Laplacian 信源分割及其并行 Gaussian 信道传输的信息隐藏技术研究*

赵慧民[1,2]，康显桂[2]，黄继武[2]
（1. 佛山科学技术学院电子信息工程系，广东 佛山 528000；
2. 中山大学信息安全技术广东省重点实验室，广东 广州 510275）

摘 要： 在研究 Costa 设置和 Cox 高斯分解的基础上，根据信源的随机状态，提出了一种新的信息隐藏传输技术。通过信源 Laplacian 条件分割，并根据图像系数方差的不同分布区域对高斯信道进行并行分解，该技术实现了在二义性攻击条件下的一种稳健信息隐藏传输方法。结合应用 SS 和 QIM（DC－DM）技术，实验结果表明，该技术在信息嵌入量、传输码率和信道容量之间都具有很好的折中性能。

关键词： 信源分割；信息隐藏；高斯信道；并行传输；信道容量
中图分类号： TP309 **文献标识码：** A **文章编号：** 0529-6579（2008）04-0029-06

信源分割模型是实现信息隐藏通信的第一要素[1-3]，目前，用酉变化（如 DCT，DWT，DDWT）对图像系数解相关之后，广泛应用的随机图像模型是具有高斯概率密度函数（pdf）形式 I. I. D 分布的模型[4]。这种模型主要研究了图像系数的全局特征，但是，如果考虑载体图像局部系数的统计特性时，信息隐藏的实现会获得更好的系统增益，这就是 Cox 提出的信源分割（Source splitting）方案[5]。因此，根据信源的全局特征并结合分割后图像系数的局部统计知识，建立随机图像模型的局部和全局之间的数学关系是我们研究信息隐藏通信实现的关键技术[1,5-7]。

为了降低实现的复杂性，实际应用的高斯信源分割模型主要通过 Costa 系统建立结构性的码本设计。这种码本使用了标量 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（DC－DM）或称为量化索引调制（QIM）[6,8]。但是，DC－DM（QIM）和 SCS 都没有考虑信源信号的概率密度函数 pdf（Probability density function）的统计特性，而在数字水印系统设计时，pdf 决定了信源信号的方差，且其方差远大于水印和噪声的方差。因而，这些方法在应用上仍然有局限性[9-10]。

基于以上分析，鲁棒的信息隐藏通信，需要充分考虑信源的工作状态，同时需要根据信道的传输性能进行折中设计。为此，本文按照高斯条件和 Laplacian 原理，对载体图像和隐藏信息的混合信源模型进行分割，并根据图像系数方差的不同分布区域对二义性 DMC（离散无记忆）攻击信道进行高斯（Gaussian）并行分解，研究设计在不同水印噪声比（WNR）环境下的一种稳健信息隐藏传输方法。

1 信息隐藏理论对信源状态和信道条件的统计知识

我们知道时域图像本身的分布并不服从某种特定的形式，但是，图像在变换域却表现出很好的分布特征[6]。经典研究的 SS、SCS、以及 QIM（DC－DM）水印算法，都是基于酉变换进行。根据信源的这种特征，需要信源状态的统计知识为信息隐藏提供条件编码要素。因此，鲁棒的信息隐藏系统，除了应具有好的嵌入/检测算法，还需要考虑：信源信号的分布特征（作为参考源）并结合信道状态（作为噪声源）提高数据隐藏的传输性能。为此，本文先从 Costa 通信问题研究信息隐藏在信源内部的统计特性。

Costa 问题可以看作高斯环境下的信源数据和均方误差准则的一种制约关系[9]。对应于通信技术的方案，它把码率为 R 数据长度为 N 的隐藏数据信息 $m\{2^0,2^1,\ldots,2^{NR}\}$ 映射编码成随机数字水印序列 $w^N = W^N(m,X^N)$，同时通过具有条件概率 $p_{Y|W,X}(y|w,x) = p(y^N|w^N,x^N)$ 的 DMC 输出 $y^N \propto Y^N$，其中，w、y 和 x 分别是系统 W、Y 和 X 的子集（即一种实现单位），而 DMC 通信的工作状态

* 收稿日期：2007－12－25
基金项目：国家自然科学基金资助项目（60403045）；佛山市科技发展专项基金资助项目（200601001）
作者简介：赵慧民（1966年生），男，博士，副教授；E-mail：zhaohuimin@tom.com

由信源载体信号 $x^N \propto X^N$ 的状态信息决定。对于具有高斯分布的信源数据 $X \sim N(0,\sigma_X^2)$，噪声数据 $Z \sim N(0,\sigma_Z^2)$ 设计的 DMC 系统，其实现的结构框图如图1。数字水印嵌入失真的约束条件为 $E[W^2] \leqslant \sigma_W^2$，攻击失真对应加性高斯噪声的方差 σ_Z^2。设随机辅助变量为 $U = W + \alpha X, \alpha$ 为系统设计的补偿因子（或补偿系数），这时系统可实现的通信码率为：

$$R(\alpha,\sigma_X^2) = \frac{1}{2}\log_2 \frac{\sigma_W^2(\sigma_W^2+\sigma_X^2+\sigma_Z^2)}{\sigma_W^2\sigma_X^2(1-\alpha)^2+\sigma_Z^2(\sigma_W^2+\alpha^2\sigma_X^2)} \quad (1)$$

Costa 说明该系统需要的优化参数为 $\alpha_{opt} = \sigma_W^2/\sigma_W^2 + \sigma_Z^2$，它需要在编码时得到 σ_Z^2 的相关知识。这种情况下，系统实现的信道传输码率不取决于信源信号的方差，而是：

$$R(\alpha_{opt}) = C^{AWGN} = \frac{1}{2}\log_2(1+\frac{\sigma_W^2}{\sigma_Z^2}) \quad (2)$$

这就是 Costa 系统在没有考虑信源干扰情况下 AWGN 信道的传输容量。可以看到，Costa 设置中，由于信源数据 X 和辅助变量 U 之间的统一矩阵为 $I(U;X) = \frac{1}{2}\log_2(1+\alpha^2\sigma_X^2/\sigma_W^2)$，这意味着，信源信号的方差 σ_X^2 越大，对每个隐藏信息位编码时需要的码字数越多，所以，Costa 通信系统对信息隐藏的实现具有指数复杂性。为此，必须通过对信源状态的进一步分析，在保证实现的码率条件下，研究隐藏信息的统计条件和编解码的一种制约关系。

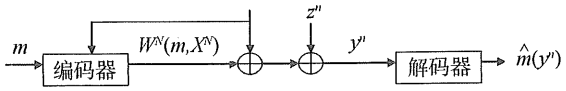

图1 信息隐藏利用信源状态和信道条件实现 Costa 的方案

Fig. 1 Costa achievement with Source state and channel conditions for information-hiding

2 信源随机状态的处理模型及其信息隐藏的条件设计

2.1 信源的 Laplacian 分割模型

基于对信源联合分布 $p(x,\sigma_X^2)$ 的分析，应用拉普拉斯概率密度函数（Laplacian - pdf）和马尔可夫数据链（Markov Chain）准则，获得 Costa 设置的分布概率为[6]：

$$p_{X,\sum_X^2}(x,\sigma_X^2) = p_{\sum_X^2}(\sigma_X^2)p_{X|\sum_X^2}(x|\sigma_X^2) \quad (3)$$

这里，$p_{\sum_X^2}(\sigma_X^2)$ 代表了信源信号的临界方差分布，而条件分布 $p_{X|\sum_X^2}(x|\sigma_X^2)$ 表示了 Laplacian - pdf 获得局部系数的一种统计行为。对应临界分布条件，全局数据的统计为：

$$p_X(x) = \int_0^\infty p_{X,\sum_X^2}(x,\sigma_X^2)\mathrm{d}\sigma_X^2 = \int_0^\infty p_{X|\sum_X^2}(x|\sigma_X^2)p_{\sum_X^2}(\sigma_X^2)\mathrm{d}\sigma_X^2 \quad (4)$$

按照无穷高斯混合模型（infinite Gaussian mixture model）的实现原理[13]，条件项在此即为 $p_{X|\sum_X^2}(x|\sigma_X^2) = \frac{1}{\sqrt{2\pi\sigma_X^2}}e^{-\frac{x^2}{2\sigma_X^2}}$，这就是零均值高斯分布的形式。这时，图像的局部统计模型就成为高斯模型，而由此得到的全局分布 $p_X(x)$ 确定了 $p_{\sum_X^2}(\sigma_X^2)$ 方差分布的范围。在已知局部数据方差的指数分布 $p_{\sum_X^2}(\sigma_X^2) = \lambda_1 e^{-\lambda_1\sigma_X^2}$ 条件形式下，全局 Laplacian - pdf 可以作为零均值 Gaussian - pdf 的一种混合加权，这里 λ_1 为指数分布的标量参数。因此，(4) 式可写为：

$$p_X(x) = \int_0^\infty \frac{1}{\sqrt{2\pi\sigma_X^2}}e^{-\frac{x^2}{2\sigma_X^2}}\lambda_1 e^{-\lambda_1\sigma_X^2}\mathrm{d}\sigma_X^2 = \sqrt{\frac{\lambda_1}{2}}e^{-\sqrt{2\lambda_1}|x|} \quad (5)$$

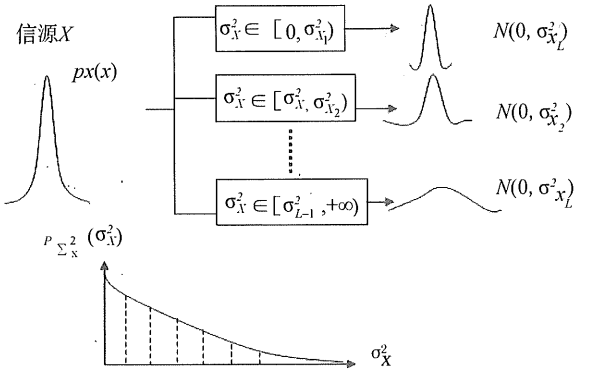

图2 L 个并行高斯信道的 Laplacian 信源分割模型

Fig. 2 L-Parallel Gaussian channels using Laplacian source splitting model

这种关系为图像分解后局部和全局系数之间的统计关系提供了一种基本数据连接。因此，同样的分割系数数据，可以按照指数 pdf 的条件作为具有局部方差分布的零均值高斯编码数据考虑，也可以同时作为全局 Laplacian 的一种统计形式。所以，按照 Laplacian 信源分割后，图像数据 X 的方差分布间隔 $[0;\sigma_{X_1}^2),[\sigma_{X_1}^2;\sigma_{X_2}^2),\cdots,[\sigma_{X_{L-1}}^2;+\infty)$，高斯信道可以划分为 L 个并行传输信道。图2说明了一种实现方案。

2.2 信息隐藏通信的条件设计

这里，我们把信源分割统计实现的边信息 S^N

$= \sigma_X^{2N}$ 仅引入到解码器端进行研究，提出一种“非对称”信息隐藏传输方法。其中，边信息 $S^N = \sigma_X^{2N}$ 的参数由 Laplacian 信源分割得到的长度为 N 的局部方差决定。图 3 是系统的实现框图。

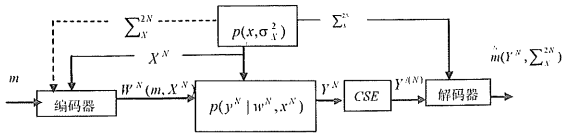

图 3　利用边信息通信实现的编解码过程

Fig. 3　Codec method of hiding communication with side information

此时，信源的工作状态 X 对编码而言是一种非因果关系，它由信源分布、攻击数据、信道状态估计 CSE（channel state estimation）共同决定。其编码函数形式为：

$$f^N:\{2^0,2^1,\ldots,2^{NR}\}\times\{2^0,2^1,\ldots,|K^N|\}\times X^N\rightarrow W^N \tag{6}$$

解码器函数形式为：

$$g^N:y^N\times\{2^0,2^1,\ldots,2^{NR}\}\times\{2^0,2^1,\ldots,S^N\}\times(2^0,2^1,\ldots|K^N|\}\rightarrow\{2^0,2^1,\ldots,2^{NR}\} \tag{7}$$

此时信息隐藏的编码器不但利用了信源信号 X^N 在信道 CSE 的状态，还考虑数据概率 $p(x,\sigma_X^2)$ 的统计 $\sum_X^{2N}$（虚线表示）因素。由于 X^N 和 $\sum_X^{2N}$ 互相关，所以，这里设定 $(X_i,\sum_{X_i}^{2})$ 是具有 $p(x_i,\sigma_{x_i}^2)$，$i-1,2,\ldots,N$ 的 I. I. D 分布。这时，信息隐藏编码器产生一种数字水印序列 $W^N(m,X^N),m\{2^0,2^1,\ldots,2^{NR}\}$。解码器根据 $Y'^{(N)}$ 和 $\sum_X^{2N}$ 得到的一种估计检测信息为 $\hat{m}(Y'^{(N)},\sum_X^{2N})$，那么，系统的平均错误概率为：

$$\overline{P_e^N}=\frac{1}{2^{NR}}\sum\nolimits_{mM}P_r[m\neq\hat{m}(Y'^{(N)},\sum\nolimits_X^{2N})\mid M=m] \tag{8}$$

为了得到一个直观设计的结果，首先，系统对 DMC 离散无记忆信道的设计如下：

$$I(W;Y,\sum\nolimits_X^2)=I(W;\sum\nolimits_X^2)+I(W;Y|\sum\nolimits_X^2)=I(W;Y|\sum\nolimits_X^2)=E_{\sum_X^2}[I(W;Y|\sum\nolimits_X^2=\sigma_X^2)] \tag{9}$$

（9）式服从隐藏信息 W 和 $\sum_X^2$ 相互独立的条件。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 *I. I. D* 分布的码字发送到 L 个并行信道，信道传输的隐藏信息 $m\{2^0,2^1,\ldots,2^{NR}\}$ 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 $S^N=\sigma_X^{2N}$，可以寻找一种联合三元组结构 $(W,Y,\sum_X^2)$ 的设置条件 $(w^N(\hat{m}),y'^{(N)},\sigma_X^{2N})A^{*(N)}(W,Y,\sum_X^2)$ 来解码隐藏的信息 $\hat{m}$。如果 $\hat{m}$ 不存在或者超过一个，那么系统声明一个错误。当 $\hat{m}\neq m$ 时，用错误概率可以说明解码器出现的所有可能情况。其中，第一类错误是，当发送和接收的序列不是一个联合三元组结构；第二类错误是，接收的信号是联合三元组但包含一个错误的码字。按照渐进平均分配原则[10]，第一类错误概率趋向于零。为了限制第二类错误，对有效长度 N，码率的约束条件设定为 $R<I(W;Y|\sum_X^2)$。

2.3　信息隐藏通信的传输码率实现条件

在图 3 信息隐藏的实现方案中，假设信源信号的统计为 $\sum_X^{2N}$ 并在编码器和解码器都可以利用，那么有：

$$I(U;Y,\sum\nolimits_X^2)-I(U;X,\sum\nolimits_X^2)=I(U;\sum\nolimits_X^2)+I(U;Y|\sum\nolimits_X^2)-I(U;\sum\nolimits_X^2)-I(U;X|\sum\nolimits_X^2)=I(U;Y|\sum\nolimits_X^2)-I(U;X|\sum\nolimits_X^2) \tag{10}$$

因此，对于 *DMC* 条件信道 $p_{Y|W,X}(y|w,x)$，如果编码器利用非因果关系实现信源编码，且信源信号统计特性 $(X_i,\sum_{X_i}^2)$ 在解码器端具有概率 $p(x_i,\sigma_{x_i}^2)$ 的 *I. I. D* 分布特性。那么，信息隐藏系统的传输容量可以定义为：

$$C_{X,\sum_X^2}^{10,01}=\max_{p(u,w|x)}[I(U;Y,\sum\nolimits_X^2)-I(U;X)] \tag{11}$$

这里，$C_{X,\sum_X^2}^{10,01}$ 表示编码器利用信源信号 X 而解码器利用统计 $\sum_X^2$ 实现的系统容量。

当信源分割模型 $p(x,\sigma_X^2)$ 按照图 2 进行时，对于所有随机变量之间联合分布 $p(x,\sigma_X^2,u,w,y)$ 的关系可以描述为：

$$p(x,\sigma_X^2)p(u,w|x)p(y|w,x)=p(\sigma_X^2)p(x|\sigma_X^2)p(u|x)p(w|u,x)p(y|w,x) \tag{12}$$

注意到关系 $\sum_X^2\rightarrow X\rightarrow U$ 形成了一种 Markov chain，所以，已知 X，则 $\sum_X^2$ 和 U 相互独立，联合方阵矩阵的结果为 $I(U;\sum_X^2|X)=0$。因此，（11）式可以进一步写为：

$$I(U;Y,\sum\nolimits_X^2)-I(U;X)=$$

$$I(U;Y,\sum\nolimits_X^2) - I(U;X) - I(U;\sum\nolimits_X^2 \mid X) =$$
$$I(U;Y,\sum\nolimits_X^2) - I(U;X,\sum\nolimits_X^2) =$$
$$I(U;Y \mid \sum\nolimits_X^2) - I(U;X \mid \sum\nolimits_X^2) \quad (13)$$

这个结果与（10）式是一致的。因此，可以把（13）代入（11）式，有：

$$C_{X,\sum_X^2}^{10,01} = \max_{p(u,w\mid x)}[I(U;Y \mid \sum\nolimits_X^2) - I(U;X \mid \sum\nolimits_X^2)] =$$
$$E_{p_{\sum_X^2}}[\max_{p(u,w\mid x)}[I(U;Y \mid \sum\nolimits_X^2 = \sigma_X^2) - I(U;X \mid \sum\nolimits_X^2 =$$
$$\sigma_X^2)]] = \int_0^\infty p_{\sum_X^2}(\sigma_X^2)[\max_{p(u,w\mid x)}[I(U;Y \mid \sum\nolimits_X^2 =$$
$$\sigma_X^2) - I(U;X \mid \sum\nolimits_X^2 = \sigma_X^2)]]\mathrm{d}\sigma_X^2 \quad (14)$$

在 Costa 研究的 AWGN 攻击信道环境下，当统计知识 $\sum_X^2 = \sigma_X^2$ 时，考虑（14）式数学期的计算问题。这时，系统的码率计算就是公式（1）中的 $R(\alpha,\sigma_X^2)$。很明显，如果编码器利用了噪声方差的信息进行了编码设计，Costa 系统就达到了信道容量，这时，解码器可以不需要信源的统计知识。但是，如果编码器未知攻击信道的状态，对于所有可能的攻击形式，需要优化选择 α，这种信息隐藏就是二义性实现问题。因此，对于所选择的 α 及其对应的码率 $R(\alpha,\sigma_X^2)$，公式（14）可以写为另一种形式：

$$R_{X,\sum_X^2}^{10,01}(\alpha) = \int_0^\infty R(\alpha,\sigma_X^2)p_{\sum_X^2}(\sigma_X^2)\mathrm{d}\sigma_X^2 \quad (15)$$

那么，通过优化选择 α 的值，信息隐藏的传输码率可以达到 DMC 的信道容量，即有关系 $R(\alpha = \alpha_{opt},\sigma_X^2) = C^{AWGN}$。所以，得到：

$$R_{X,\sum_X^2}^{10,01}(\alpha) \leqslant R(\alpha_{opt}) = C^{AWGN} \quad (16)$$

（16）中等式存在的条件是 $\alpha = \alpha_{opt} = \dfrac{\sigma_W^2}{\sigma_W^2 + \sigma_Z^2}$。因此，有：

$$R_{X,\sum_X^2}^{10,01}(\alpha) = R(\alpha_{opt})\int_0^\infty p_{\sum_X^2}(\sigma_X^2)\mathrm{d}\sigma_X^2 =$$
$$R(\alpha_{opt}) = C^{AWGN} \quad (17)$$

这样，在 Costa 研究的基础上，本文的研究方法通过对信源的 Laplacian 条件分割和 Gaussian 信道的状态实现了一种稳健信息隐藏传输的研究目标。

3 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，我们比较了不同技术方法的实现结果。图 4 显示了本文对 Costa 用优化补偿参数实现公式（2）中 AWGN 信道的系统容量。同时，对高斯和 Laplacian 信源变换的统计信号，在 WIR = −6 dB 和 WIR = −16 dB 条件下，图中分别说明了基于二进制 SCS 和 QIM（DC − DM）以及 SS 方法的 Costa 离散近似实现的容量性能分析。其中，当选择 α = 0 时，本技术应用 SS 方法实现的系统码率为：

$$R_{X,\sum_X^2}^{10,01}(0) = \int_0^\infty \frac{1}{2}\log_2(1+\frac{\sigma_W^2}{\sigma_X^2+\sigma_Z^2})p_{\sum_X^2}(\sigma_X^2)\mathrm{d}\sigma_X^2$$

而对于选择 α = 1，应用 QIM（DC − DM）方法实现的系统码率为：

$$R_{X,\sum_X^2}^{10,01}(1) = \int_0^\infty \frac{1}{2}\log_2(\frac{\sigma_W^2}{\sigma_Z^2}+\frac{\sigma_W^2}{\sigma_X^2+\sigma_Z^2})p_{\sum_X^2}(\sigma_X^2)\mathrm{d}\sigma_X^2$$

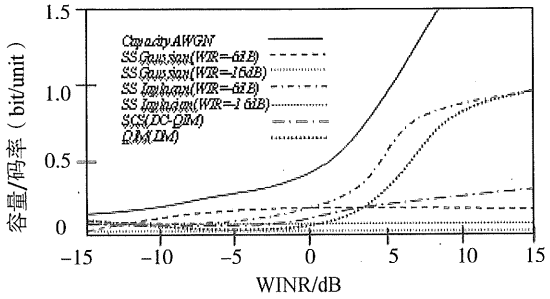

图 4 本文应用 SCS，QIM 和 SS 技术实现的 Costa 码率

Fig. 4 Achievable rate of Costa with SCS, QIM and SS

由图可见，在 Gassuian 和 Laplacian 不同信源的条件下，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 信源分割下实现的码率比 Gassuian 信源下的码率大许多。

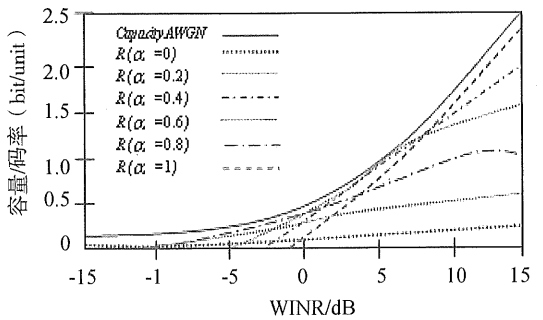

图 5 WIR = 6 dB，本文 Costa 设置不同 α 时实现 R（α，σ_x^2）码率

Fig. 5 Achievable rates of Costa（α，σ_x^2）with different α and WIR = −6 dB

按照提出的方案，为了研究边信息对解码器的影响，对 Costa 公式（1）设置不同的补偿参数 α 的值，图 5 在 WIR = −6 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公式(17)，图 6 显示了在 WIR = −6 dB 和不同补偿参数 α 的值时，解码器结合边信息进行解码，系统实现 $R_{X,\sum_X^2}^{10,01}(\alpha)$ 的不同码率。在 WIR = −6 dB 时，应用不同补偿参数 α 的值，图 7 说明了本文研究的方法和 Costa 方案实现的码率差 $R_{X,\sum_X^2}^{10,01}(\alpha) - R(\alpha)$（即率增益问题）。

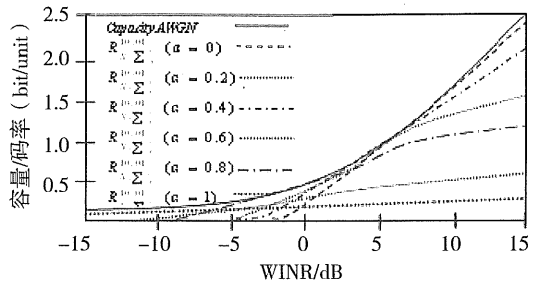

图 6　WIR = −6 dB，Costa 解码器结合边信息实现 $R_{X,\Sigma_S^2}^{10.01}(\alpha)$ 码率

Fig. 6　Achievable rates of Costa with side-informatior at the decoder $R_{X,\Sigma_S^2}^{10.01}(\alpha)$

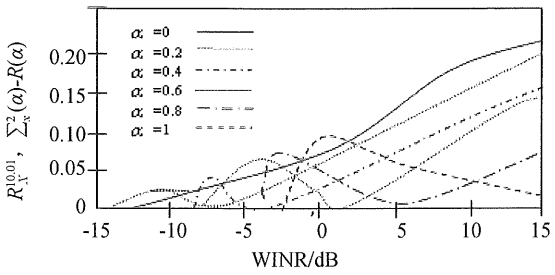

图 7　WIR = −6 dB，系统实现的率增益，$R_{X,\Sigma_S^2}^{10.01}(\alpha) - R(\alpha)$

Fig. 7　Rate gain as the difference $R_{X,\Sigma_S^2}^{10.01}(\alpha) - R(\alpha)$ for WIR = − 6 dB

由图可见，对于 SS 方法 $\alpha = 0$ 的情况，在低 WNR 环境下，$R(0)$ 达到了系统信道的传输容量；而在高 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 $R_{X,\sum_X^2}^{10,01}(0)$ 明显大于 $R(0)$。考虑 QIM 方法 $\alpha = 1$ 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，系统的性能大大降低；但是，这种情况下，本文研究实现的传输码率 $R_{X,\sum_X^2}^{10,01}(1)$ 仍然具有良好的性能。

4　结　论

在二义性 DMC − Gassuian 攻击信道条件下，考虑 Laplacian 信源分割的统计状态，本文提出了一种鲁棒的信息隐藏实现方法。该方法根据 Costa 理论分别应用了 SS 和 QIM 技术进行了系统分析。当固定补偿参数 $\alpha = 0$ 时，SS 方法是 Costa 理论的一种特殊情况。而当固定补偿参数 $\alpha = 1$ 时，QIM 方法就是 Costa 实现的一种近似逼近。同时，本文根据随机映射参数理论，在各种 α 条件下，也实现了不同 WNR 环境下一种非对称解码的折中条件，从而验证了理论分析的正确性。

参考文献：

[1] TOPAKA E, VOLOSHYNOVSKIYA S, KOVALA O, et al. Security analysis of robust data-hiding with geometrically structured codebooks[EB/OL]. [2008 − 03 − 12]. http://sip. unige. ch,2008.

[2] VOLOSHYNOVSKIYA S, KOVALA O. Data-hiding with host state at the encoder and partial side information at the decoder[EB/OL]. [2008 − 01 − 10]. http://sip. unige. ch,2008.

[3] WU Min, HONG Heather, YU Alex Gelman. Multi-level data hiding for digital image and video[J]. IEEE Transactions on Image Processing, 2007, 23(6): 1775 − 1784.

[4] COX J, MILLER L. Watermarking as Communications with Side Information[J]. Proceedings of the IEEE, 1999, 87(7): 1127 − 1140.

[5] COX J, MILLER M L B. Digital watermarking[M]. San Francisco: Morgan Kaufmann Publishers, Inc, 2001.

[6] GU Linmin, FANG Yanmei, HUANG Jiwu. Revaluation of error correcting coding in watermarking channel[J]. Proc of CANS2005, Lecture Notes Computer Science (LNCS), Springer-Verlag. Berlin, Heidelberg, 2005, 38(10): 274-287.

[7] VOLOSHYNOVSKIY S, PEREIRA S, IQUISE V. Attack modelling: Towards a second generation watermarking benchmark[J]. Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001, 8(1): 1177 − 1214.

[8] COSTA M. Writing on dirty paper[J]. IEEE Trans on Information Theory, 1983, 29(3): 439 − 441.

[9] MOULIN P, O'SULLIVAN J. Information-theoretic analysis of information hiding[J]. IEEE Trans on Information Theory, 2003, 49(3): 563 − 593.

[10] CANNONS J L, MOULIN P. Design and statistical analysis of a hash-aided image watermarking system[J]. IEEE Trans on Image Processing, 2004, 13(10): 1393 − 1406.

Laplacian Source Splitting and Parallel Gaussian Channel Transmission for Information-Hiding Technology

ZHAO Hui-min[1,2], *KANG Xian-gui*[2], *HUANG Ji-wu*[2]

(1. Department of Electronic & Information, Foshan University, Foshan Guangdong 528000, China;
2. Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: Based on Costa set-up and Cox Gaussian-decomposition for stochastic mixture source, a novel information-hiding communication technology is proposed. By means of splitting to the source with Laplacian distribution, the method forms a Markov chain between the global and local statistics of image coefficients. On the other hand, though parallel Gaussian channel according to its variances intervals, the system approaches a good transmission performances under various WNR that corresponds to the attack channel ambiguity. Comparing the theoretical results with the empirical data obtained by experimentation considered SS and QIM (DC-DM) techniques, the system resolves the trade-off between embedding capacity and channel rates as well as robust

Key words: source-splitting; information-hiding; Gaussian channel; parallel transmission; channel capacity

(上接第28页)

Experimental Investigation on Imbalance Heat Load of the Two-phase Dual-Evaporator Cooling System

LIU Jie[1], *GUO Kai-hua*[2], *HE Zhen-hui*[2], *LI Ting-xuen*[2] *LV Mou*[1]

(1. Institute of Environmental and Municipal Engineering, Qing Dao Technological University, Qingdao 266033, China; 2. Center of Space TECH, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: A brief review of the two-phase cooling loop driven by mechanical pump is presented, and a proposed experimental system with dual-Evaporator by using CO_2 as the working fluid is described. In order to apply this technology for the thermal control systems, tests have been performed to clearly comprehend its performance under cyclic temperature changing. Special attention has been paid to the heat rejection characteristics under unbalance heat load on the dual-Evaporator. From the experiments, it demonstrates that when heat load unbalance happens, the mass flow distribution between two branch has changed, the higher heat load is, the smaller mass flow is gotten. At last the mass flow would gasify completely and temperature at the outlet of a higher heat load branch would enhance. Meanwhile, decreasing heat load difference is benefit for the mass flow equalization and is an effective means for the evaporative stability. In a word, the two-phase Mechanical Pumped Cooling System with dual-Evaporator has more advantages than capillary pump cooling loop not only on the heat rejection capacity and isothermal characteristic but also on dealing with unbalance heat load.

Key words: thermal control system; driven by mechanical pump; dual-evaporator; space applications