# 基于宏块重要性测度的重同步方法

邱锦波 冯 镔 喻 莉 朱光喜
(华中科技大学电子与信息工程系 武汉光电国家实验室(筹) 武汉 430074)

**摘 要** 重同步是视频传输中一种重要的错误恢复方法。对视频传输过程中的失真进行分析后,提出了基于宏块重要性测度的重同步新方法。通过定义宏块重要性测度,充分利用视频信息的重要性结合码流长度,对压缩视频流进行打包,使得视频包的重要性保持一致。分别采用基于宏块个数、基于码流长度和本方法对不同类型的测试序列进行了视频包丢失实验。结果表明,本文方法平均失真的波动最小,因此在传输过程中,无论哪一个视频包发生丢失,都不会对视频质量带来剧烈的波动,提高了主观视觉效果。

**关键词** 重同步,错误恢复,重要性测度,无线视频传输
**中图法分类号** TP37 **文献标识码** A

## Macroblock Importance Estimation Based Resynchronization Approach

QIU Jin-bo FENG Bin YU Li ZHU Guang-xi
(Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan National Laboratory for Optoelectronics, Wuhan 430074, China)

**Abstract** Resynchronization is an important error resilient approach for video transmission. The video transmission distortion was analyzed and a new macroblock importance estimation based resynchronization approach was proposed. Through the definition of macroblock importance estimation, the approach utilized the macroblock importance combining with the bit stream length to packet compressed video with the same importance. The proposed approach is compared with number of macroblock based method and bit stream length based method by different test sequences for the same video packet loss pattern. The experimental results show that the new approach can decrease video quality fluctuation in error prone channel and increase subjective quality greatly.

**Keywords** Resynchronization, Error resilient, Importance estimation, Wireless video transmission

## 1 引言

由于现有的视频压缩编码标准如 H. 264, MPEG-4 和 AVS 都采用变长编码技术进行统计编码,在消除码流数据之间相关冗余的同时,也降低了码流的抗误码能力。尽管无线网络的发展非常迅速,但是无线网络的动态性和异构性、高的错误率、传输链路的不可预测性、高度压缩的视频码流对传输错误非常敏感的特点,都对无线视频传输的质量产生很大的影响。为了提高无线视频传输的质量,在视频编码端有重同步、数据分隔、RVLC、I 宏块更新等错误恢复方法[1],在解码端有基于时间、空间、频域等错误隐藏方法[2],在传输过程中有结合视频编码的率失真特性所提出的信源信道联合编码方法[3]、与无线信道动态资源分配相结合的不平等保护方法等[4],其中重同步方法是一种重要的错误恢复手段[5,6]。

在视频解码器中,一个随机比特错误就会造成解码器无法正常解码。如果强行继续解码,将造成更多数据丢失,使得解码器失去同步,且必须等待下一个同步头才能重新恢复解码。重同步方法则是在码流中按一定间隔加入重同步信息,一旦出现误码导致解码器失去同步,解码器可以跳过这部分错误数据,从下一个重同步头开始正常解码,这部分跳过的数据则利用其他工具进行错误恢复和隐藏。

定义视频码流中相邻的重同步标志之间的数据为一个视频包。在 H. 261 和 H. 263[7] 标准中,数据是按照一个 GOB (Group of Block)来进行打包的。一个 GOB 包含一行或者多行宏块的数据。每个 GOB 都有其头信息,通过 GOB 头就可以定位当前 GOB 在视频中的位置,这种方法可以看作是一种空间域的重同步。H. 263 的重同步方法,缺点很明显:当视频的纹理或者运动比较复杂的时候,码流中两个重同步标志之间的间隔将非常大;当同步丢失时,需要丢弃大量数据才能重新找到同步标志,这对错误的恢复是非常不利的。因此在 MPEG-4 标准[8]中对这种打包方法加以改进,提出按照码流长度进行打包。当编码器产生码流长度超过一定门限时,即

到稿日期:2009-06-03 返修日期:2009-08-14 本文受国家自然科学基金(60873127),湖北省自然科学基金(2008CDB329 和 2007ABA090),国家科技支撑计划项目(2008BAH30B12),中芬国际合作项目(S2010GR0445)资助。
邱锦波(1977—),博士,讲师,主要研究方向为多媒体信息处理与多媒体通信,E-mail:qiujb@hust.edu.cn;冯 镔(1978—),博士,讲师,主要研究方向为视频数据挖掘;喻 莉(1970—),教授,博士生导师,主要研究方向为无线多媒体网络;朱光喜(1945—),教授,博士生导师,主要研究方向为无线多媒体通信。

在下一个宏块的码流之前插入一个重同步标志，开始一个新的视频包。这种打包方法的好处是视频包的长度相当，受到错误的影响相对较小。尤其在与可逆变长编码相结合时，具有显著的效果。

即使采用基于码流长度的视频打包方法，其每个视频包的重要性也并不一样。在同样的信道条件下，具有不同重要性的视频包发生丢失时，对视频质量的影响波动很大。在传输过程中，不可能对每一个具有不同重要性的视频包进行不同级别的保护。如果能够使得每一个视频包具有相同的重要性，那么在传输过程中将能减小视频质量的波动，使得主观质量更好。因此本文对信道传输失真及误差蔓延对视频质量的影响进行系统分析，在此基础上提出宏块重要性测度的定义，并提出一种新的根据宏块重要性测度进行视频打包的方法，以减小由于丢包带来的视频质量波动，使其更加有利于无线环境下的视频传输。

## 2 传输失真分析

在进行传输失真分析之前，本文假设编码端采用最常用的随机更新I宏块的错误恢复方法，I宏块更新率为$\beta$，在解码端采用复制前一帧对应位置像素的错误隐藏方法。

定义$F(n,i)$为第$n$帧图像的第$i$个宏块，$\hat{F}(n,i)$和$\tilde{F}(n,i)$分别为编码端重建值和经过传输以后解码端重建值。对于采用帧间编码模式的像素来说，$e(n,i)$为经过运动补偿以后的残差值，$\hat{e}(n,i)$和$\tilde{e}(n,i)$分别为编码端残差重建值和经过传输以后解码端残差重建值。在解码端采用直接复制前一帧图像对应位置的像素来进行错误隐藏，如果数据接收正确，其重建值为$\hat{F}(n,i)$；如果检测到数据错误或者丢失，那么这部分数据将用前一帧的重建数据替代，其重建值为$\tilde{F}(n-1,i)$。

对于采用帧内编码方式的I宏块，如果传输正确，恢复值为$\hat{F}(n,i)$，信道传输失真为0；如果发生错误或丢失，错误隐藏值为$\tilde{F}(n-1,i)$，其信道传输失真为：

$$\begin{aligned}D_t^I(n,i)&=E\{[\hat{F}(n,i)-\tilde{F}(n,i)]^2\}\\&=E\{[\hat{F}(n,i)-\tilde{F}(n-1,i)]^2\}\\&=E\{[\hat{F}(n,i)-\hat{F}(n-1,i)+\hat{F}(n-1,i)-\tilde{F}(n-1,i)]^2\}\\&=E\{[\hat{F}(n,i)-\hat{F}(n-1,i)]^2\}+E\{[\hat{F}(n-1,i)-\tilde{F}(n-1,i)]^2\}\end{aligned}\tag{1}$$

式中，$E\{[\hat{F}(n,i)-\hat{F}(n-1,i)]^2\}=a\cdot MSE(n,n-1)$，$a$为与信源编码相关的常数，$MSE(n,n-1)$为$i$宏块第$n$和$n-1$帧之间的均方误差。得到：

$$D_t^I(n,i)=a\cdot MSE(n,n-1)+D_t(n-1,i)\tag{2}$$

如果把视频编码器看作是一个低通滤波器[9]，那么重建帧就可以看作是原始图像经过低通滤波器以后的输出。从这个角度来看，$a$可以看作是编码器所带来的能量损失率，这个比率与编码器的量化参数相关，表示在编码过程中丢掉了多少信息。

对于采用帧间编码方式的P宏块像素，如果传输正确，恢复值为$\hat{e}(n,i)+\tilde{F}(n-1,j)$，这里$j$宏块是$i$宏块在前一帧图像中运动参考的像素值：

$$\begin{aligned}D_t^P(n,i)&=E\{[\hat{F}(n,i)-\tilde{F}(n,i)]^2\}\\&=E\{[\hat{F}(n,i)-\hat{e}(n,i)-\tilde{F}(n-1,j)]^2\}\\&=E\{[\hat{F}(n-1,j)-\tilde{F}(n-1,j)]^2\}\end{aligned}\tag{3}$$

式中，$E\{[\hat{F}(n-1,j)-\tilde{F}(n-1,j)]^2\}$为前一帧图像运动参考像素的传输失真值，定义$E\{[\hat{F}(n-1,j)-\tilde{F}(n-1,j)]^2\}=b\cdot D_t(n-1,i)$，其中$b$是表示视频运动程度的常数。

如果发生错误或丢失，错误隐藏值为$\tilde{F}(n-1,i)$，其信道传输失真同式(2)：

$$D_t^P(n,i)=a\cdot MSE(n,n-1)+D_t(n-1,i)\tag{4}$$

根据前面的分析可知，采用帧内编码模式的宏块所占比例为$\beta$，如果宏块传输正确，其失真为：

$$D_t(n,i)=\beta\cdot D_t^I+(1-\beta)\cdot D_t^P=(1-\beta)\cdot b\cdot D_t(n-1,i)\tag{5}$$

如果宏块传输错误，其失真为：

$$D_t(n,i)=a\cdot MSE(n,n-1)+D_t(n-1,i)\tag{6}$$

## 3 基于宏块重要性测度的打包方法

### 3.1 宏块重要性测度定义

现有的编解码标准，其编码过程和码流生成都是以宏块为单位，因此同样以宏块为单位定义其重要性测度。对于当前帧每一个宏块，假设它所在的数据包发生丢失，无疑会给整个视频序列带来失真。这个失真包括两个部分：一个部分是该宏块丢失给当前帧带来的失真，这部分失真与视频序列的复杂程度相关；另一个部分是由于该宏块不能正确解码而给后续帧带来的失真，这部分失真不仅与视频序列的复杂程度相关，还与视频编解码器所采用的错误恢复和错误隐藏方式相关。后面的分析依然采用和第2节同样的错误恢复与隐藏方法。

**定义1** 宏块的重要性测度$I$为假设当前宏块丢失对整个视频序列带来的失真。

$I$分为两个部分：一个部分是该宏块丢失引起的当前第$n$帧的失真，定义为$I_c(n)$；另一个部分是该宏块丢失引起后续第$n+l$帧的失真，定义为$I_p(n+l)$。总失真为：

$$I=I_c(n)+\sum_{l=1}^{\infty}I_p(n+l)\tag{7}$$

$I_c(n)$在编码端可以很容易得到。对第$n$帧第$i$宏块，其重建值为$\hat{F}(n,i)$，如果在传输过程中丢失，根据采用的直接复制前一帧对应位置像素进行错误隐藏的方法，解码端实际解码值为$\hat{F}(n-1,i)$，因此当该宏块发生丢失的时候，其失真为：

$$I_c(n)=E\{[\hat{F}(n,i)-\hat{F}(n-1,i)]^2\}=a\cdot MSE(n,n-1)\tag{8}$$

下面计算当前宏块丢失对后续第$n+l$帧产生的失真$I_p(n+l)$。假设当前第$n$帧第$i$宏块将作为第$n+1$帧第$k$宏块的参考，根据传输失真分析，其给下一帧带来的失真为$E\{[\hat{F}(n+1,k)-\tilde{F}(n+1,k)]^2\}=b\cdot I_c(n)$。由于在编码过程中采用了$I$宏块更新，如果像素$k$正好位于采用帧内编码方式的宏块内，那么其失真为0，错误蔓延被中止。如果其后续帧均正确接收，那么将不会再有错误发生。因此第$n+1$帧的失真为：

$$I_p(n+1)=(1-\beta)\cdot b\cdot I_c(n)\tag{9}$$

总失真 $I$ 为：

$$I=I_c(n)+\sum_{l=1}^{L}I_p(n+l)=I_c(n)+\sum_{l=1}^{L}[(1-\beta)b]^l I_c(n)=\sum_{l=0}^{L}[(1-\beta)b]^l I_c(n) \quad (10)$$

式中，$b$ 和 $\beta$ 都是大于 0、小于 1 的参数。当 $L\to\infty$ 时，

$$I=\frac{1}{1-b(1-\beta)}I_c(n)=\frac{1}{1-b(1-\beta)}\cdot a\cdot MSE(n,n-1) \quad (11)$$

根据式(11)即可计算出该宏块的重要性测度，也就是该宏块丢失对整个视频序列所带来的失真。

### 3.2 基于重要性测度的打包方法

在编码端设定一个重要性测度阈值 $T_I$，对每一个宏块 $k$，根据式(10)计算其重要性测度 $I_k$。当已编码的宏块其重要性测度之和超过阈值 $T_I$，即在下一个宏块的码流之前插入一个重同步标志，开始一个新的视频包。按照这样的想法对基于宏块重要性测度的打包方法进行实验并与 H.263 基于宏块和 MPEG-4 基于长度的方法进行对比，发现基于宏块重要性测度的打包方法具有和基于宏块打包方法一样的缺点，有的视频包其码流长度非常长。根据 Thomas Stockhammer 等的研究，在无线信道中，视频包越长，其发生错误的概率越大，同样不利于传输[10]。

为了克服这个缺点，结合 MPEG-4 基于长度的打包方法添加了一个限制条件：码流长度的门限 $T_L$。当已编码的宏块其重要性测度之和超过阈值 $T_I$ 或者已编码的宏块其码流长度超过阈值 $T_L$ 时，即在下一个宏块码流之前插入一个重同步标志，开始一个新的视频包。这样，既避免了重要宏块发生错误带来质量急剧下降，又避免了由于视频包过长而使视频包发生错误的概率增加。

## 4 实验结果与分析

为了检验基于宏块重要性测度的打包方法的有效性，分别采用基于宏块个数、基于码流长度和本文方法对 Mother & daughter，Carphone 和 Foreman 等不同类型的测试序列进行了实验。仿真的序列长度为 200 帧，码率 256kbps。基于宏块个数的方法(简称 MB 方法)以行为单位插入重同步头，对 QCIF 序列，每帧图像 9 个视频包。基于码流长度的方法(简称 LEN 方法)，根据码率设定视频包的大小为 950 比特，与 MB 方法对应，使码流包含基本相同数量的视频包。本文方法根据不同序列，平均分配视频包的重要性测度，保证视频包的个数和前 2 种方法基本相同。按照前面的参数设置，整个编码码流包含约 1800 个视频包，仿真选取从编号为 500～1500 之间，以 10 为间隔，记录单个视频包发生丢失时对序列平均失真的影响。

图 1、图 2、图 3 分别为 Foreman 序列的实验结果。图 1 为每个视频包包含宏块个数的对比，MB 方法当然其宏块个数为一个固定值 11，LEN 方法和本文方法宏块个数并不固定。图 2 为视频包长度的对比，可以看出，MB 方法的包长度变化很大，LEN 方法能够比较好地保持包的长度，本文方法介于两者之间。图 3 为单个视频包发生丢失时对序列平均失真的影响。MB 方法失真的波动最大，其最大值甚至超过 3000；而 LEN 方法相对波动较小，这是因为码流长度也可以部分反映视频的复杂程度；本文方法平均失真的波动最小，基本能够稳定在 500 以下，因此在传输过程中，无论哪一个视频包发生丢失，都不会对视频质量带来剧烈的波动。

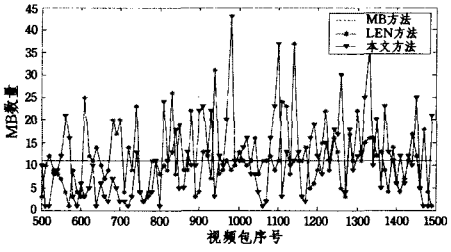


图 1 Foreman 序列视频包宏块个数对比

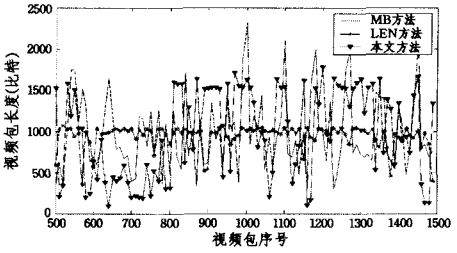


图 2 Foreman 序列视频包长度对比

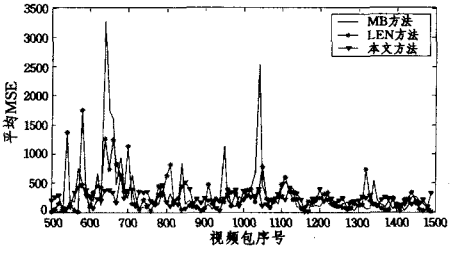


图 3 Foreman 序列平均失真对比

对 Mother & daughter 序列和 Carphone 序列，其结果与 Foreman 序列类似。将 3 个序列不同视频包丢失带来失真的平均值与均方差进行了统计，结果见表 1。从表 1 中数据可以看出，基于重要性测度的方法，其平均失真与 MB 方法和 LEN 方法基本相差不大，但是其均方差获得了较大的改善。也就是说，在同样的信道条件下，本文提出的基于宏块重要性测度的打包方法能够减小由于视频包丢失引起的视频质量波动，从而提供更加平滑的视频服务。

表 1 不同序列平均失真与均方差比较

| | 平均失真 | | | 均方差 | | |
|---|---|---|---|---|---|---|
| | M & D | Carphone | Foreman | M&D | Carphone | Foreman |
| MB 方法 | 46.58 | 107.93 | 474.14 | 104.13 | 127.61 | 303.45 |
| LEN 方法 | 34.32 | 124.73 | 313.99 | 55.25 | 164.18 | 278.08 |
| 本文方法 | 43.54 | 103.19 | 185.81 | 37.27 | 77.01 | 232.66 |

在前面的分析中，采用的是随机 I 宏块更新的错误恢复和复制前一帧图像的错误隐藏方法，其重要性测度如式(11)所示。在实际应用中，如果采用不同的错误恢复和错误隐藏方法，该式的表述将具有不同的形式，但是其本质是相同的。

**结束语** 本文通过分析压缩视频传输过程的失真，提出基于宏块重要性测度的重同步新方法，充分利用视频信息的重要性结合码流长度，对压缩视频流进行打包，使得视频包的重要性保持一致。实验表明，即使在传输过程中不采取任何不平等保护策略，该方法在视频包发生丢失的时候，也可以显著减小视频质量的波动，改善主观视觉效果。

(下转第 106 页)

证明：假设任意多项式时间攻击者 $A_{i(i=1,2)}$ 获取了第 $j$ 次会话密钥 $key_j = H_2(Q_A, Q_B, kPK_B, x_APK_B, u)$，进一步假设 $A_i$ 获得发送者 $A$ 的私钥 $(D_A, x_A)$，他要想获得第 $i$ 次 $(i \neq j)$ 次会话密钥 $key_i = H_4(Q_A, Q_B, kPK_B, x_APK_B, u)$ 在计算上是不可行的，因为计算 $key_i$ 需要知道 $kPK_B$ 或 $x_BR$，这将面临 CDH 数学难题。因此，本方案满足前向安全性。

### 4.2 有效性

由于计算资源的限制，通信终端一直是签密方案效率的瓶颈，因此，以下从终端的角度出发来分析签密方案性能，包括计算量（不考虑离线计算量）与密文长度两方面，并与现有协议进行比较。如表 1 所列，第 2 列 $x+y+z$ 表示 $x$ 次 $G_2$ 中的指数运算次数，$y$ 次 $G_1$ 中的点乘运算次数以及 $z$ 次双线性对运算次数，其中 $(n)$ 表示可交于代理服务器执行的运算次数，$|G_1|$ 表示 $G_1$ 中一个元素的长度，$c$ 表示密文长度，$k$ 表示一个 $Z_q^*$ 上随机数的长度，$h$ 表示一个 $\{0,1\}^n$ 上哈希值的长度。

从表 1 可以看出，本方案在计算量上是最优的。在密文长度方面，文献[4]较本方案少一个 $Z_q^*$ 上随机数的长度，但该长度较 $|G_1|$ 与 $c$ 的长度几乎可忽略不计。另外，当存在代理服务器时，本方案只需要一次点乘运算。由此可见，本方案更适合于网络安全应用。

表 1 有效性比较

| 方案 | Cost | Len |
|---|---|---|
| 方案[4] | 1+5+(3) | $2\|G_1\|+c$ |
| 方案[5] | 6+3+2 | $2\|G_1\|+c+k+h$ |
| 方案[10] | 0+4+3 | $2\|G_1\|+c+k$ |
| 新方案 | 0+[1+(2)]+(1) | $2\|G_1\|+c+k$ |

**结束语** 本文结合无证书密码系统与在线/离线签名的优点，提出了一个高效的无证书的在线/离线签密方案，并在随机预言模型中给出了安全性证明。在 CBDH 与 CDH 问题是困难的假设下，本方案被证明是安全的，而且利用无证书密码系统还避免了基于 PKI 密码体系证书管理复杂性以及基于身份密码系统固有的密钥托管问题。与现有的签密方案相比，本方案效率更高，且当存在代理服务器时，只需要一次点乘运算。将来的工作是设计通用的以及更为有效的无证书的在线/离线签密方案。

## 参 考 文 献


[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) (cost (signature) + cost (encryption)) [C] // Proceedings of the Cryptology-CRYPTO'97. Santa Barbara, California, USA, 1997: 165-179

[2] Shamir A. Identity-based cryptosystems and signature schemes [C] // Proceedings of the Cryptology - CRYPTO'84. Santa Barbara, California, USA, 1984: 47-53

[3] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography [C] // Proceedings of the ASIACRYPT 2003. Taipei, Taiwan, 2003: 452-473

[4] Barbosa M, Farshim P. Certificateless Signcryption [EB/OL]. http://eprint.iacr.org/2008/143.pdf, 2008

[5] Wu Chen-huang, Chen Zhi-xiong. A New Efficient Certificateless Signcryption Scheme [C] // Proceedings of the ISISE'08. Shanghai, China, 2008: 661-664

[6] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and Provably Secure Certificateless Multi-receiver Signcryption [C] // Proceedings of the ProvSec 2008. Shanghai, China, 2008: 52-67

[7] 李发根，胡予濮，李刚. 一个高效的基于身份的签密方案 [J]. 计算机学报，2006，29(9)：1641-1647

[8] Even S, Goldreich O, Macali S. On-line/off-line digital signatures [J]. Journal of Cryptology, 1996, 9: 35-67

[9] Zhang F, Mu Y, Susilo W. Reducing security overhead for mobile networks [C] // Proceedings of the 19th International Conference on Advanced Information Networking and Applications. Taipei, Taiwan, 2005: 398-403

[10] Sun Dong-dong, Huang Xin-yi, Mu Yi, et al. Identity-Based On-line/Off-line Signcryption [C] // Proceedings of the IFIP International Conference on Network and Parallel Computing. Shanghai, China, 2008: 34-41


(上接第 83 页)

## 参 考 文 献


[1] Wang Yao, Wenger S, Wen Jiantao, et al. Error resilient video coding techniques[J]. IEEE Signal Processing Magazine: 2000, 17(4): 61-82

[2] Wang Yao, Zhu Qinfan. Error control and concealment for video communication: a review[J]. Proceedings of the IEEE, 1998, 86(5): 974-997

[3] He Zhihai, Cai Jianfei, Chen Changwen. Joint source channel rate-distortion analysis for adaptive mode selection and rate control in wireless video coding[J]. IEEE Transactions on CSVT, 2002, 12(6): 511-523

[4] Ru Congchong, Yin Liuguo, Lu Jianhua, et al. UEP Video Transmission Based on Dynamic Resource Allocation in MIMO OFDM System[C] // Proceedings, 2007 IEEE Wireless Communications and Networking Conference (WCNC'07). 2007: 310-315

[5] Wang Yu, Chau Lap-Pui, Yap Kim-Hui. A Novel Resynchronization Method for Scalable Video Over Wireless Channel[C] // 2006 IEEE International Conference on Multimedia and Expo. 2006: 1669-1672

[6] Fang Tao, Chau Lap-Pui. Efficient content-based resynchronization approach for wireless video[J]. IEEE Transactions on Multimedia, 2005, 6(7): 1021-1027

[7] ITU-T. Video coding for low bit rate communications[S]. ITU-T Recommendation H.263, 1998

[8] MPEG-4 Video Verification Model version 18.0[S]. ISO/IEC JTC1/SC29/WG11 N3908 January 2001/Pisa

[9] Stuhlmuller K, Farber N, Link M, et al. Analysis of video transmission over lossy channels[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(6): 1012-1032

[10] Stockhammer T, Hannuksela M M, Wiegand T. H.264/AVC in Wireless Environments[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(7), 657-673