doi:10.11959/j.issn.1000-436x.2016231

面向网络语音隐写的抗分组丢失联合编码

高瞻瞻[1]，汤光明[1]，张伟伟[2]
(1. 解放军信息工程大学，河南 郑州 450001；2. 解放军外国语学院研究生大队，河南 洛阳 471003)

摘 要：VoIP（voice over IP）是基于 UDP/IP 协议族的语音通信技术，当信道环境变差时不可避免地会产生网络分组丢失，这给建立在其上的 VoIP 隐写的可靠传输带来了挑战。提出利用纠删码对秘密信息进行冗余预处理，再结合矩阵嵌入编码实现最小失真的隐写，从而建立了基于联合编码的嵌入和提取模型。在此基础上，分析了关键参数对联合编码性能的影响并给出了最优参数的选取算法。实验结果表明，所提联合编码能够有效提高隐写系统的抗分组丢失能力，且能减少对语音流的修改。
关键词：VoIP 隐写；联合编码；分组丢失恢复；纠删码；矩阵嵌入
中图分类号：TP391 **文献标识码**：A

Anti-packet-loss joint encoding for voice-over-IP steganography

GAO Zhan-zhan[1], TANG Guang-ming[1], ZHANG Wei-wei[2]
(1. PLA Information Engineering University, Zhengzhou 450001, China;
2. Graduate Brigade, PLA University of Foreign Languages, Luoyang 471003, China)

Abstract: VoIP (voice over IP) is a kind of voice communication technology based on UDP/IP protocols. Packet loss will inevitably happen when the channel environment deteriorates, which can pose challenges to the reliable transmission of VoIP steganography. A steganographic model based on joint encoding was proposed. In this model, packet erasure coding was introduced to preprocess the secret data. And the encoded data were embedded into voice packets with minimum distortion using matrix embedding. Furthermore, the influences of key parameters on the performance of joint coding were studied. The selection algorithm for optimal parameters was also given. Experimental results show that the proposed joint coding can effectively improve steganographic resistance to packet loss, and decrease the number of modifications to the voice stream.
Key words: VoIP steganography, joint encoding, packet loss recovery, erasure coding, matrix embedding

1 引言

网络语音电话（VoIP, voice over IP）基于计算机网络技术，采用分组交换协议实现通话，比传统电路交换的方式效率更高也更经济，是未来语音通信的主要手段。与存储型载体（如图像、文本、音频、视频等）不同，VoIP 数据流为隐写术提供了更为庞大的载体空间。不仅本身所包含的语音信号可以作为隐写载体，而且其涉及的 Internet 各层网络协议也为隐写提供了良好的载体环境。不仅如此，语音数据流动态变化，它的瞬时性和“即用即弃”的特性使 VoIP 隐写具有很强的隐蔽性。如何利用 VoIP 实现隐蔽通信并消除其中潜在的安全隐患已经成为隐写术研究的热点。

依据语音信号的处理过程，可以将现有基于 VoIP 的隐写算法大致归为 2 类：基于协议的隐写和基于语音压缩编码的隐写。第一类方法主要将秘密信息嵌入到 UDP/IP 协议族中的预留、填充或可选

收稿日期：2016-05-09；**修回日期**：2016-09-01
基金项目：国家自然科学基金资助项目（No.61272488）；河南省科技攻关基金资助项目（No.122102210047）；全军军事类研究生基金资助项目（No.2015JY125）
Foundation Items: The National Natural Science Foundation of China (No.61272488), The Key Scientific and Technological Project of Henan Province (No.122102210047), The Foundation for Military Science Graduate of PLA (No.2015JY125)

字段[1]，或者通过调制发送数据分组的速率来传递秘密信息[2]；第二类方法通过替换语音分组中的不重要参数或修改语音压缩编码规则实现秘密信息的嵌入，如 Dittmann 等[3]基于 LSB 替换的抗提取 VoIP 隐写、Wei 等[4]提出的具有较高安全性的自适应隐写算法、Geiser 等[5]针对 AMR 语音编码固定码矢搜索过程设计的一种大容量隐写算法，以及 Huang 等[6]基于 G.723.1 语音编码基音周期预测过程的隐写算法。

尽管 VoIP 隐写研究已取得巨大发展，但是 VoIP 通信采用不可靠的 UDP 协议进行传输，网络分组丢失在所难免，且为保证实时性，很多 VoIP 系统在分组丢失发生时采用分组丢失隐藏技术而非恢复技术，使其中携带的秘密信息无法被正确接收。传统的顽健隐写研究主要针对图像载体，大多集中在变换域隐写[7]和基于扩频[8]的隐写，或者基于某种图像统计量的顽健性建立隐写算法[9]，应用受限。此外，另一种提高隐写顽健性的方法是采用纠错编码方法对秘密信息进行预处理后再实施嵌入。文献[10,11]建议采用具有极强纠错功能的 Repeat-Accumulate（RA）码增加信息冗余，文献[12]利用纠删编码和矩阵嵌入掩码之间的校验级联，提出一种在保证信息完整性的前提下面向最小化隐写失真的抗损矩阵嵌入框架。针对网络干扰引起的比特丢失，以上方案可以有效增强隐写的抗损、纠错性能。但信道纠错码是比特级的，无法克服链路丢帧问题，导致这些方案不能有效抵抗 VoIP 分组丢失。

针对这一问题，本文引入分组编码对秘密信息进行预处理，并将其与矩阵嵌入编码有效结合，建立了抗分组丢失的联合编码。在此基础上，通过分析关键参数对秘密信息顽健性和隐写失真的影响，给出了最优参数的选取方法。实验结果表明，所提方案能够在提高 VoIP 隐写抗分组丢失能力的同时有效减小隐写失真。

2　相关工作

2.1　删除信道与纠删编码

为设计合适的隐蔽通信系统需了解信道特性，明确其对输出编码符号的影响。为此给出如下定义。

定义 1　二进制删除信道（BEC）。输入为二值变量 0、1，输出或为输入的二值变量 0、1，或为删除 E，且通常传输过程中不同的输入编码符号被删除的概率相同。

通信系统中，接收方一般无法获知待纠正的误码位置，而在某些情况下误码错误所在的位置却可以得到，这种情况称为删除错误。基于 IP 网络的数据传输就是这样的典型例子，因为丢失的数据分组在数据流中的位置已知，这说明 VoIP 通信具有明显的删除信道特征。VoIP 隐写的秘密信息往往是经过加密处理的二值变量，它们或者被正确接收和提取，或者由于误码、拥塞、错误路由等原因而被删除。因此，可以认为 VoIP 隐蔽通信的信道是二进制删除信道。

寻找并恢复所有删除错误的过程称为纠删，用来纠正删除错误的线性码称为纠删码。用 $C_1(l,k)$ 表示一纠删码，k 为源数据的个数，l 为编码后的数据个数。纠删编码的过程可以表示成 $\boldsymbol{y}=\boldsymbol{G}_1^{\mathrm{T}}\boldsymbol{x}$。其中，$\boldsymbol{x}$ 是源数据向量，$\boldsymbol{y}$ 是编码数据向量，$\boldsymbol{G}_1$ 称为 $C_1(l,k)$ 的生成矩阵。理想的纠删码可以利用编码数据中的任意 k 个重构出源数据 $\boldsymbol{x}$。

2.2　矩阵嵌入编码

矩阵嵌入用纠错码的陪集表示载密体序列，用病灶携带秘密信息，通过寻找检验矩阵的陪集首来减小载体修改量，是提高隐写嵌入效率的有效途径。

令 $\boldsymbol{H}$ 表示线性码 $C_2(n,n-m)$ 的校验矩阵，$\boldsymbol{c}^{\mathrm{T}}\in \mathrm{GF}^n(2)$ 表示载体，秘密信息为 $\boldsymbol{m}\in \mathrm{GF}^m(2)$。对 $\boldsymbol{m}$ 和 $\boldsymbol{Hc}$ 进行按位异或运算，得到病灶 $\boldsymbol{u}=\boldsymbol{m}\oplus\boldsymbol{Hc}$，进而得到其在 $\boldsymbol{H}$ 下的陪集

$$\boldsymbol{C}_{\boldsymbol{H}}(\boldsymbol{u})=\left\{\boldsymbol{z}\in \mathrm{GF}_2^n \mid \boldsymbol{Hz}=\boldsymbol{u}\right\} \tag{1}$$

每个陪集 $\boldsymbol{C}_{\boldsymbol{H}}(\boldsymbol{u})$ 含有 2^{n-m} 个向量，其中，拥有最小汉明重量的向量称为 $\boldsymbol{C}_{\boldsymbol{H}}(\boldsymbol{u})$ 的陪集首，用 $e_L(\boldsymbol{u})$ 表示。

$$e_L(\boldsymbol{u})=\arg\min_{\boldsymbol{x}\in\boldsymbol{C}_{\boldsymbol{H}}(\boldsymbol{u})}\omega(\boldsymbol{x}) \tag{2}$$

具有最小失真的载密体 $\boldsymbol{s}$ 可通过式(3)得到。

$$\boldsymbol{s}=\boldsymbol{c}\oplus e_L(\boldsymbol{u}) \tag{3}$$

接收端用校验矩阵 $\boldsymbol{H}$ 左乘 $\boldsymbol{s}$ 即可正确提取秘密信息。如何以较低的计算复杂度找到陪集首是矩阵嵌入设计的核心。目前，针对存储型载体的矩阵嵌入研究已较为成熟，如 Filler 等[13]提出的量化格子编码（STC 码），其嵌入效率接近理论上限。设计适宜网络语音的矩阵嵌入编码来减小隐写失真、提高抗检测性是 VoIP 隐写的一个重要方向。如 Tian 等[14]对汉明码校验矩阵的结构进行改造，克服了汉明码只能实现个别嵌入率的缺点，所提 AME 编码更适用于 VoIP 隐写。Yan 等[15]根据 G.729 语音帧中

各参数承载秘密信息能力的不同，将载体数据分为三元和二元 2 类并提出了一种 3 层隐写编码。

3 抗分组丢失联合编码

本文提出对秘密信息进行纠删编码预处理，然后利用矩阵嵌入编码实施隐写，设计了面向 VoIP 隐写的抗分组丢失联合编码，其嵌入和提取模型如图 1 所示。不同于比特误码，为抵抗网络分组丢失，模型引入了纠删分组编码技术。分组编码以数据块为单位进行前向纠错。通过将数据块内相同位置上的比特进行位编码，再按编码时的位置组合所得冗余位，从而得到具有纠删能力的编码数据块。

依据抗分组丢失联合编码模型，信息嵌入的具体过程如下。

步骤 1 发送方首先对秘密信息 $\boldsymbol{m}(|\boldsymbol{m}|=M)$分组，形成 k 个信息块 $\boldsymbol{m}^{\mathrm{T}}=(\boldsymbol{m}_1^{\mathrm{T}},\boldsymbol{m}_2^{\mathrm{T}},\cdots,\boldsymbol{m}_k^{\mathrm{T}})$。

步骤 2 记纠删码 $C_1(l,k)$ 对应的生成矩阵为 $\boldsymbol{G}_1=\{0,1\}^{k\times l}$，校验矩阵为 $\boldsymbol{H}_1=\{0,1\}^{(l-k)\times l}$。利用式（4）将信息块中对应比特进行位编码。

$$(\hat{m}_{1,j},\hat{m}_{2,j},\cdots,\hat{m}_{l,j})^{\mathrm{T}}=\boldsymbol{G}_1^{\mathrm{T}}(m_{1,j},m_{2,j},\cdots,m_{k,j})^{\mathrm{T}},\quad j\in\{1,2,\cdots,\frac{M}{k}\}\tag{4}$$

其中，$m_{i,j}$ 表示第 i 个源信息块的第 j 个元素，$\hat{m}_{i,j}$ 表示第 i 个编码信息块的第 j 个元素。组合所得编码元素形成编码信息块 $\hat{\boldsymbol{m}}^{\mathrm{T}}=(\hat{\boldsymbol{m}}_1^{\mathrm{T}},\hat{\boldsymbol{m}}_2^{\mathrm{T}},\cdots,\hat{\boldsymbol{m}}_l^{\mathrm{T}})$。

步骤 3 将编码信息块 $\hat{\boldsymbol{m}}_i$，$i\in\{1,2,\cdots,l\}$ 作为二元线性码 $C_2(n,n-\frac{M}{k})$ 的伴随式，通过矩阵嵌入隐藏到数据分组 $\boldsymbol{X}_i$ 中。其中，n 表示数据分组内载体元素的个数。记码 $C_2(n,n-\frac{M}{k})$ 对应的校验矩阵为 $\boldsymbol{H}_2=\{0,1\}^{\frac{M}{k}\times n}$，此时具有最小失真的载密体通过式(5)得到。

$$\boldsymbol{Y}_i=\boldsymbol{X}_i+\arg\min_{\boldsymbol{x}\in C_{\boldsymbol{H}_2}(\boldsymbol{u})}\omega(\boldsymbol{x}),\ C_{\boldsymbol{H}_2}(\boldsymbol{u})=\{\boldsymbol{z}\in\{0,1\}^n\mid\boldsymbol{H}_2\boldsymbol{z}=\boldsymbol{u}\}\tag{5}$$

信息提取过程如下。

步骤 1 接收方利用校验矩阵 $\boldsymbol{H}_2$ 从接收的数据分组 $\boldsymbol{Y}^*=\{\boldsymbol{Y}_1^*,\boldsymbol{Y}_2^*,\cdots,\boldsymbol{Y}_l^*\}$ 中提取秘密信息 $\{\hat{\boldsymbol{m}}_1^*,\hat{\boldsymbol{m}}_2^*,\cdots,\hat{\boldsymbol{m}}_l^*\}$。若某数据分组 $\boldsymbol{Y}_i^*$ 因受损等原因被删除，则 $\hat{\boldsymbol{m}}_i^*=\varnothing$。

$$\hat{\boldsymbol{m}}_i^*=\boldsymbol{H}_2\boldsymbol{Y}_i^*\tag{6}$$

步骤 2 基于纠删码译码恢复出被删除的信息块。用 $\kappa=\{i:\boldsymbol{m}_i^*\neq\varnothing\}$ 和 $\bar{\kappa}=\{i:\boldsymbol{m}_i^*=\varnothing\}$ 分别代表秘密信息 $\{\hat{\boldsymbol{m}}_1^*,\hat{\boldsymbol{m}}_2^*,\cdots,\hat{\boldsymbol{m}}_l^*\}$ 中完好信息块与损毁信息块的索引集合。依照 κ 和 $\bar{\kappa}$ 将集合 $\{\hat{\boldsymbol{m}}_1^*,\hat{\boldsymbol{m}}_2^*,\cdots,\hat{\boldsymbol{m}}_l^*\}$ 划分为完好信息子集 $\boldsymbol{m}_\kappa^*=\{\boldsymbol{m}_i^*:i\in\kappa\}$ 和受损信息子集 $\boldsymbol{m}_{\bar{\kappa}}^*=\{\boldsymbol{m}_i^*:i\in\bar{\kappa}\}$。相应地，校验矩阵 $\boldsymbol{H}_1$ 按列划分为对应的 2 个子矩阵 $\boldsymbol{H}_{1\kappa}$ 和 $\boldsymbol{H}_{1\bar{\kappa}}$。在子矩阵 $\boldsymbol{H}_{1\bar{\kappa}}$ 各列不相关的前提下，纠删码可通过高斯消元求解式(7)来恢复受损信息。

$$\boldsymbol{H}_{1\bar{\kappa}}\boldsymbol{m}_{\bar{\kappa},j}^*=\boldsymbol{H}_{1\kappa}\boldsymbol{m}_{\kappa,j}^*,\ j\in\{1,2,\cdots,\frac{M}{k}\}\tag{7}$$

其中，$\boldsymbol{m}_{\kappa,j}^*$ 表示所有完好信息块内第 j 个元素构成的向量，$\boldsymbol{m}_{\bar{\kappa},j}^*$ 表示受损信息块第 j 个元素构成的向量。组合所得元素即可恢复受损信息块 $\boldsymbol{m}_{\bar{\kappa}}^*$。

步骤 3 合并各信息块得到最初的秘密信息。

4 联合编码的性能分析

如何实现纠删编码与矩阵嵌入编码的最优联合，保证 VoIP 隐写在一定删除概率下既能成功译码又能最小化嵌入影响是该模型需要解决的首要问题。为此，本节分析关键参数对联合编码性能的影响。

4.1 联合编码的抗分组丢失能力

用 p 表示单个数据分组通过二元删除信道后被

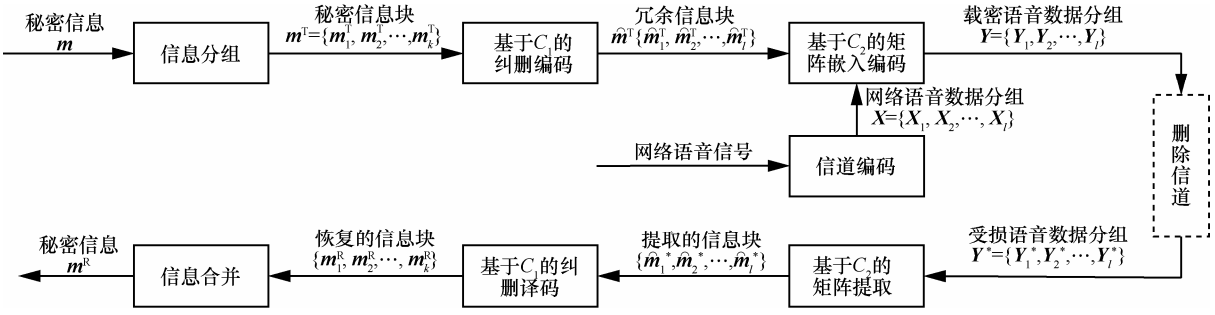


图 1 抗分组丢失联合编码的信息嵌入和提取模型

正确接收的概率，用随机变量 X 表示经信道传输后可用的载密数据分组个数，则随机变量 X 服从二项分布，$X \sim \mathrm{B}(l,p)$。以一定删除概率下收方获得完整秘密信息的概率 P_{suc} 来描述本文联合编码的抗分组丢失能力。理想的纠删码能够在接收方得到任意 k 个编码信息块后成功译码，因此，依据伯努利概型可知

$$P_{\mathrm{suc}} = 1 - \sum_{i=0}^{k-1} \mathrm{C}_l^i p^i (1-p)^{l-i} \tag{8}$$

记纠删码的冗余度 $w = \dfrac{l}{k}$。依据上式建立 P_{suc} 与初始秘密信息分组数 k、编码冗余度 w 的关系

$$F(k,w) \overset{\mathrm{def}}{=} P_{\mathrm{suc}} = 1 - \sum\nolimits_{i=0}^{k-1} \mathrm{C}_{kw}^i p^i (1-p)^{kw-i} \tag{9}$$

从式（9）可见，初始信息分组数和冗余度是影响联合编码抗分组丢失能力的关键参数。下面分别研究它们对编码性能的影响。

定理 1　给定数据分组被正确接收的概率 p，若冗余度 w 不变，则当 $w < \dfrac{1}{p}$ 时，$\lim\limits_{k\to\infty} F(k,w) = 0$；当 $w = \dfrac{1}{p}$ 时，$\lim\limits_{k\to\infty} F(k,w) = \dfrac{1}{2}$；当 $w > \dfrac{1}{p}$ 时，$\lim\limits_{k\to\infty} F(k,w) = 1$。

证明

1) 随机变量 $X \sim \mathrm{B}(l,p)$，故其数学期望 $\mu = lp = kwp$，方差 $\sigma^2 = kwp(1-p)$。

$$\begin{aligned} F(k,w) &= \sum_{i=k}^{kw} \mathrm{C}_{kw}^i p^i (1-p)^{kw-i} \\ &= P(X \geqslant k) = P(X - \mu \geqslant k - \mu) \end{aligned}$$

当 $w < \dfrac{1}{p}$ 时，$k - \mu = k - kwp > k - kp \cdot \dfrac{1}{p} = 0$。

依据切比雪夫不等式，有下式成立：$P(X-\mu \geqslant k-\mu) \leqslant \dfrac{\sigma^2}{(k-\mu)^2}$。

进一步可得 $F(k,w) \leqslant \dfrac{\sigma^2}{(k-\mu)^2} = \dfrac{wp(1-p)}{k(1-wp)^2}$。

在这种情况下，若 w 一定，$\lim\limits_{k\to\infty} F(k,w) = \lim\limits_{k\to\infty} \dfrac{wp(1-p)}{k(1-wp)^2} = 0$。

2) 随机变量 $X \sim \mathrm{B}(l,p)$，依据棣莫弗－拉普拉斯中心极限定理有下式成立。

$$\begin{aligned} \lim_{k\to\infty} F(k,w) &= \lim_{kw\to\infty} F(k,w) = 1 - \lim_{kw\to\infty} P(X \leqslant k-1) \\ &= 1 - \lim_{kw\to\infty} P\left(\frac{X - kwp}{\sqrt{kwp(1-p)}} \leqslant \frac{k-1-kwp}{\sqrt{kwp(1-p)}} \right) \\ &= 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t \end{aligned}$$

当 $w = \dfrac{1}{p}$ 时，$x = \dfrac{k-1-kwp}{\sqrt{kwp(1-p)}} = \dfrac{-1}{\sqrt{k(1-p)}}$。故

$$\begin{aligned} \lim_{k\to\infty} F(k,w) &= 1 - \left(\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{0} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t - \frac{1}{\sqrt{2\pi}} \int_{\frac{-1}{\sqrt{k(1-p)}}}^{0} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t \right) \\ &= 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{0} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t + \frac{1}{\sqrt{2\pi}} \int_{\frac{-1}{\sqrt{k(1-p)}}}^{0} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t \\ &= \frac{1}{2} + \frac{1}{\sqrt{2\pi}} \int_{\frac{-1}{\sqrt{k(1-p)}}}^{0} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t \end{aligned}$$

在这种情况下，若 w 一定，$\lim\limits_{k\to\infty} F(k,w) = \dfrac{1}{2} + \lim\limits_{k\to\infty} \dfrac{1}{\sqrt{2\pi}} \int_{\frac{-1}{\sqrt{k(1-p)}}}^{0} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t = \dfrac{1}{2}$。

3) $F(k,w) = 1 - P(X \leqslant k-1) \geqslant 1 - P(X \leqslant k) = 1 - P(X - \mu \leqslant k - \mu)$

当 $w > \dfrac{1}{p}$ 时，$k - \mu = k - kwp < 0$。

依据切比雪夫不等式有下式成立。

$$P(X - \mu \leqslant k - \mu) \leqslant \frac{\sigma^2}{(k-\mu)^2}$$

进一步可得

$$F(k,w) \geqslant 1 - \frac{\sigma^2}{(k-\mu)^2} = 1 - \frac{wp(1-p)}{k(1-wp)^2}$$

因此，$1 - \dfrac{wp(1-p)}{k(1-wp)^2} \leqslant F(k,w) < 1$。

在这种情况下，若 w 一定，$k \to \infty$ 会令 $F(k,w) \to 1$。

证毕。

由定理 1 及其证明过程可知，若冗余度固定，只有当 $w > \dfrac{1}{p}$ 时，联合编码的抗分组丢失能力随初始信息分组数单调递增。其他情况下增加分组个数反而会降低系统的抗损能力。这也就意味着冗余度 $w > \dfrac{1}{p}$ 时应用纠删编码才有意义，否则，不如对秘密信息整体进行冗余复制。因此，应用联合编码应

保证 $w>\frac{1}{p}$。在此前提下，有定理 2 成立。

定理 2 给定数据分组被正确接收的概率 p，若初始信息分组数 k 不变且 $w>\frac{1}{p}$，联合编码的抗分组丢失能力随着冗余度的增加逐渐增强。

证明 记 $a_i(kw)=\mathrm{C}_{kw}^{i}p^{i}(1-p)^{kw-i}$，$i\in\{0,1,\cdots,k-1\}$，则 $F(k,w)=1-\sum_{i=0}^{k-1}a_i(kw)$。

$$\begin{aligned}\frac{a_i(kw+1)}{a_i(kw)}&=\frac{\mathrm{C}_{kw+1}^{i}p^{i}(1-p)^{kw+1-i}}{\mathrm{C}_{kw}^{i}p^{i}(1-p)^{kw-i}}\\&=\frac{(kw+1)(1-p)}{kw+1-i}\\&=1+\frac{i(1-p)-(kw+1-i)p}{kw+1-i}\\&=1+\frac{i-(kw+1)p}{kw+1-i}\end{aligned}$$

当 $w>\frac{1}{p}$ 时，对于任一 $\frac{a_i(kw+1)}{a_i(kw)}$ 有 $i<k+p<(kw+1)p$。又由于 $i<kw+1$，故 $\frac{i-(kw+1)p}{kw+1-i}<0$，即 $\frac{a_i(kw+1)}{a_i(kw)}<1,\quad i\in\{0,1,\cdots,k-1\}$。

因此，$1-\sum_{i=0}^{k-1}a_i(kw+1)>1-\sum_{i=0}^{k-1}a_i(kw)$。

在这种情况下，若 k 一定，$F(k,w)$ 随着 w 的增加单调递增。

证毕。

综合定理 1 和定理 2，应用本文提出的联合编码进行隐蔽通信时，应保证冗余度 $w>\frac{1}{p}$；在此前提下，增大初始信息分组数或进一步增大冗余度都可以有效地提升联合编码的抗分组丢失能力。

4.2 联合编码的抗检测能力

VoIP 通信实时性要求高，隐写发送方不宜对语音流 X 实施缓存，也就不能根据各数据分组对隐写耐受性的差异实现全局最优的嵌入。因此，本文将网络流中的数据分组近似处理，假设它们适宜隐写的程度相当。在此前提下研究秘密信息嵌入引起的语音流失真，并用失真大小来描述本文联合编码的抗检测能力。针对某种信息分组方式 $\boldsymbol{m}^{\mathrm{T}}=(\boldsymbol{m}_1^{\mathrm{T}},\boldsymbol{m}_2^{\mathrm{T}},\cdots,\boldsymbol{m}_k^{\mathrm{T}})$，$\boldsymbol{m}_i$ 的长度记为 r_i。$\boldsymbol{m}_i$ 依序列 $\boldsymbol{\zeta}$ 嵌入总数为 N 的语音分组中，序列 $\boldsymbol{\zeta}$ 构成集合 $\boldsymbol{S}_N$。此时语音流总的失真的期望为

$$D(\boldsymbol{X},\boldsymbol{Y})=\mathrm{E}\left(\frac{1}{N!}\sum_{\boldsymbol{\zeta}\in\boldsymbol{S}_N}\sum_{i=1}^{k}D(X_{\boldsymbol{\zeta}(i)},Y_{\boldsymbol{\zeta}(i)}^{\boldsymbol{m}_i})\right)\tag{10}$$

将秘密信息视为随机串，又由于各语音数据分组具有近似相同的隐写特性，上式可简化为

$$D(\boldsymbol{X},\boldsymbol{Y})=\mathrm{E}\left(\sum_{i=1}^{k}D(X_i,Y_i^{\boldsymbol{m}_i})\right)=\mathrm{E}\left(\sum_{i=1}^{k}\frac{r_i}{e_i^{r_i}}\right)=\sum_{i=1}^{k}\frac{r_i}{e^{r_i}}\tag{11}$$

其中，e^{r_i} 表示各数据分组嵌入 r_i 比特秘密信息时的嵌入效率。据此得到定理 3。

定理 3 针对联合编码下的 VoIP 隐写，载体失真随冗余度 w 的增大而增大；若 w 不变，最优的秘密信息分组数 $k^{\mathrm{opt}}=\arg\max_k e^{\frac{M}{k}}$。

证明 秘密信息 m 的长度为 M，因此，初始信息分组数为 k 时各信息块的长度 $r_i=\frac{M}{k},\ i\in\{1,2,\cdots,k\}$。纠删处理增加了信息块，真正被嵌入的分组个数 $l=kw$，隐写对载体数据流带来的总失真为

$$\begin{aligned}G(k,w)\overset{\mathrm{def}}{=}D(\boldsymbol{X},\boldsymbol{Y})&=\sum_{i=1}^{l}\frac{\frac{M}{k}}{e^{\frac{M}{k}}}=l\cdot\frac{M}{k}\cdot\frac{1}{e^{\frac{M}{k}}}\\&=kw\cdot\frac{M}{k}\cdot\frac{1}{e^{\frac{M}{k}}}=M\frac{w}{e^{\frac{M}{k}}}\end{aligned}$$

由 $G(k,w)$ 的函数形式易知，载体失真随冗余度 w 线性递增；若 w 不变，最小化失真应选择使 $e^{\frac{M}{k}}$ 取最大值时的分组数。

证毕。

当载体元素个数 $n=100$ 时，实验得到不同嵌入率下几种常见矩阵嵌入编码的嵌入效率，结果如图 2 所示。

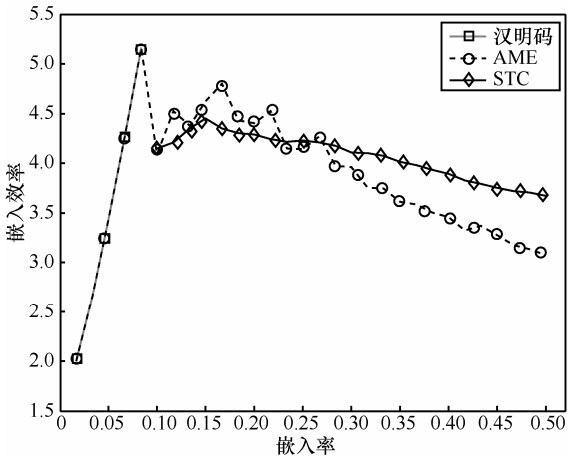


图 2 几种矩阵嵌入编码的嵌入效率

由图 2 可知，矩阵嵌入编码的嵌入效率虽有起伏，但基本呈现先增大后减小的趋势。基于这一变化规律，并结合定理 1 和定理 3 可知：对于确定的秘密信息和载体集，$k \leqslant k^{\text{opt}}$ 时，增大初始信息分组数 k 既能提高抗分组丢失能力又能减小隐写失真；$k > k^{\text{opt}}$ 时，增大 k 能提高抗分组丢失能力但会增大失真。

5　最优参数的选取

联合编码的关键参数为初始信息分组数 k 和冗余度 w，二者对隐蔽通信系统的抗分组丢失能力和抗检测能力都具有至关重要的影响，如果选取不恰当，难免顾此失彼。基于第 4 节分析，本节在数据分组删除概率已知的情况下给出选取 k、w 的具体算法，使联合编码达到最优。

理想的 VoIP 隐写既具有很强的抗分组丢失能力，同时又能最小化嵌入带来的影响，以此为目标进行参数优化。语音流中所含的数据分组个数为 N，如果编码信息块的数量 kw 超过 N，那么至少有 2 个编码信息块会被嵌入到同一个数据分组中，导致信息块的删除概率相互间不再独立。因此，应限定 $kw \leqslant N$。最优的 k 和 w 通过求解以下优化问题确定。

$$\begin{cases} \max\ F(k,w) = 1 - \sum_{i=0}^{k-1} \mathrm{C}_{kw}^{i} p^{i} (1-p)^{kw-i} \\ \min\ G(k,w) = M \dfrac{w}{e^{\frac{M}{k}}} \\ \text{s.t.}\quad kw \leqslant N,\ w \geqslant \dfrac{1}{p} \\ \qquad k \in \{1,2,\cdots,N\} \end{cases} \tag{12}$$

参数选取的具体算法如下。

输入　数据分组正确接收的概率 p，数据分组个数 N，数据分组内载体元素个数 n，秘密信息长度 M，抗分组丢失要求 P^{req}

输出　初始信息分组数 k，冗余度 w

步骤 1　初始化 $k = \left\lceil \dfrac{M}{n} \right\rceil$，$w = \dfrac{1}{p} + \gamma$，$\gamma$ 为较小的正数。依据矩阵嵌入编码嵌入效率的变化情况，找到嵌入效率最高时对应的嵌入率 α^{opt}，计算出相应的分组个数 $k^{\text{opt}} = \dfrac{M}{n\alpha^{\text{opt}}}$。

步骤 2　计算 $F(k,w)$，判断是否满足抗分组丢失要求。若 $F(k,w) \geqslant P^{\text{req}}$，进入步骤 3；否则进入步骤 4。

步骤 3　此时已满足抗分组丢失要求，在 $k \leqslant \dfrac{N}{w}$ 且 $k \leqslant k^{\text{opt}}$ 成立的前提下，逐步递增分组数 k 来进一步减小隐写失真，输出 w 及满足条件时最大的 k。

步骤 4　定义辅助函数为

$$F'(k,w) = \begin{cases} P^{\text{req}} - F(k,w), & F(k,w) < P^{\text{req}} \\ 0, & F(k,w) \geqslant P^{\text{req}} \end{cases} \tag{13}$$

引入惩罚参数 θ（θ 一般取值很大），将式(12)中的 2 个目标转化为如下单一目标

$$H(k,w) = G(k,w) + \theta F'(k,w) \tag{14}$$

在 $w \leqslant \dfrac{N}{k}$ 成立的前提下逐步递增 w，依式(14)计算并存储相应的 $H(k,w)$。

步骤 5　若 $k < \dfrac{N}{\frac{1}{p} + \gamma}$，$k = k + 1$ 并返回步骤 4；否则比较 $H(k,w)$，找到使其最小的参数组合并输出。

若冗余度仅取整数，步骤 4、步骤 5 循环遍历的次数约为 $\sum_{i=\left\lceil \frac{M}{n} \right\rceil}^{\left\lfloor k < \frac{N}{\frac{1}{p}+\gamma} \right\rfloor} \left(\left\lfloor \dfrac{N}{i} \right\rfloor - \left\lceil \dfrac{1}{p} + \gamma \right\rceil \right)$。考虑到矩阵编码（如汉明码）可能只适用于部分嵌入率，这会限制初始分组数的备选范围，因此实际的循环次数会更少。

6　实验结果与分析

本文所提基于联合编码的嵌入和提取模型是一种通用模型，适用于多种 VoIP 隐写算法。下面以 2 个实验为例说明该模型的有效性。

6.1　实验 1

针对 G.723.1 6.3 kbit/s 语音帧，文献[16]采用语音质量感觉评估（PESQ）方法对帧中各比特的抗噪性进行测试，选取了 18 bit 的最低有效位。在此基础上，结合矩阵嵌入编码和 LSB 替换隐写提出 CLFW 算法，算法具有较大的隐写容量。RS 编码是唯一可以满足任意个数的编码数据（l）和初始数据（k）的 MDS（maximum distance separable）编码方法，即达到了理论上最优的纠删性能[17]。Tian 等[14]的嵌入编码在 VoIP 隐写下性能较好。采用以上隐写算法和编码进行实验。其中，RS 码具体使

用的是柯西码。

一个语音 IP 分组中包含的语音帧数目越多，语音帧越大，实际占用的带宽就越小[18]。但分组中的语音帧越多，语音编解码器的处理时延就越大。除此之外，编/解码还有不可避免的算法时延，G.723.1（6.4 kbit/s）一帧的时延为 37.5 ms。通常认为 150 ms 以下的时延经过一定的处理后可以被正常接收；大于这个值就会严重影响语音的传输质量。考虑到以上问题，一个 IP 分组典型情况下装载 3 个 G.723.1 语音帧，分组内的载体元素个数 $n=18\times3=54$。此时，Tian 等[14]的矩阵编码的嵌入效率如图 3 所示。

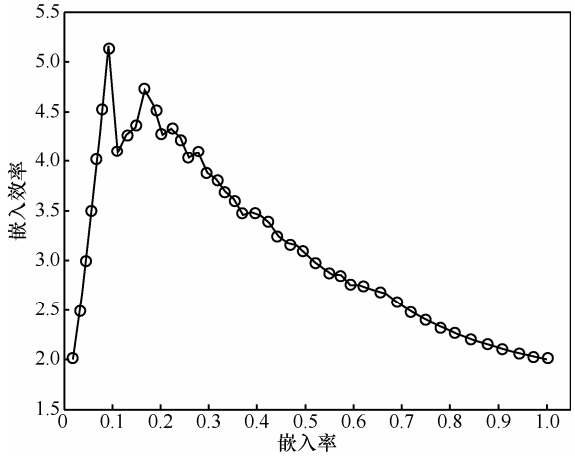


图 3　Tian 等[14]的矩阵编码在不同嵌入率下的嵌入效率（n=54）

图 3 中的嵌入率表示实际嵌入的信息量与载体元素数之比，而非数据分组内全部的比特数。由图 3 可知，$\alpha^{\text{opt}}=\dfrac{5}{54}$。RS 码具有较大的编解码复杂度，这限制了编码码长，实验中取数据分组个数 $N=40$。实验要求隐蔽通信失败的概率低于 0.1，即 $P^{\text{req}}=0.90$。依参数选取算法得到各嵌入量下的最优参数，如表 1 所示。

表 1 显示许多嵌入量下都无法应用联合编码，这是因为随着信道删除概率的增大，联合编码对冗余度的要求不断增加，导致有限的数据分组不足以嵌入秘密信息。依联合编码过程并利用所得最优参数进行秘密的嵌入和提取，统计其嵌入效率。将接收端译码结果与源秘密信息比对，计算接收端译码成功的概率。实验结果如图 4、图 5 所示。图 4 数据说明,联合编码在多数嵌入率下的译码成功率都超过了 90%，具备抗分组丢失能力。值得注意的是，图 5 中嵌入效率表示源秘密信息大小与嵌入修改量的比值，而非编码信息量与修改量的比值。

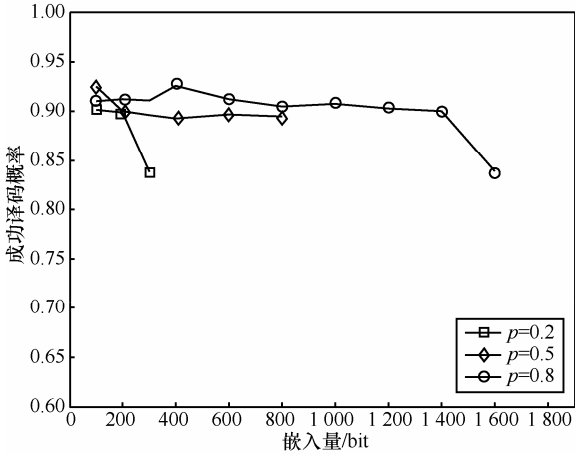


图 4　联合编码下接收端成功译码的概率（实验 1）

表 1　　联合编码的最优参数（P^{req}=0.90, N=40）

嵌入量 M/bit	p=0.2		p=0.5		p=0.8	
	初始分组数 k	冗余度 w	初始分组数 k	冗余度 w	初始分组数 k	冗余度 w
100	5	7.6	12	2.583 3	23	1.391 3
200	5	7.6	16	2.437 5	29	1.350 0
300	6	6.666 7	16	2.437 5	26	1.384 6
400	—	—	16	2.437 5	28	1.392 9
600	—	—	16	2.437 5	29	1.379 3
800	—	—	16	2.437 5	29	1.379 3
1 000	—	—	—	—	29	1.379 3
1 200	—	—	—	—	29	1.379 3
1 400	—	—	—	—	29	1.379 3
1 600	—	—	—	—	30	1.333 3
1 800	—	—	—	—	—	—

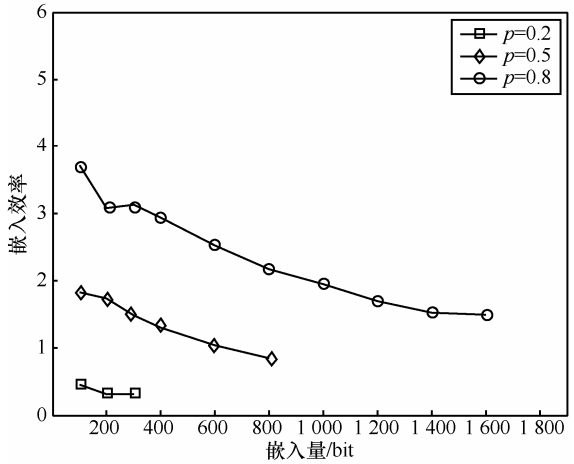


图 5　联合编码的嵌入效率（实验 1）

保持 $p=0.8$ 和 $M=400$ 不变，选取不同可靠性要求 $P^{\text{req}}=\{0.99,0.95,0.90,0.75,0.60,0.45,0.30,0.20\}$ 下的联合编码最优参数，进而得到成功译码概率与嵌入效率间的关系，并与 Liu 等[12]的方法对比，如图 6 所示。Liu 等的方法基于系统卷积码和网格码 STCs 设计，属于比特级顽健隐写，因此实验中需对秘密信息整体进行纠删处理，编码难度大。图中各点反映的是该方法在纠删编码码率取 $\left\{\frac{1}{3},\frac{3}{8},\frac{2}{5},\frac{1}{2},\frac{2}{3},\frac{3}{4},\frac{4}{5},\frac{5}{6}\right\}$ 时的抗损性及嵌入效率（STC 子矩阵高 $h=10$）。由图 6 可知，相同抗分组丢失能力下本文方法的嵌入效率更高。

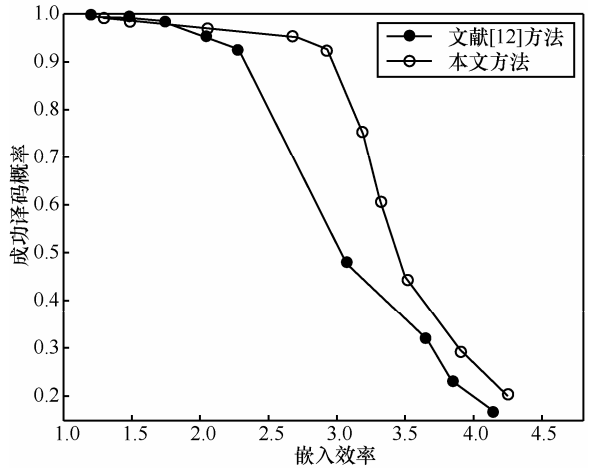


图 6　成功译码概率与嵌入效率间的关系（实验 1）

6.2　实验 2

实验 1 所述隐写方案的嵌入量有限，为解决这一问题，考虑增加数据分组个数 N。RS 码编译码复杂度大，不宜继续使用，而 Raptor 码是一类基于图的线性纠错码，可用于对长码进行编码。Raptor 码没有固定码率，发送端能生成无限多的编码分组。当接收端信道条件不好，分组丢失较多的时候，只要接收更多的编码分组就可以了。Tian 等[14]的矩阵嵌入编码是对汉明码的改进，在大嵌入率下的嵌入效率不如 STC 码。基于以上分析进行实验 2，实验同样基于 CLFW 算法，但联合编码使用的是 Raptor 码、STC 码。

首先得到 STC 码在 $n=54$ 时的嵌入效率，如图 7 所示。实验中设定子矩阵高 $h=8$。理论上 STC 码的嵌入效率随嵌入率的减小而增大，但由于码长较短，其卷积编码的优势无法发挥，因此，在嵌入率极小时实际的嵌入效率有所下降。

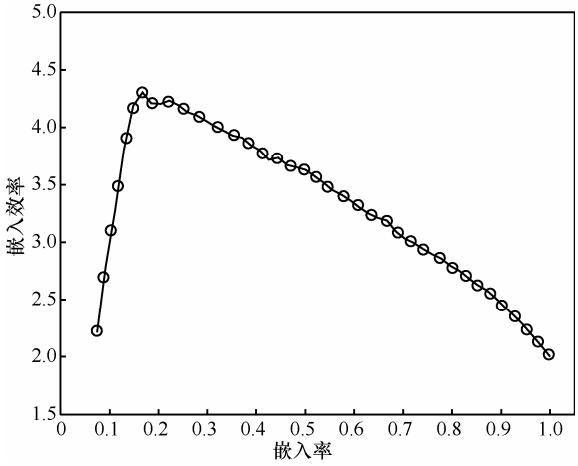


图 7　STC 码在不同嵌入率下的嵌入效率（n=54）

Raptor 码不是 MDS 码，接收端需要接收略大于源数据分组个数的编码数据分组才能正确译码。因此，式（8）可以修正为

$$P_{\text{suc}}=1-\sum_{i=0}^{(1+\varepsilon)k-1}\mathrm{C}_l^i p^i(1-p)^{l-i} \tag{15}$$

进一步可推知此时联合编码应保证冗余度 $w>\frac{1+\varepsilon}{p}$，其他结论同定理 1、定理 2。依经验取 $\varepsilon=0.2$ 并按参数选取算法得到此时的最优参数如表 2 所示。表 2 中 w 表示解码端成功译码时的编码冗余度的期望。

利用最优参数进行联合编码嵌入和提取。图 8 显示的是在发送数据分组个数等于期望冗余度时的译码成功率。嵌入效率的变化如图 9 所示。所得结果说明基于联合编码的隐写在抵抗分组丢失的同时具有较高的嵌入效率。

表 2　　联合编码的最优参数（P^{req}=0.90, N=200）

嵌入量 M/bit	p=0.2		p=0.5		p=0.8	
	初始分组数 k	冗余度 w	初始分组数 k	冗余度 w	初始分组数 k	冗余度 w
100	14	7.428 6	14	2.785 7	20	1.650 0
200	24	7.125 0	24	2.750 0	40	1.650 0
300	27	7.148 1	37	2.702 7	34	1.617 6
400	28	7.107 1	49	2.653 1	49	1.591 8
600	28	7.107 1	74	2.608 1	69	1.579 7
800	28	7.107 1	69	2.623 2	99	1.565 7
1 000	28	7.107 1	74	2.608 1	114	1.561 4
1 200	28	7.107 1	75	2.626 7	104	1.567 3
1 400	28	7.107 1	74	2.608 1	119	1.563 0
1 600	30	6.666 7	74	2.608 1	128	1.562 5
1 800	—	—	75	2.626 7	128	1.562 5

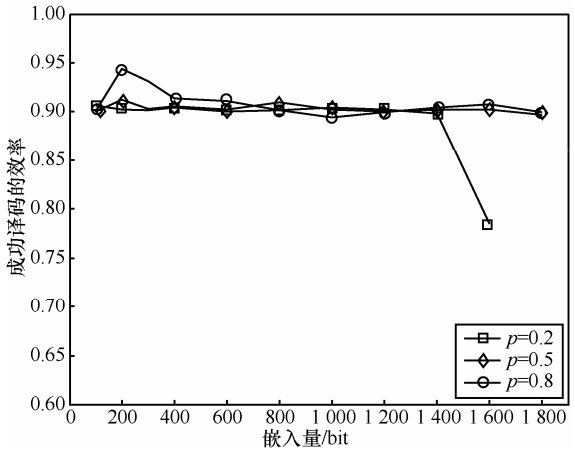


图 8　联合编码下接收端成功译码的概率（实验 2）

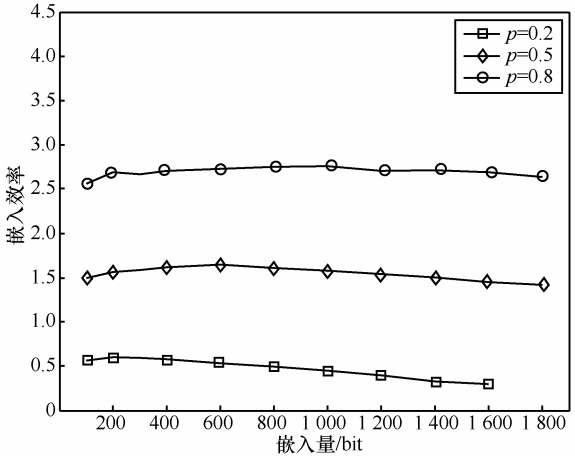


图 9　联合编码的嵌入效率（实验 2）

保持 $p=0.8$ 和 $M=2\,000$ 不变，选取不同可靠性要求下的最优参数，明确此时成功译码概率与嵌入效率间的关系。为体现方法本身的影响，实验同样令 Liu 等[12]方法的子矩阵 $h=8$，实验结果如图 10 所示。由于纠删编码和嵌入编码选取的变化，联合编码的嵌入效率与实验一相比有所下降，但仍优于已有方法。

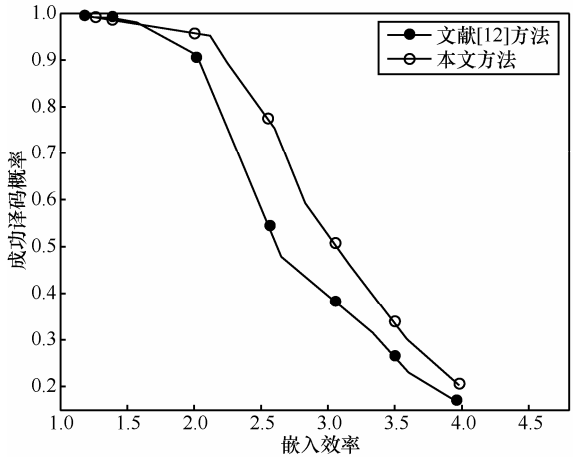


图 10　成功译码概率与嵌入效率间的关系（实验 2）

7　结束语

VoIP 通信存在不可避免的网络分组丢失，为了保证建立在 VoIP 信道上的隐蔽通信的可靠性，本文结合纠删编码与矩阵嵌入编码，提出基于联合编码的隐写模型。将待传输的秘密信息分组，通过分组编码获得冗余的信息块，再利用矩阵嵌入编码将纠删处理后的信息块嵌入到语音数据分组中；当某些数据分组丢失时，接收方利用与之关联的冗余信息块将其恢复。相关实验表明，所提模型适用于多种隐写算法和编码方式，能够在各种信道环境下保

证隐蔽通信的顽健性，且具有较高的嵌入效率。需要说明的是，为简化表达，本文模型将语音流中的数据分组进行了等效处理，具体应用时可以将数据分组先分类（如静音分组、非静音分组）再实施隐写，使模型更接近实际，进一步提升编码效果。

参考文献：

[1] MURDOCH S, LEWIS S. Embedding covert channels into TCP/IP[C]// Proceedings of 7th Information Hiding Workshop. Barcelona, Spain, 2005, 3727: 247-261.

[2] CABUK S, BRODLEY C E, SHIELDS C. IP covert timing channels: design and detection[C]//Proceedings of the 11th ACM Conference on Computer and Communications Security. CCS 2004, Washington, DC, USA, 2004: 178-187.

[3] DITTMANN J, HESSE D, HILLERT R. Steganography and steganalysis in voice over IP scenarios: operational aspects and first experiences with a new steganalysis tool set[C]// Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents. San Jose, California, USA, 2005, 5681: 607-618.

[4] WEI Z, ZHAO B, LIU B, et al. A novel steganography approach for voice over IP[J]. Journal of Ambient Intelligence & Humanized Computing, 2014, 5(4):601-610.

[5] GEISER B, VARY P. High rate data hiding in ACELP speech codecs[C]// Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing. Las Vegas, Nevada, USA, 2008: 4005-4008.

[6] HUANG Y F, LIU C H, TANG S Y, et al. Steganography integration into a low-bit rate speech codec[J]. IEEE Transaction on Information Forensics and Security, 2012, 7(6): 1865-1875.

[7] ZHAO M, DANG Y. Color image copyright protection digital watermarking algorithm based on DWT&DCT[C]// Proceedings of 2008 International Conference on Wireless Communications, Networking and Mobile Computing. Dalian, China, 2008: 659-662.

[8] COX I J, KILIAN J, LEIGHTON F T, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12):1673-1687.

[9] 李晓博, 周诠. 统计量移位的鲁棒无损图像信息隐藏[J]. 中国图象图形学报, 2012, 17(11): 1359-1366.
LI X B, ZHOU Q. Robust lossless image data hiding with statistical quantity shifting[J]. Journal of Image and Graphics, 2012, 17(11): 1359-1366.

[10] SOLANKI K, SARKAR A, MANJUNATH B S. YASS: yet another steganographic scheme and resists blind steganalysis[C]// Proceedings of 9th international Workshop on Informtion Hiding. Saint Malo, France, 2007: 16-31.

[11] SARKAR A, MADHOW U, MANJUNATH B S. Matrix embedding with pseudorandom coefficient selection and error correction for robust and secure steganography[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 225-239.

[12] LIU W W, LIU G J, DAI Y W. Damage-resistance matrix embedding framework: the contradiction between robustness and embedding efficiency[J]. Security and Communication Networks, 2015, 8(9): 1636-1647.

[13] FILLER T, JUDAS J, FRIDRICH J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920-935.

[14] TIAN H, QIN J, HUANG Y, et al. Optimal matrix embedding for voice-over-IP steganography[J]. Signal Processing, 2015, 117: 33-43.

[15] YAN S, TANG G, SUN Y, et al. A triple-layer steganography scheme for low bit-rate speech streams[J]. Multimedia Tools & Applications, 2015, 74(24): 11763-11782.

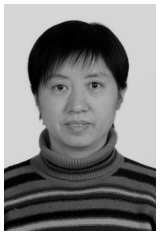
[16] LIU J, ZHOU K, TIAN H. Frame-bitrate-change based steganography for voice-over-IP[J]. Journal of Central South University, 2014, 21(12):4544-4552.

[17] 罗象宏, 舒继武. 存储系统中的纠删码研究综述[J]. 计算机研究与发展, 2012, 49(1): 1-11.
LUO X H, SHU J W. Summary of research for erasure code in storage system[J]. Journal of Computer Research and Development, 2012, 49(1): 1-11.

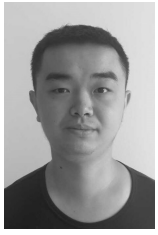
[18] 黄永峰, 李星. IP 语音包的自适应编码和封装算法的研究[J]. 电子与信息学报, 2002, 24(12): 1829-1834.
HUANG Y F, LI X. An adaptive voice coding and packeting scheme for IP telephony[J]. Journal of Electronics & information Technology, 2002, 24(12): 1829-1834.

作者简介：

高瞻瞻（1988-），男，河北正定人，解放军信息工程大学博士生，主要研究方向为信息隐藏、多媒体信号处理。



汤光明（1963-），女，湖南常德人，解放军信息工程大学教授、博士生导师，主要研究方向为信息安全、数据挖掘和体系对抗。



张伟伟（1989-），男，河南许昌人，解放军外国语学院博士生，主要研究方向为文本识别、图像处理。

doi:10.11959/j.issn.1000-436x.2016229

天地一体化信息网络安全保障技术研究进展及发展趋势

李凤华[1]，殷丽华[1]，吴巍[2]，张林杰[2]，史国振[3]
（1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；
2. 中国电子科技集团公司第五十四研究所，河北 石家庄 050000；3. 北京电子科技学院信息安全系，北京 100070）

摘 要：天地一体化信息网络由天基骨干网、天基接入网、地基节点网、地面互联网、移动通信网等多种异构网络互联融合而成，对实现国家安全战略目标具有重要意义。首先，介绍了天地一体化信息网络架构，以及卫星节点暴露、信道开放、异构网络互连等特征，并从物理层、运行层、数据层 3 个层面分析了天地一体化信息网络面临的威胁；其次，从物理安全、运行安全、数据安全 3 个层面对抗损毁、抗干扰、安全接入、安全路由、安全切换、安全传输、密钥管理等安全保障技术的研究现状进行了阐述；最后，针对天地一体化信息网络特点和安全保障需求，指出了天地一体化信息网络安全保障技术发展趋势和研究方向。

关键词：天地一体化信息网络；威胁；安全保障；安全架构
中图分类号：TP302 **文献标识码**：A

Research status and development trends of security assurance for space-ground integration information network

LI Feng-hua[1], YIN Li-hua[1], WU Wei[2], ZHANG Lin-jie[2], SHI Guo-zhen[3]
(1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
2. CETC 54, Shijiazhuang 050000, China;
3. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: Space-ground integration information network consists of space-based backbone network, space-based access network, the node net of foundation, Internet, mobile communication network, which has important significance for the realization of the target of national security strategy. Firstly, the characteristics of space-ground integration network, such as exposed channel, heterogeneous network integration, etc, were analyzed. Also, the corresponding threats from the physical layer, operation layer, data layer were introduced. Secondly, a comprehensive study on current status of survivability, anti-jamming, secure access, secure routing, secure handoff, secure transmission and key management were made. Finally, combined with research status, the important trends were proposed.

Key words: space-ground integration information network, threats, security assurance, security architecture

1 引言

随着卫星研制、火箭发射、运载、多星发射等各类技术的不断进步和应用，卫星网络迅速发展。借助于卫星网络，人类的“足迹”得以在太空的各个地方出现。同时，随着国家安全、航空航天、灾害预警等需求的不断增强，以及空间探索等任务的逐渐深入，各种战略信息任务在陆、海、空、天等不同维度空间不断开展，使原先相互独立的网络根据需要进行信息共享，实现跨地域、跨空域通信和网络各节点协同工作，这促使卫星网络进一步发展，并要求卫星网络与空间飞行器、地面网络等有

收稿日期：2016-08-24；**修回日期**：2016-09-27
通信作者：李凤华，lfh@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800303）；国家“核高基”科技重大专项基金资助项目（No.2015ZX01029101）
Foundation Items: The National Key Research and Development Program of China (No.2016YFB0800303), The National Science and Technology Major Project of China (No.2015ZX01029101)