

# 基于非对称数据结构实现信息隐藏通信的方法研究

赵慧民<sup>1,2</sup>, 康显桂<sup>2</sup>, 黄继武<sup>2</sup>

(1. 西安邮电学院信息与控制系, 陕西西安 710121; 2. 中山大学广东省信息安全技术重点实验室, 广东广州 510275)

**摘要:** 数据结构是影响信息隐藏通信实时性能的关键技术. 为此, 系统设计需要对信源统计、信道状态与传输码率之间进行折衷考虑. 按照信息隐藏通信的要求, 把信源的统计特性以边信息在解码端进行处理, 本文提出了一种非对称数据结构实现信息隐藏通信的方法. 结合图像系数的方差分布和不同 WNR 环境下的信道状态, 该方法能够降低了系统编解码实现的复杂性. 分别应用 SCS 和 QIM(DC2DM) 及 SS 技术, 结果表明, 该方法实现的通信系统都具有较好的折衷性能.

**关键词:** 信息隐藏通信; 边信息; 编解码; 非对称; 码率

**中图分类号:** TP309      **文献标识码:** A      **文章编号:** 0372-2112 (2009) 06-1362-05

## An Information Hiding Communication Method Research Based on Asymmetric Data Structure

ZHAO Huimin<sup>1,2</sup>, KANG Xiangui<sup>2</sup>, HUANG Jiwu<sup>2</sup>

(1. Department of Information & Control, Xi'an University of Posts & Telecommunication, Xi'an, Shaanxi 710121, China;

2. Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou, Guangdong 510275, China)

**Abstract:** Data structure is one of the key technologies for realtime information hiding communication system. Therefore, the system design should be a related problem between source statistics and channel state as well as transmission rates. To satisfy some requirements with side information at decoder, the paper presents a new method to approach information hiding communication performances with asymmetric data structure. By means of variances distribution of image coefficients and channel states under various WNR, the proposed method can reduce system complex. Comparing the theoretical results by experimentation considered SCS and QIM(DC2DM) as well as SS techniques, the communication system possess the good tradeoff performances.

**Key words:** data hiding communication; side information; codec; asymmetric data structure; transmission rates

### 1 引言

数据隐藏技术是数字多媒体加密、数字内容处理和数字信息传输管理的最新实现方法. 目前, 包括数字版权保护、数字签名、内容完整性识别以及保密通信和水印多媒体处理, 都需要大量地应用数据隐藏实现技术.

目前, 信息隐藏技术的通信设计主要基于 Gel. fand Pinsker 提出的相关理论<sup>[1]</sup>, 但是, Gel. fand Pinsker 理论没有考虑传输信道的状态估计信息. 在均方误差的准则下, Costa 论证了 Gel. fand Pinsker 数据隐藏编码实现所需要的传输信道容量问题, 并说明高斯信道的传输容量可逼近随机干扰系统的通信容量<sup>[2]</sup>. 但在 Costa 论证中, 由于随机变量参数的设置和补偿系数需要优化选择, 因此, 系统的实现具有指数复杂性.

为了降低实现的复杂性, 实际应用的 Costa 系统编解码都基于了分层结构性的码本设计<sup>[3]</sup>. 这种码本使用了 (2D) 标量 Costa 系统方案(即 SCS 算法), 或多维格型 (multidimensional lattices) 矢量量化器, 称为失真补偿抖动调制(DC2DM) 或称为量化索引调制(QIM). 但是, DC2DM(QIM) 和 SCS 都没有考虑信源信号的概率密度函数 (probability density function), 而概率密度函数决定了信源信号的方差, 且其方差远大于水印和噪声信号的方差.

为此, Moulin 和 O. Sullivan<sup>[4]</sup> 使用信息理论的方法对数据隐藏和攻击者之间的 Gel. fand Pinsker 问题进行了深入的分析, 并把信源统计的边信息作为一种密钥形式进行处理; 另一方面, 它又与信源信号保持某种相关从而形成一种联合条件分布. 通过利用实际图像在独立

收稿日期: 2008-03-20; 修回日期: 2008-12-11

基金项目: 国家自然科学基金重点项目(No. 60633030); 国家自然科学基金(No. 90604008); 广东省自然科学基金团队项目(No. 04205407); 佛山市科技发展专项基金(No. 200601001)

高斯信道中的传输, Moulin 和 O. Sullivan 应用了这种原理分析了实际图像的数据隐藏容量. 但在 Moulin 和 O. Sullivan 的实现方法中, 这些并行信道之间需要进行严格的功率优化分配, 才能满足数据隐藏通信限定的约束条件. 针对这种情况, 本文前期的研究利用非均匀错误保护和动态规划策略实现了一种率失真最小化的信道传输技术<sup>[5,6]</sup>. 但这种技术由于攻击信道参数存在随机性并具有不同的码率, 通信时会产生较大的时延.

基于以上分析, 本文研究的目的是扩展 Gel'fand-Pinsker 理论的系统设计, 按照高斯条件和 Laplacian 原理, 对载体图像和隐藏信息的混合信源模型进行分割, 利用非因果关系进行条件编解码, 并把信源统计实现的边信息仅仅引入到解码器端进行设计, 从而提出一种 / 非对称0数据隐藏传输的通信方法. 其实现的整体目标是, 非严格要求 Costa 设计对攻击信道状态的学习过程, 同时达到在不同水印噪声比(WNR)环境下的一种稳健传输系统.

## 2 数据隐藏通信的研究对象模型

对应于通信技术的方案, 结合数据隐藏的原理, 这里把码率为 R, 数据长度为 N 的隐藏信息  $m \in \{2^0, 2^1, \dots, 2^{NR}\}$  映射编码为随机数字水印序列  $w^N = W^N(m, X^N, K^N)$ , 并通过具有条件概率  $p_{Y|W,X}(y|w,x) = p(y^N|w^N, x^N)$  的离散无记忆信道输出  $y^N \in Y^N$ . 其中,  $w, y$  和  $x$  分别是系统 W, Y 和 X 的一种实现变量, 且离散无记忆信道的工作状态由信源信号  $x^N \in X^N$  的状态信息决定. 数字水印信号方差嵌入失真的约束条件为  $E[\sum_{i=1}^N W_i^2] \leq NR\sigma_w^2$ , 决定了由于水印信号嵌入引起的误编码率.  $E[d^N(\hat{Y}, Y)] \leq NR\sigma_d^2$  表示在攻击和噪声信道环境下引起的通信失真. 其中,  $d^N(\hat{Y}, Y) = \frac{1}{N} \sum_{i=1}^N d(Y_i, \hat{Y}_i)$ ,  $d(Y_i, \hat{Y}_i) = (Y_i - \hat{Y}_i)^2$ , 且有关系  $\hat{Y} = X + W$  代表了信源和水印信号在攻击信道下的混合数据(stego2data), 在此基础上, 建立了如图 1 的通信模式, 图中, CSE/CSC(Channel State Estimation)为信道状态估计和信道状态补偿.

与数据通信的主要区别是, 本系统在解码器端利用了边信息 SI(side information)的数据  $S^N = U(X^N, K^N)$  进行检测解码. 其中, 函数  $U(\#)$  表示了某种 Hash 散列变换, 或使用公开密钥  $K^N$  从载体数据中提取的某种统计

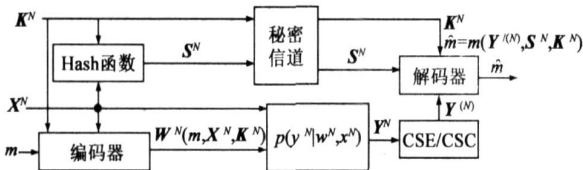


图1 基于边信息实现数据隐藏通信的模型

特性.

为此, 本文先从两种经典的信息隐藏通信方法研究其实现的理论基础.

### 2.1.1 Gel'fand-Pinsker 实现数据隐藏通信的形式

Gel'fand-Pinsker 理论的方法是把隐藏的信息  $m \in \{2^0, 2^1, \dots, M\}$ ,  $M = 2^{NR}$ , 编码成数字水印序列  $W^N$  并通过离散无记忆信道  $p_{Y|W,X}(y|w,x)$  传输的一种通信技术. 他把信源信号  $X^N$  只作为编码器端的一种干扰信号, 其实现形式如图 2.

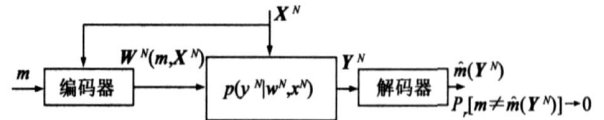


图2 Gel'fand-Pinsker利用边信息实现数据通信的形式

边信息在此的分布形式为  $p_X(X) = \prod p_X(x_i)$ . 该系统实现的主要问题是寻求可靠通信条件下的最大传输码率  $R = \frac{1}{N} \log_2 M$ .

假设一随机辅助变量 U 的条件分布形式为  $p_{U|X}(u|x)$ , 它决定的编码函数为  $f^N: G^N \rightarrow V^N \times W^N$ , 其中  $U \in G, W \in W, X \in V$ . 使用随机变量映射的编码方式, Gel'fand-Pinsker 理论实现的传输容量为<sup>[6]</sup>:

$$C_X^{I0} = \max_{p(u, w|x)} [I(U; Y) - I(U; X)] \quad (1)$$

这里, 我们用上下标注代表对应编码器可用状态或解码器所利用的有效统计状态, 因此,  $C_X^{I0}$  表示了信源 X 在编码器端(非解码器端)作为可用状态, 系统实现的信道容量, 其中,  $I(U; Y)$  和  $I(U; X)$  分别表示 Y 和 U, X 和 U 之间的一致性统一方阵.

对于式(1), Gel'fand-Pinsker 理论没有给出详细的证明. 但是, 为了保证编解码实现时, 通信传输出现的错误概率最小, 系统的码本必须由  $2^{N(R+R')}$  个码字组成 ( $R'$  代表 U 实现隐藏信息时生成的码率). 因此, Gel'fand-Pinsker 系统在设计时每个隐藏信息位需要的码字数近似等于  $2^{N(U;X)}$ , 且没有考虑攻击信道的状态信息.

### 2.1.2 Costa 实现数据隐藏通信的形式

Costa 把 Gel'fand-Pinsker 的实现形式看作高斯环境下的系统数据与均方误差准则的一种制约关系<sup>[7]</sup>. 其无记忆信道  $p_{Y|W,X}(y|w,x)$  传输的信源数据为  $X \sim N(0, R_X^2)$ , 噪声数据为  $Z \sim N(0, R_Z^2)$ , 图 3 为该系统的实现框图. 这时, 数字水印数据嵌入引起失真的约束条件为  $E[W^2] \leq R_w^2$ , 攻击失真则对应了加性高斯噪声的方差  $R_Z^2$ . 设随机辅助变量矩阵形式为  $U = W + AX$ , A 为系统

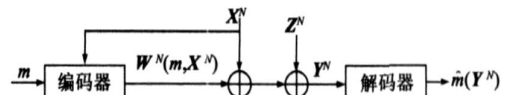


图3 Costa利用信源状态信息实现数据通信的形式

设计的补偿因子(或补偿系数),这时系统可实现的通信码率为:

$$R(A, R_x^2) = \frac{1}{2} \log_2 \frac{R_w^2 (R_w^2 + R_x^2 + R_z^2)}{R_w^2 R_x^2 (1-A)^2 + R_z^2 (R_w^2 + A^2 R_x^2)} \quad (2)$$

Costa 说明该系统需要的优化参数为  $A_{opt} = \frac{R_w}{R_w + R_z}$ , 它需要在编码时得到  $R_z^2$  的相关知识. 这种情况下, 系统实现的码率不取决于信源载体信号的方差, 而是:

$$R(A_{opt}) = C^{AWGN} = \frac{1}{2} \log_2 \left[ 1 + \frac{R_w}{R_z} \right] \quad (3)$$

式(3)就是系统在没有考虑信源干扰情况下 AWGN 信道的传输容量.

可见, 在 Costa 系统设计时, 由于  $I(U; X) = \frac{1}{2} \log_2 \left[ 1 + A^2 \frac{R_x}{R_w} \right]$ , 意味着, 信源信号的方差  $R_x^2$  越大, 对每个信息隐藏位编码时需要的码字数越多, 所以, Costa 系统对数据隐藏的实现具有指数复杂性.

### 3 信息隐藏通信的非对称数据结构及其实现方法

根据 Gel. fandPinker 和 Costa 通信系统的实现理论, 对于图 1 的研究对象, 这里, 我们把信源统计(通过西变化, 如 DCT, DWT, DDWT)得到的边信息  $S^N = R_x^{2N}$  仅仅引入到解码器端进行设计, 从而提出一种/非对称0数据结构实现信息隐藏通信的方法. 其中, 边信息  $S^N = R_x^{2N}$  的参数大小按照 Laplacian 分布处理后得到的长度为 N 的局部方差决定. 图 4 是该系统的实现原理框图. 为了消除量化噪声和嵌入失真对信源的干扰, 根据信源和信道状态的估计(CSE), 该系统通过随机映射解编码进行实现. 图中,  $p(x, R_x^2)$  代表由 Laplacian 概率密度函数对信源分割后得到的一种图像系数的分布统计.

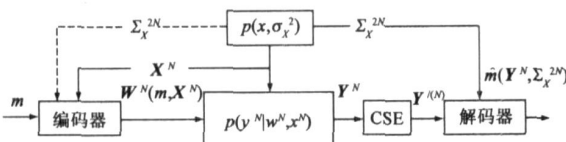


图4 编码器结合信源状态对信道编码以及解码器利用边信息解码的过程

为了得到一个直观的实现结果, 首先, 对离散无记忆信道的描述如下:

$$\begin{aligned} I(W; Y, E_x^2) &= I(W; E_x^2) + I(W; Y | E_x^2) \\ &= I(W; Y | E_x^2) \\ &= E_{E_x^2} [I(W; Y | E_x^2 = R_x^2)] \quad (4) \end{aligned}$$

由于式(4)服从水印信息 W 和统计  $E_x^2$  相互独立的条件, 所以, 这时随机编码参数生成了系统设计的码

本, 编码器通过分布  $p_w(w^N) = \prod_{i=1}^N p_w(w_i)$  产生  $2^{NR}$  个 IID 分布的码字发送到并行信道, 信道传输的隐藏信息  $m \in \{2^0, 2^1, \dots, 2^{NR}\}$  码字总数为  $W^N(m)$ . 解码器根据接收的矢量  $y^{(N)}$  和有效的边信息  $S^N = R_x^{2N}$ , 可以通过寻找一种联合三元组结构  $(W, Y, E_x^2)$  的条件  $(w^N(\hat{m}), y^{(N)}, R_x^{2N}) \in A_1^{*(N)}(W, Y, E_x^2)$  来检测隐藏的信息位  $\hat{m}$ .

在图 4 的系统中, 假设编码器和解码器都利用了信源信号统计的边信息  $E_x^{2N}$  (即对称数据结构的实现方法, 虚线表示) 进行设计, 那么有:

$$\begin{aligned} &I(U; Y, E_x^2) - I(U; X, E_x^2) \\ &= I(U; E_x^2) + I(U; Y | E_x^2) \\ &\quad - I(U; E_x^2) - I(U; X | E_x^2) \\ &= I(U; Y | E_x^2) - I(U; X | E_x^2) \quad (5) \end{aligned}$$

这时 Gel. fandPinker 定义的通信系统容量为:

$$C_{X, E_x^2}^{0,01} = \max_{p(u, w|x)} [I(U; Y, E_x^2) - I(U; X)] \quad (6)$$

当信源分割  $p(x, R_x^2)$  按照 Laplacian 概率密度函数进行时, 已知 X, 由于  $E_x^2$  和 U 相互独立, 则  $I(U; E_x^2 | X) = 0^{[7]}$ . 因此, 信源统计的边信息  $E_x^{2N}$  可以仅仅引入到解码端(即非对称数据结构的实现方法, 去掉虚线)进行设计, 则有:

$$\begin{aligned} &I(U; Y, E_x^2) - I(U; X) \\ &= I(U; Y, E_x^2) - I(U; X) - I(U; E_x^2 | X) \\ &= I(U; Y, E_x^2) - I(U; X, E_x^2) \\ &= I(U; Y | E_x^2) - I(U; X | E_x^2) \quad (7) \end{aligned}$$

这个结果与式(5)是一致的, 但是, 它简化了信源编码数据对边信息的要求, 因此, 这种实现方法实际上降低了系统设计的复杂性. 把式(7)代入式(6), 有:

$$\begin{aligned} C_{X, E_x^2}^{0,01} &= \max_{p(u, w|x)} [I(U; Y | E_x^2) - I(U; X | E_x^2)] \\ &= E_{p_{E_x^2}} \left[ \max_{p(u, w|x)} [I(U; Y | E_x^2 = R_x^2) - I(U; X | E_x^2 = R_x^2)] \right] \\ &= Q_0 \int p_{E_x^2}(R_x^2) \left[ \max_{p(u, w|x)} [I(U; Y | E_x^2 = R_x^2) - I(U; X | E_x^2 = R_x^2)] \right] dR_x^2 \quad (8) \end{aligned}$$

在 AWGN 环境下, 当边信息的统计知识为  $E_x^2 = R_x^2$  时, 对于选择一定的 A 系统容载的设计就是求信道传输码率  $R(A, R_x^2)$  的问题. 那么, 式(8)可以写为另一种形式:

$$R_{X, E_x^2}(A) = \int Q R(A, R_x^2) p_{E_x^2}(R_x^2) dR_x^2 \quad (9)$$

我们可以通过优化选择 A 的值, 达到系统码率可以实现的<sup>10,01</sup>最大传输容量, 即有关系  $R(A = A_{opt}, R_x) = C^{AWGN}$ . 所以, 有关系:

$$R_{x, E_x^2}(A) [ R(A_{pt}) = C^{AWGN} \tag{10}$$

式(10)中等式存在的条件是  $A = A_{opt} = \frac{R_w^2}{R_x^2 + R_z^2}$ , 其结果就是实现了 Costa 条件下的信息隐藏通信问题. 所以, 把 Costa 公式(2)和式(3)代入式(9)得到关系:

$$R_{x, E_x^2} = R(A_{pt}) \int p_{E_x^2}(R_x) dR_x = R(A_{pt}) = C^{AWGN} \tag{11}$$

这时系统编码的数据结构为:

$$f^N: \{2^0, 2^1, \dots, 2^{NR}\} @ \{2^0, 2^1, \dots, |K^N|\} @ X^N y W^N \tag{12}$$

而解码器的数据结构为:

$$g^N: y^N @ \{2^0, 2^1, \dots, 2^{NR}\} @ \{2^0, 2^1, \dots, S^N\} @ \{2^0, 2^1, \dots, |K^N|\} y \{2^0, 2^1, \dots, 2^{NR}\} \tag{13}$$

当  $N y \lfloor$  时, 系统的平均错误概率密度函数为:

$$\overline{P_e^N} = \frac{1}{2^{NR}} \int P_e [g(Y^N, S^N, K^N) X_m | M = m] y 0 \tag{14}$$

那么, 我们认为这种通信的实现过程是最优化的, 且达到稳健可靠的研究目的<sup>[8]</sup>.

### 4 实现结果及其性能分析

为了对提出的方法得到一个合理的性能分析, 在 AWGN 信道攻击下, 我们比较了其在不同隐藏技术情况下的实现结果. 图 5 显示了本文对 Costa 用优化补偿参数实现 AWGN 信道的系统容量问题. 同时, 对高斯和 Laplacian 信源变换的统计信号, 在水印图像比  $WIR = -6\text{dB}$  和  $WIR = -16\text{dB}$  条件下, 图中分别说明了基于二进制 SCS 和 QIM(DC2DM) 以及 SS 方法的 Costa 离散近似实现的信道容量性能分析. 其中, 当  $A = 0$  时, 把式(2)代入式(11), 应用 SS 方法系统实现的码率为:

$$R_{x, E_x^2}(0) = \int \frac{1}{2} \log_2 \left[ 1 + \frac{R_w^2}{R_x^2 + R_z^2} \right] p_{E_x^2}(R_x) dR_x \tag{15}$$

而当  $A = 1$  时, 应用 QIM(DC2DM) 方法, 系统实现的系统码率为:

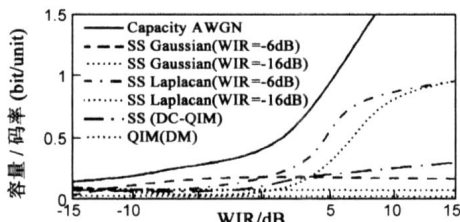


图 5 本文应用 SCS, QIM 和 SS 技术实现的 Costa 码率

$$R_{x, E_x^2}(1) = \int \frac{1}{2} \log_2 \left[ \frac{R_w^2}{R_x^2 + R_z^2} + \frac{R_w^2}{R_x^2 + R_z^2} \right] p_{E_x^2}(R_x) dR_x \tag{16}$$

由图可见, 在高斯和 Laplacian 不同信源的条件, 较低 WNR 时, 各种条件下 SS 方法实现的码率差别不大; 但在较高 WNR 时, 对数字水印来说, 由于信源信号作为干扰噪声, 所以, SS 方法在 Laplacian 信源分布下实现的码率比高斯信源下的码率大许多.

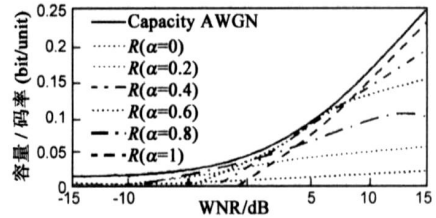


图 6  $WIR = -6\text{dB}$ , 本文对 Costa 设置不同  $\alpha$  时实现  $R(\alpha, \sigma_x^2)$  码率

按照研究的方法, 为了比较边信息对解码器的影响, 对 Costa 公式(2)设置不同的补偿参数 A 的值, 图 6 在  $WIR = -6\text{dB}$  时显示了本系统实现的不同码率性能. 根据本文研究得到的式(10)和式(11), 图 7 显示了在  $WIR = -6\text{dB}$  和不同补偿参数 A 的值时, 解码器结合边信息进行解码, 系统实现  $R_{x, E_x^2}(A)$  的不同码率. 在  $WIR = -6\text{dB}$  时, 应用不同补偿参数 A 的值, 图 8 说明了研究的方法和 Costa 方案实现的码率差  $R_{x, E_x^2}(A) - R(A)$  (即率增益问题).

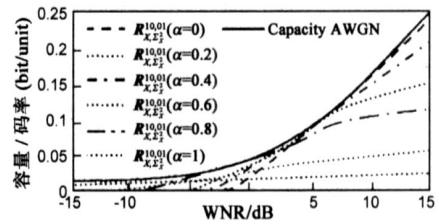


图 7  $WIR = -6\text{dB}$ , Costa 解码器结合边信息实现  $R_{x, E_x^2}^{10,01}(\alpha)$  码率

由图可见, 对于 SS 方法  $A = 0$  的情况, 在较低 WNR 环境下,  $R(0)$  达到了系统信道的传输容量; 而在较高 WNR 环境下, 由于信源信号的方差对系统的性能有较大的影响, 实现的码率变化较大. 如果解码器端利用了边信息解码, 那么系统在较高的 WNR 环境下, 码率  $R_{x, E_x^2}(0)$  明显大于  $R(0)$ . 考虑 QIM 方法  $A = 1$  的近似情况, 在高 WNR 环境下,  $R(1)$  达到了高斯信道的传输容

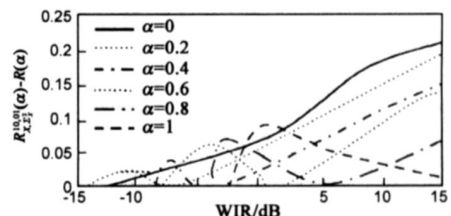


图 8  $WIR = -6\text{dB}$ , 系统实现的率增益

量. 相对而言, 在低 WNR 环境下, 由于每个信息位需要的码字较大且检测的错误概率较高, 系统的性能会降低, 但本文研究实现的传输码率  $R_{X, E^2(X)}^{10, \alpha}$  (1) 仍然具有良好的性能.

## 5 结论

在攻击信道条件下, 编码时考虑信源的状态, 而在解码时利用边信息的统计条件, 本文提出了一种非对称数据结构实现信息隐藏通信的具体应用方法. 在 Gel. fandPinker 和 Costa 基础上, 该方法分别应用了 SS 和 QIM 技术进行了系统分析. 当固定补偿参数  $A=0$  时, SS 方法是 Costa 理论的一种特殊情况. 而当固定补偿参数  $A=1$  时, QIM 方法就是 Costa 实现的一种近似逼近. 同时, 本文根据 Gel. fandPinker 随机映射编码理论, 在各种 A 条件下, 解码器利用边信息能够达到不同 WNR 环境下信道传输的折中条件, 从而验证了理论分析的正确性. 本文的研究方法对于数据隐藏传输系统相关领域的实现具有一定的指导意义.

## 参考文献:

- [1] E Topaka, S Voloshynovskiy, O Kovala, et al. Security analysis of robust data hiding with geometrically structured codebooks [EB/OL]. [http:// sip. unige. ch](http://sip.unige.ch), 2008- 01- 28.
- [2] S Voloshynovskiy, O Kovala, et al. Data hiding with host state at the encoder and partial side information at the decoder [EB/OL]. <http:// sip. unige. ch>, 2008- 02- 20.
- [3] Min Wu, Hong Heather, Yu Alex Gelman. Multilevel data hiding for digital image and video [J]. IEEE Transactions on Image Processing, 2007, 23(6): 1775- 1784.
- [4] P Moulin, O Sullivan J. Information theoretic analysis of information hiding [J]. IEEE Transactions on Information Theory, 2003, 49(3): 563- 593.
- [5] Gu L2min, Fang Yan2mei, Huang J2wu. Reevaluation of error correcting coding in watermarking channel [A]. Proc of CANS2005, Lecture Notes Computer Science(LNCS) [C]. Beijing: Science Press, 2005, 38(10): 274- 287.
- [6] 赵慧民, 方艳梅. 一种非均匀错误保护实现最优码率分配的技术 [J]. 中山大学学报, 2007, 46(1): 43- 47.  
Zhao hui2min, Fang Yan2mei. An optimal rate allocation method search based on unequal error protection [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2007, 46(1): 43 - 47. (in Chinese)
- [7] 方艳梅, 谷利民, 黄继武. 利用边信息嵌入的 CDMA 水印信道性能研究 [J]. 电子学报, 2006, 34(1): 45- 50.  
Fang Yan2mei, Gu L2min, Huang J2wu. Performance analysis of CDMA based watermarking channel with side information embedding [J]. Acta Electronica Sinica, 2006, 34(1): 45- 50. (in Chinese)
- [8] Kang Xiangui, Huang Jiwu, et al. A DWTDFT composite watermarking scheme robust to both affine transform and JPEG compression [J]. IEEE Transaction on Circuits and Systems for Video Technology, 2003, 13(8): 776- 786.

## 作者简介:

**赵慧民** 男, 1966 年 3 月生于陕西, 博士, 副教授, 中国电子学会高级会员. 2001 年 6 月获中山大学电子与通信工程系博士学位. 现在西安邮电学院信息与控制系工作. 主要研究方向: 电子信息和数据安全. E-mail: zhachuimin@tom.com

**康显柱** 男, 博士, 中山大学信息科学与技术学院副教授. 研究方向: 多媒体通信与信息安全、信息隐藏与数字水印、数字权限管理等. Email: isskxg@mail.sysu.edu.cn

**黄继武** 男, 中山大学信息科学与技术学院教授, 博导, IEEE 高级会员. 研究方向: 多媒体通信与信息安全、信息隐藏通信技术等. Email: issljw@mail.sysu.edu.cn