

文章编号:1001-9081(2014)06-1671-05

doi:10.11772/j.issn.1001-9081.2014.06.1671

## 适用于移动通信视频点播的感知加密算法

郭雨, 柏森\*, 郭辉, 唐鉴波

(应急通信重庆市重点实验室(重庆通信学院), 重庆 400035)

(\*通信作者电子邮箱 [baisencq@126.com](mailto:baisencq@126.com))

**摘要:**在视频点播(VOD)应用中,为刺激用户购买高质量的视频版本,往往希望播放的加密视频仍可部分感知,这就是所谓的“感知加密”,因此,需要研究特别的加密算法对视频进行加密。针对目前适用于移动通信视频点播的H.264视频感知加密算法较为缺乏的问题,提出了一种基于祖冲之(ZUC)算法和压缩感知(CS)的视频加密算法。首先利用ZUC构建随机测量矩阵,之后利用测量矩阵对量化后的离散余弦变换(DCT)系数进行测量,并将测量值作为新的量化后的DCT系数进行编码,使新的系数与原始系数不同,从而实现加密。最后定义了良好的感知加密算法应具备的特征。实验结果表明,该算法对视频的压缩码率影响较小,具有较低的时间复杂度,并且算法对密钥变化敏感,有较好的感知安全性。

**关键词:**视频加密; 感知加密; 压缩感知; 祖冲之算法; H.264

中图分类号: TN919.81 文献标志码:A

### Perceptual encryption algorithm for mobile communication VOD application

GUO Yu, BAI Sen\*, GUO Hui, TANG Jianbo

(Chongqing Key Laboratory of Emergency Communication (Chongqing Communication Institute), Chongqing 400035, China)

**Abstract:** In Video-On-Demand (VOD) applications, it is desired that the encrypted multimedia data are still partially perceptible after encryption in order to stimulate the purchase of the high-quality versions of the multimedia products. This perceptual encryption requires specific algorithms for encrypting the video data. Due to lack of H.264 video perceptual encryption algorithms for mobile communication application, a video encryption algorithm based on ZU Chongzhi's (ZUC) algorithm and Compressive Sensing (CS) was proposed. First of all, ZUC algorithm was utilized to construct a random measurement matrix. Then the quantified Discrete Cosine Transformation (DCT) coefficients were measured by measurement matrix, and the measured values were regarded as new quantified DCT coefficients to encode, which realized the encryption by using the difference between original and new coefficients. Finally, the characteristics of a good perception encryption algorithm were defined. The experimental results show that the proposed algorithm has little effect on video compression bit rate with low time complexity, and it is also sensitive to key change with good perceptual security.

**Key words:** video encryption; perceptual encryption; compressed sensing; ZU Chongzhi's (ZUC) algorithm; H.264

### 0 引言

随着4G通信的试点运营,移动互联网迎来崭新的时代,移动通信已成为人们生活娱乐中必不可少的一部分。目前手机视频点播业务的更新速度已与互联网视频点播业务同步,人们可以随时随地观看最新的视频内容。然而如何在付费视频点播业务中,既保护视频的安全性,使他人无法未经许可地复制和传播视频,又使未付费用户可以粗略地观看视频内容从而决定是否付费,成为手机付费业务视频点播中的研究热点。因此,研究一种适用于移动互联网的视频点播的感知加密方案具有较好的应用前景。移动通信的视频点播的感知视频加密方案因设备、带宽、蓄电量等条件限制具有以下特点:一是视频点播业务是为了防止未经许可的复制和传播视频,因此必须具有较好的感知安全性,即未经许可的用户只能模糊地浏览视频的概貌,无法清晰地浏览视频的全部内容;二

是因移动通信受带宽和手机等移动设备的运算速度、蓄电量的限制,感知加密算法必须对视频的码率影响小,且算法复杂度要低,以节约珍贵的移动通信带宽和移动设备的蓄电量;三是感知加密后的视频仍然能够被标准解码器解码,即感知加密视频具有语义和编码兼容性<sup>[1]</sup>。

文献[2]针对目前现有的H.264视频加密算法作了分类,将H.264加密算法分为在H.264编码之前加密、帧内预测模式加密、帧间预测模式加密、运动矢量加密、残差系数加密、离散余弦变换(Discrete Cosine Transform, DCT)后的系数加密等,并对每类加密算法的优缺点作了详细的分析,指出哪些算法可用于感知加密,哪些算法不能够用于感知加密。文献[1]提出了一种MPEG视频编码标准的感知加密的算法,分别加密帧内直流(Direct Current, DC)系数、帧间非零DC系数的符号和运动矢量,该算法具有较快的加密速度和良好的感知加密效果,能够抵抗已知密文分析和已知明文分析,有较

收稿日期:2013-11-22;修回日期:2014-01-15。 基金项目:国家自然科学基金资助项目(61272043);重庆市基础与前沿研究计划项目(cstc2013jjB40009);重庆高校创新团队建设计划项目(KJTD201343)。

作者简介:郭雨(1989-),男,内蒙古呼伦贝尔人,硕士研究生,主要研究方向:图像/视频加密;柏森(1963-),男,四川达州人,教授,博士,主要研究方向:信息隐藏、信息加密、数字水印;郭辉(1982-),男,河南辉县人,硕士研究生,主要研究方向:信息隐藏、信息加密。

高的安全性。文献[3]提出基于移动通信的 H.264 感知加密方法,文中加密宏块块编码模式(Coded Block Pattern, CBP)、拖尾系数的符号和非零系数的幅值,其优点是具有算法复杂度低、对码率影响小、加密速度快等优点,作者虽说此算法具有较高安全性,但是没有给出相应的安全性分析或者实验数据。文献[4]是通过同时对帧内预测模式(Intra Prediction Mode, IPM)、运动矢量差、DCT 残差系数以不同的强度加密实现感知加密的,其优点是可以取得较好的加密效果和具备较高的安全性。文献[1,3~4]都是通过将多种参数同时加密来取得较高的加密效果和保证较高的安全性,然而需要加密的数据量仍然偏大。文献[5]通过改变每个 DCT 蝶形运算的算子的权重系数,使其产生的系数与标准的 DCT 系数不同,从而实现对 H.264 视频感知加密;虽然可以取得较好的感知加密效果和具有较高的安全性,然而这样必须对标准解码器进行修改,否则不能够正常解码加密后的视频,即此加密算法不具备编码兼容性。文献[6]在文献[5]的基础上,根据 MPEG-4 视频编解码算法不同于 H.264 视频编解码算法的一些特点作了相应的修改,将 H.264 视频感知加密算法移植到 MPEG-4 中,其具备的优缺点也与文献[5]相同。

本文结合文献[7]提出的基于压缩感知(Compressed Sensing, CS)的 H.264 感兴趣区域加密算法和 4G 国际通信长期演进(Long Term Evolution, LTE)的加密标准算法——祖冲之(ZU Chongzhi's, ZUC)算法,提出了一种适用移动通信视频点播的 H.264 视频感知加密算法。加密时,首先根据密钥,利用 ZUC 算法产生二值序列;然后,利用二值序列构建随机测量矩阵,并对矩阵进行正交化,降低矩阵列向量之间的相关性;最后,利用正交化的测量矩阵对含有残差系数宏块的量化后的 DCT 系数进行测量,并将测量值作为新的量化后的 DCT 系数进行编码,由于新的系数与原始系数不同,从而实现加密。与其他文献相比,本文算法具备编码兼容性,不需要对解码器进行相应的修改即可读取加密后的视频码流;同时,本文只对单一的 DCT 系数进行加密,将压缩感知的测量值作为新的 DCT 系数进行编码传输,比采用高级加密标准(Advanced Encryption Standard, AES)等算法对 DCT 系数进行异或加密等方法安全性更高,使得传统的密码分析手段失去作用。

## 1 ZUC 算法与压缩感知算法

### 1.1 ZUC 算法的安全性及其在图像加密中的应用

ZUC 算法是我国自主研发的第一个被国际密码标准收录的加密标准,现已被第三代合作伙伴计划(3rd Generation Partnership Project, 3GPP)确定为 4G 国际通信 LTE 的国际标准中的加密标准。ZUC 算法分为三个逻辑单元,在算法的线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)设计中,首次采用素域  $GF(2^{31}-1)$  的  $m$  序列,该序列周期长、统计特性好,具有线性结构弱、比特关系符合率低等优点,因此 ZUC 算法具有较强的抵抗二元域上密码攻击方法的能力<sup>[8]</sup>。文献[9]提出了基于“16 比特半字”的猜测决定攻击,其计算复杂度为  $2^{392}$ ,证明了 ZUC 算法的内部状态规模小于 SNOW3G,在抵抗猜测决定攻击方面,ZUC 明显优于 SNOW3G,有较高的安全性,能满足加密文本、图像和视频的安全性需求。文献[10]探讨了利用 ZUC 算法对图像进行加

密的可能性,该方案利用 ZUC 算法产生的流密钥序列对待加密图像的每个像素逐个异或加密。由于图像数据量巨大,在未结合相应的压缩方案直接在空域对图像像素值进行加密虽然可以取得良好的加密效果,但是需要加密的数据量大,且加密图像仍需占用较多存储空间,不便于网络传输。

### 1.2 压缩感知算法在图像和视频加密中的应用

压缩感知算法是基于信号的稀疏性,不需要通过对原始信号进行采样就可以获得有用信号,从而突破了传统的香农定理对于信号采样带宽的要求。压缩感知算法应用十分广泛,在图像和视频处理、数据压缩、信息论、大气、地质等领域具有重大应用意义。文献[11]对压缩感知算法作了详细的理论推导和介绍,并分析了现在压缩感知算法的研究难点和热点,最后探讨压缩感知从稀疏约束到低秩约束优化的发展历程。由于视频编解码有着一些不同于图像的特点(例如帧间预测、帧内预测、运动估计等),目前研究基于压缩感知的视频编解码算法较少。文献[12]提出了一种基于压缩感知的图像加密算法,首先使用随机测量矩阵对图像经 DCT 后的系数进行测量,将测量值作为新的 DCT 系数;之后利用 LFSR 生成密钥序列,对随机测量矩阵进行平移加密,从而达到对图像进行加密的目的。文献[13]提出一种鲁棒性强的基于压缩感知的图像加密算法,首先对图像进行 DCT 并量化,之后利用 Gaussian 随机矩阵对量化后的 DCT 系数进行测量,并对测量值使用 Arnold 进行置乱加密,同时利用 Logistic 混沌序列产生的二值序列对测量值按位异或加密,此加密算法虽然安全性较高,但较为复杂,且随机矩阵也需要通过信道传输给解码端,增加了信道的负担。

## 2 基于 CS 和 ZUC 算法的 H.264 视频加密算法

残差系数经 DCT 并量化后的系数(Quantized Coefficient, QC)对重建视频的质量有着较大的影响,可以通过改变 QC 实现对视频的加密。由于 QC 本身已是稀疏信号,因此可以直接使用测量矩阵对 QC 进行测量,省略了对原始视频帧的稀疏化过程。使用测量矩阵对 QC 测量后的测量值作为新的 QC,相当于改变了 QC 值,从而达到加密的目的。本加密算法由三部分组成:利用 ZUC 算法构建随机测量矩阵;利用测量矩阵对 QC 进行采样测量;对测量值在熵编码之前进行预处理,使其能够满足 H.264 编解码标准。

### 2.1 构建测量矩阵

测量矩阵的好坏对重建信号质量有着较大的影响。本文结合文献[14]思想构建随机正交测量矩阵,并使用文献[15]方法对随机测量矩阵进行优化,以获得更好的重构效果。

Step1 设待生成的测量矩阵  $\varphi \in \mathbb{R}^{M \times N}$  ( $M \leq N$ ),将  $\varphi$  初始化为零矩阵。使用 128 比特二值序列 Key 作为 ZUC 算法的密钥序列和初始向量,构建  $M \times N$  的矩阵为  $A = [a_0, a_1, \dots, a_k, \dots, a_{N-1}]$ ,其中  $a_k$  ( $k = 0, 1, \dots, N-1$ ) 是由 ZUC 算法生成  $M$  比特的二值列向量。

Step2 将  $\varphi$  按列向量的表达形式为  $\varphi = [x_0, x_1, \dots, x_k, \dots, x_{N-1}]$ ,其中  $x_k$  ( $k = 0, 1, \dots, N-1$ ) 为  $M$  维的列向量。将  $a_k$  与  $x_k$  一一对应,若当前  $a_k$  的元素值为 1,则将对应位置的  $x_k$  的值设为 1,直到  $x_k$  中有  $K$  值为 1。如式(1)所示:

$$x_{ki} = \begin{cases} 1, & a_{ki} = 1 \text{ 且 } \sum_{j=1}^i a_{kj} \leq K \\ 0, & \text{其他} \end{cases} \quad (1)$$

其中: $x_{ki} \in \mathbf{x}_k; a_{ki} \in \mathbf{a}_k; i = 0, 1, \dots, M - 1$ 。

Step3 按照文献[15]方法,将 $\varphi$ 的列向量进行 Schmidt 正交化,得到用于对 QC 进行测量的测量矩阵 $\varphi$ 。

## 2.2 对 QC 进行测量

为了提高计算效率和减小对码率的影响,在进行测量时,选取一个宏块单位(即 $16 \times 16$ 个系数)的 QC 进行测量和计算。具体测量步骤如下:

Step1 若当前 CBP 值为 0,即当前宏块无亮度残差系数,则不对当前宏块进行测量;若 CBP 值不为零,则对当前宏块进行测量。

Step2 设当前待测量宏块的 QC 向量为 $\mathbf{Q} \in \mathbb{R}^{16^2}$ ,按式(2)测量:

$$\mathbf{Q}_M = \varphi \mathbf{Q} \quad (2)$$

其中: $\varphi \in \mathbb{R}^{M \times 16^2}, \mathbf{Q}_M \in \mathbb{R}^M, M$ 为测量值的数目,对重建视频帧和码率有影响。 $M$ 若较大,则可以在一定范围内提高重建视频帧的质量,但是会降低码率;反之亦然。经实验得出,当 $M$ 取值范围如式(3)时,可以在重建视频帧质量和码率较好的取得折中。

$$\lceil 0.8N \rceil \leq M \leq \lfloor 0.9N \rfloor \quad (3)$$

## 2.3 熵编码预处理

由于 $\varphi \in \mathbb{R}^{M \times 16^2}$ ,且 $M \leq 16^2$ ,按照式(2)可知 $\mathbf{Q}_M$ 值的数目 $M \leq 16^2$ ,为了能够和标准编解码器语义兼容,方便后续的熵编码处理,需要在 $\mathbf{Q}_M$ 后补 $16^2 - M$ 个零,作为新的 QC 系数 $\mathbf{Q}'_M$ 参与后续编码处理。

## 2.4 解密及重构

在对 H.264 码流解码后,若当前解码出 CBP 参数值不为 0,则需要对当前 QC 向量 $\mathbf{Q}'_M$ 进行重构,恢复原始的 QC 向量 $\mathbf{Q}$ 。

Step1 根据 2.1 节,利用 128 比特的密钥 Key 构建测量矩阵 $\varphi$ 。

Step2 取 $\mathbf{Q}'_M$ 前 $M$ 个值,得到测量值 $\mathbf{Q}_M$ 。

Step3 根据测量值 $\mathbf{Q}_M$ ,利用文献[16]提出的改进的后退型最优正交匹配追踪(Orthogonal Matching Pursuit,OMP)图像重建方法,重构原始 QC 系数 $\mathbf{Q}$ ,并继续后续解码运算。

## 3 实验结果及分析

文献[17]认为感知加密会降低视频效果,但是降质后的视频仍是可感知的。本文结合文献[17],认为一个良好的感知加密算法应具有以下特征:

1) 感知加密的视频应具有语义和编码兼容性,即感知加密后的视频可以被任何标准解码器播放。这是由于未付费的用户需要通过标准解码器观看感知加密后的视频,以便决定是否付费。

2) 感知加密后的视频凭人眼仍可大概地看出视频主体所包含的内容。例如含人脸的视频感知加密后,仍可看出这是一张人脸,但是无法获取人脸的特征,也无法看到此人脸所在视频帧的背景信息。这是为了刺激视频点播用户购买高清质量的视频。

3) 在保证条件 1)前提下,客观加密效果评价应尽可能好,即加密后的视频帧与原始视频帧差别大。

4) 因为感知加密主要应用于视频付费点播业务,过于复杂加解密算法将导致无法实时浏览视频内容,因此加解密算法应具有尽可能低的时间复杂度。

5) 付费视频点播业务主要是通过互联网进行点播,由于网络带宽有限,因此加密算法对视频的码率影响应尽可能地小。

6) 感知加密主要用于保护被点播视频的版权问题,是视频未经付费或许可,即使复制和传播也无法清晰地浏览视频内容,或者破解密钥的时间代价远大于视频的收费时间,尽量做到对密钥变化敏感,即感知加密应具有较高的安全性。

### 3.1 加密效果分析

#### 3.1.1 主观加密效果评价

本文主观加密效果是对大小为 $176 \times 144$  的 Foreman 视频序列进行仿真实验,仿真中使用 JM8.6 作为仿真软件。加密后效果图和解密后的效果如图 1 所示。从图中可以得出,本文感知加密算法加密后的视频能够被标准解码器正常解码,并且能够在较好的扰乱原始视频内容的同时仍可被感知,满足感知加密评价标准的条件 1)~2),由于缺乏理想的重构算法,加密算法对重构后的视频帧质量有较小的影响。

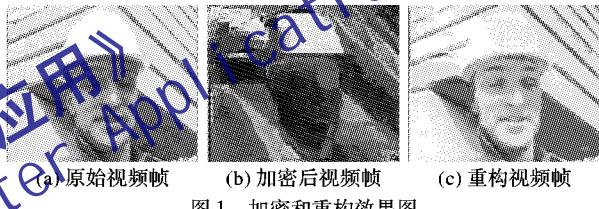


图 1 加密和重构效果图

#### 3.1.2 客观加密效果评价和重建视频序列质量

由于图像像素之间存在很强的相关性,而且这些相关性携带着图像结构的重要信息,人眼视觉可提取图像中的结构信息,并高度自适应地实现这一目标<sup>[18]</sup>。与采用峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)对加密视频进行加密效果评价相比,基于结构相似度(Structure Similarity, SSIM)的客观视频质量评价方法<sup>[19]</sup>适应人类视觉系统,能够更好地反映视频加密效果的优劣。SSIM 的评价标准为若两幅图像完全一样,则 SSIM 值为 1;相反地,若两幅图像差别越大,则 SSIM 越小,SSIM 的极限为 0。图 2 为 50 帧的加密视频和重建视频分别与原始视频对比的 SSIM。

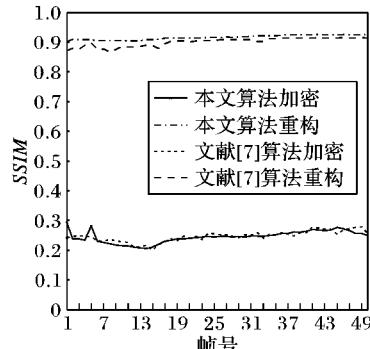


图 2 加密视频和重建视频与原始视频的对比

从图 2 可以得出,重构的视频帧的 SSIM 在 0.9 左右,比文献[7]重构质量略好,这是由于优化了测量矩阵和借鉴了更好的重构算法。而加密后的视频帧的 SSIM 在 0.25 左右,

与文献[7]相比基本持平,可知本文加密算法满足感知加密评价标准的条件 3),能够较好地加密原始视频帧中有效信息。

### 3.2 码率分析

对于视频通信而言,因通信信道带宽有限,需要对视频编码的码率进行控制,以确保码流的传输和信道带宽的充分利用<sup>[20]</sup>。H.264 中码率的计算方法是:

$$\text{码率} = \frac{1}{1000} \times \frac{\text{文件大小} \times 8}{\text{时间}} \quad (4)$$

其中:码率的单位是 Kb/s,文件大小的单位是 KB,时间的单位是 s。码率能够反映编码后视频压缩率与编码效率。表 1 是原始视频码率、重构视频码率和加密后视频码率的对比。

表 1 本文算法与文献[3]算法的码率对比 Kb/s

原始视频码率	重构视频码率	加密后视频码率	
		本文算法	文献[3]算法
124.62	127.68	130.2	128.92

从表 1 可看出:加密后视频码率和原始视频码率与重构视频码率相比基本增加不大,与使用文献[3]算法对所有宏块进行加密后视频的码率相比,相差较小。由此可见本文算法对码率影响较小,加密算法满足感知加密评价标准的条件 4)。

### 3.3 算法时间复杂度分析

本文从加密过程和重建过程对算法的时间复杂度进行分析。在加密过程中,建立测量矩阵时采用顺序查找的方式,时间复杂度为  $O(n)$ ,其中  $n$  表示问题规模;在对 QC 进行测量时,采用的是矩阵的乘法运算,时间复杂度为  $O(n^3)$ 。则加密一个宏块的时间复杂度为  $O(n^3)$ ,为线性复杂度。在重建过程中,通过密钥建立测量矩阵,则时间复杂度为  $O(n)$ ;在对 QC 进行重构时,OMP 算法在进行循环迭代过程中恢复原始信号总共涉及 5 次矩阵乘法,则时间复杂度为  $O(n^3 \times n)$ ,即  $O(n^4)$ 。则重建过程的时间复杂度为  $O(n^4)$ ,为多项式复杂度。综上分析,本文加密算法能够满足实时加密与解密,满足感知加密评价标准的条件 5)。

### 3.4 密钥雪崩效应分析

从密钥更换的有效性考虑,视频加密算法对密钥的变换应是敏感的,即密钥具有所谓的雪崩现象<sup>[21]</sup>。密钥雪崩效应测试主要是反映密钥改变后密文改变的程度,即新的加密视频帧中有多少个像素点与旧加密视频帧不同。因此,定义式(5)反映密钥敏感程度:

$$S = \sum_{i=0}^{M \times N} s_i \quad (5)$$

其中:

$$s_i = \begin{cases} 1, & c_i \neq c'_i \\ 0, & c_i = c'_i \end{cases}$$

$c_i$  是旧加密视频帧像素值, $c'_i$  是新加密视频帧的像素值,反映视频帧的大小。 $S$  反映密钥的敏感程度, $S$  越大,表示新的加密视频帧的像素与旧的加密视频帧中的像素不同越多,若所有像素都不同,则  $S$  的值为  $M \times N$ 。图 3 是 50 帧视频在仅对初始密钥改变 1 比特后的  $S$  值。

从图 3 可看出: $S$  值接近每帧总的像素数目  $176 \times 144$ 。

可以得出结论,当加密密钥发生细微改变时,会导致密文产生较大的变化,则本文算法具有较好的密钥雪崩效应,具有良好的安全性。而且文献[22]表明,当无法构建出原始的测量矩阵时,图像是不可能被重构的。因此,本文算法具有良好的安全性,满足感知加密评价标准的条件 6)。

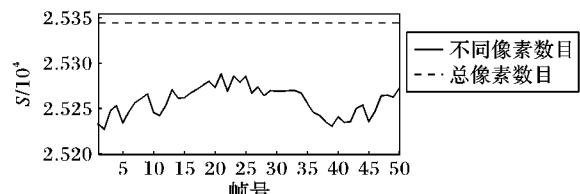


图 3 密文对密钥的敏感性测试

综上所述,本文感知加密算法满足感知评价标准的 6 个条件,具有较好的感知加密效果。

### 3.5 影响视频重构质量的因素分析

#### 3.5.1 测量值数目 $M$ 值的确定

经对同一视频的 50 次实验,表 2 是随着测量值数目 (Number of Measured Values, NMV) 的增加码率和重构视频质量 SSIM 变化情况的平均值。正常编码情况下,码率为 348.7 Kb/s,SSIM 值为 0.965。从表 2 可看出,随着 NMV 的增加,码率和 SSIM 都在增加,当 NMV 在 200 至 230 时,可以在视频重构质量和码率之间取得较好的折中,其变化范围为  $0.8 \times 256 \leq M \leq 0.9 \times 256$ 。

表 2 码率和 SSIM 随 NMV 变化情况

NMV	码率/(Kb·s <sup>-1</sup> )	SSIM	NMV	码率/(Kb·s <sup>-1</sup> )	SSIM
20	197.3	0.297	160	336.5	0.743
40	221.8	0.381	180	347.6	0.852
60	248.4	0.431	200	349.5	0.882
80	274.9	0.495	220	353.1	0.897
100	295.5	0.532	240	355.7	0.914
120	307.9	0.616	256	358.5	0.951
140	323.3	0.671			

#### 3.5.2 测量矩阵优化对重构视频质量的影响

优化前的 SSIM 为 0.8201,优化后为 0.9013,优化后的测量矩阵可以得到更好的重构质量,这是由于采用正交化优化后,进一步去除了测量矩阵列向量之间的相关性,更加符合压缩感知测量矩阵的构造性质。

## 4 结语

本文结合 CS 算法和 ZUC 算法,提出了一种适用于移动通信中视频点播的 H.264 视频感知加密算法。实验结果表明:本文算法具有较好的感知安全性,算法时间复杂度低且对码率影响较小。

### 参考文献:

- [1] LI S, CHEN G, CHEUNG A, et al. On the design of perceptual MPEG-video encryption algorithms [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2007, 17(2): 214–223.
- [2] STUTZ T, UHL A. A survey of H.264 AVC/SVC encryption [J]. Circuits and Systems for Video Technology, 2012, 22(3): 325–339.
- [3] WANG L, WANG W, MA J, et al. Perceptual video encryption

- scheme for mobile application based on H.264 [J]. The Journal of China Universities of Posts and Telecommunications, 2008, 15: 73 – 78.
- [4] WANG Y, DENG H. The video encryption scheme based in H.264 on perceptual encryption algorithm standards [J]. Application of Electronic Technique, 2012(1): 56. (王亚民, 邓虎超. H.264 标准中基于感知加密算法的视频加密方案[J]. 电子技术应用, 2012 (1): 56.)
- [5] AU YEUNG S K, ZENG B. A new design of multiple transforms for perceptual video encryption [C]// Proceedings of the 2012 19th IEEE International Conference on Image Processing. Piscataway: IEEE Press, 2012: 2637 – 2640.
- [6] AU YEUNG S K, ZENG B. Improved perceptual video encryption using multiple  $8 \times 8$  transforms in MPEG-4 [C]// Proceedings of the 2012 7th International ICST Conference on Communications and Networking in China. Piscataway: IEEE Press, 2012: 185 – 188.
- [7] TONG L, DAI F, ZHANG Y. Compressive sensing based video scrambling for privacy protection [C]// Proceedings of the 2011 IEEE Visual Communications and Image Processing. Piscataway: IEEE Press, 2011: 1 – 4.
- [8] FENG J. ZUC algorithm: 3GPP LTE international encryption standard [J]. China Information Security, 2011(12): 45 – 46. (冯秀涛. 3GPP LTE 国际加密标准 ZUC 算法[J]. 信息安全与通信保密, 2011(12): 45 – 46.)
- [9] GUAN J, DING L, LIU S. Guess and determine attack on SNOW3G and ZUC [J]. Journal of Software, 2013, 24(6): 1324 – 1333. (关杰, 丁林, 刘树凯. SNOW3G 与 ZUC 流密码的猜测决定攻击[J]. 软件学报, 2013, 24(6): 1324 – 1333.)
- [10] REN G, QIAO S, HEI Y. The application and implementation of ZUC stream cipher in the digital image encryption [J]. Science Technology and Engineering, 2013, 13(3): 766 – 770. (任高峰, 乔树山, 黑勇. 祖冲之算法在数字图像加密中的应用与实现[J]. 科学技术与工程, 2013, 13(3): 766 – 770.)
- [11] MA J, XU J, BAO Y, et al. Compressive sensing and its application: from sparse to low-rank regularized optimization [J]. Signal Processing, 2012, 28(5): 609 – 623. (马坚伟, 徐杰, 鲍跃全, 等. 压缩感知及其应用: 从稀疏约束到低秩约束优化[J]. 信号处理, 2012, 28(5): 609 – 623.)
- [12] ATHIRA V, GEORGE S N, DEEPTHI P P. A novel encryption method based on compressive sensing [C]// Proceedings of the 2013 International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing. Piscataway: IEEE Press, 2013: 271 – 276.
- [13] HUANG R, SAKURAI K. A robust and compression - combined digital image encryption method based on compressive sensing [C]// Proceedings of the 2011 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Washington, DC: IEEE Computer Society, 2011: 105 – 108.
- [14] BERINDE R, INDYK P. Sparse recovery using sparse random matrices [EB/OL].[2013-10-10]. <http://people.csail.mit.edu/indyk/report.pdf>.
- [15] LIN X, LU G, YAN J, et al. Measurement matrix of compressive sensing based on Gram-Schmidt orthogonalization [C]// Proceedings of the 2011 6th International Conference on Image and Graphics. Piscataway: IEEE Press, 2011: 205 – 210.
- [16] FANG H, ZHANG Q, WEI H. Image reconstruction based on improved backward optimized orthogonal matching pursuit algorithm [J]. Journal of South China University of Technology: Natural Science, 2008, 36(8): 23 – 27. (方红, 章权兵, 韦穗. 改进的后退型最优正交匹配追踪图像重建方法[J]. 华南理工大学学报: 自然科学版, 2008, 36(8): 23 – 27.)
- [17] LIU F, KOENIG H. A survey of video encryption algorithms [J]. Computers and Security, 2010, 29(1): 3 – 15.
- [18] YAO Y, XU Z. Visual security assessment for video encryption based on structural distortion [J]. Computer Engineering, 2008, 34(23): 23 – 25. (姚晔, 徐正全. 基于结构失真度的视频加密视觉保密性评价[J]. 计算机工程, 2008, 34(23): 23 – 25.)
- [19] WANG Z, LIU L, BOVIK A C. Video quality assessment based on structural distortion measurement [J]. Signal Processing: Image Communication, 2004, 19(2): 121 – 132.
- [20] CHEN J, LIU J, CAO X. In-depth understanding of video codec technology: H.264 standard and reference model [M]. Beijing: Beijing University of Aeronautics and Astronautics Press, 2012. (陈靖, 刘京, 曹喜信. 深入理解视频编解码技术: 基于 H.264 标准及参考模型 [M]. 北京: 北京航空航天大学出版社, 2012.)
- [21] CHEN G, LIAO X. Image encryption based on discrete chaotic maps [J]. Journal of Computer Applications, 2005, 25(S1): 121 – 123. (陈果, 廖晓峰. 一种基于混沌映射的图像加密算法[J]. 计算机应用, 2005, 25(S1): 121 – 123.)
- [22] RACHLIN Y, BARON D. The secrecy of compressed sensing measurements [C]// Proceedings of the 2008 46th Annual Allerton Conference on Communication, Control, and Computing. Piscataway: IEEE Press, 2008: 813 – 817.

(上接第 1648 页)

- [9] ZHOU C, XIE A. Dynamic niche-based self-organizing learning algorithm [J]. Journal of Software, 2011, 22(8): 1738 – 1748. (周传华, 谢安世. 一种基于动态小生境的自组织学习算法[J]. 软件学报, 2011, 22(8): 1738 – 1748.)
- [10] QIAO P, ZHENG L, MA L. Research on a niche genetic algorithm [J]. Journal of Harbin University of Science and Technology, 2011, 16(1): 90 – 93. (乔佩利, 郑林, 马丽丽. 一种小生境遗传算法研究[J]. 哈尔滨理工大学学报, 2011, 16(1): 90 – 93.)
- [11] LU Q, XIE P, SUN B. Sharing scheme-based adaptive hybrid genetic algorithm [J]. Computer Simulation, 2012, 29(12): 274 – 278. (陆青, 谢品杰, 孙波. 基于共享机制的自适应混合遗传算法[J]. 计算机仿真, 2012, 29(12): 274 – 278.)
- [12] ZHANG X, DAI G, XU N. Study on diversity of population in genetic algorithms [J]. Control Theory and Applications, 1998, 15(1): 17 – 23. (张晓绩, 戴冠中, 徐乃平. 遗传算法种群多样性的分析研究[J]. 控制理论与应用, 1998, 15(1): 17 – 23.)
- [13] XING X, YAN J. A novel genetic algorithm based on diversity maintaining and its simulation [J]. Computer Simulation, 2010, 27(4): 206 – 209. (邢小军, 闫建国. 一种基于多样性保持的遗传算法及其仿真[J]. 计算机仿真, 2010, 27(4): 206 – 209.)
- [14] LI M. The basic theory and application of genetic algorithms [M]. Beijing: Science Press, 2002: 164 – 165. (李敏强. 遗传算法的基本理论与应用 [M]. 北京: 科学出版社, 2002: 164 – 165.)