiping Li. Overview of fine granularity scalability in MPEG-4 video standard[J]. IEEE transactions on circuits and systems for video technology, 2001, 11(3): 301– 317.

[2] Qi Wang, Feng Wu, Shipeng Li, Yuzhuo Zhong, Ya-Qin Zhang. Fine-granularity spatially scalable video coding [A]. IEEE Int'l Conf on Acoustics, Speech and Signal Processing (ICASSP'2001) [C]. Salt Lake City, 2001. 1801– 1804.

[3] Kalluri R. Fine granular scalability for H.26L-based video streaming[A]. International Conference on Consumer Electron-

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

ics (ICCE)[C]. Auckland, New Zealand, 2002. 346- 347.

[4] 刘元超,李永全. MPEG-4 精细可扩展性视频编码技术研究[J]. 信息技术, 2006, (03): 40- 42.
Liu Yuan-chao, Li Yong-quan. Research on FGS video coding technology based on MPEG-4 [J]. Information Technology, 2006(03): 40- 42. (in Chinese)

[5] Susie J, Wee S J, Apostolopoulos J G. Secure scalable streaming enabling transcoding without decryption [A]. Proc IEEE Int Conf Image Processing [C]. Thessaloniki, Greece: PIEEE, 2001. 1. 437- 440.

[6] Raphael Grosbois, Pierre Gerbelot, Touradj Ebrahimi. Authentication and access control in the JPEG 2000 compressed domain [A]. Proc of the SPIE 46th Annual Meeting: Applications of Digital Image Processing XXIV [C]. San Diego, 2001. 8. 95- 104.

[7] 张连发,叶娇阳. MPEG-4 FGS 架构的视频编码器的研究与应用[J]. 计算机工程与应用, 2005, (25): 99- 101.
Zhang Lian-fa, Ye Jiao-yang. Research and application of FGS architecture video encoder[J]. Computer Engineering and Applications, 2005, (25): 99- 101. (in Chinese)

[8] Yeongyun Kim, Sung ho Jin, Tae Meon Bae, Yong Man Ro. A selective video encryption for the region of interest in scalable video coding [A]. 2007 IEEE Region 10 Conference [C]. Taipei, Taiwan: IEEE TENCON. 2007. 1- 4.

[9] 朱红,吴成柯,方勇. 基于 H.264 的自适应选择增强 FGS 视频编码[J]. 电子学报, 2005, (12): 2204- 2208.
Zhu Hong, Wu Cheng-ke, Fang Yong. Adaptive selective enhancement FGS video coding based on H. 264[J]. Acta Electronica Sinica, 2005, (12): 2204- 2208. (in Chinese)

[10] Mariusz H Jakubowski, Ramarathnam Venkatesan. The Chain & Sum Primitive and Its Applications to MACs and Stream Ciphers[J]. EUROCRYPT, 1998: 281- 293.

[11] Mantin I, Shamir A. A practical attack on broadcast RC4[A]. Proc. Fast Softwar encryption 2001[C]. Yokohama, Japan: Springer-Verlag, 2001. 152- 164.

作者简介:

文振　男,1962 年 3 月出生于广东信宜. 清华大学计算机科学与技术专业毕业, 工学硕士, 现为深圳大学信息工程学院软件工程系副教授, 软件工程系系主任, 主要研究方向为流媒体编码、基于内容视频检索.
Email: wenzk@szu.edu.cn

袁　春　男, 1969 年出生于江西景德镇, 2002 年毕业于清华大学计算机系, 获博士学位. 2003 年至 2004 年于法国国家信息和自动化研究院(INRIA) SMIS 项目组担任博士后研究员. 现在清华大学深圳研究生院信息学部任教. 主要研究方向为安全媒体信息系统、媒体流网络应用安全访问控制、安全数据库等.

张基宏　男, 1964 年 6 月出生于江苏海安, 东南大学无线电专业毕业, 博士学位, 现为深圳大学教授, 信息学院院长. 主要研究方向为图像编码、矢量量化和模糊逻辑.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net