



研究与开发

基于分段 STC 的音频隐写算法

张雪垣, 王让定, 严迪群, 林昱臻

(宁波大学信息科学与工程学院, 浙江 宁波 315211)

摘要: 在隐写领域中, STC (syndrome-trellis code) 隐写编码是时下最为先进的隐写算法之一。提出了一种基于 STC 的隐写算法——分段 STC。该算法利用分段、局部优化, 可有效降低载体失真。首先对音频最低有效位 (least significant byte, LSB) 载体流进行了分段切割, 随后利用最佳子校验矩阵将分段的密信嵌入分段载体中。该隐写算法在现有的语音样本库 TIMIT 库以及通过网络歌曲自制的样本库上进行了隐写实验。实验结果表明, 该思路下的算法可以有效地降低载体的失真元素个数和提高隐写算法的不可检测性。本文算法相较于传统 STC 算法, 失真元素个数的优化程度最高可达到 24%; 对比同类音频隐写算法, 本文算法生成的隐写后音频具备更加优秀的不可感知性能。

关键词: 分段 STC; 载体密信分配; 最佳子校验矩阵; WAV 隐写

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019071

An audio steganography algorithm based on segment-STC

ZHANG Xueyuan, WANG Rangding, YAN Diqun, LIN Yuzhen

College of Information Science and Engineering, Ningbo University, Ningbo 315211, China

Abstract: In steganography field, syndrome-trellis code is a state-of-the-art steganography algorithm. A steganography algorithm of Segment-STC was proposed. Segment-STC could locally optimize the distortion by segmentation. Firstly, the LSB-stream (least significant bit, LSB) of audio cover was segmented as few sub-segments. Then, the segmented message in each sub-segment was embedded to the optimal submatrix. The TIMIT dataset and author collected online songs as databases was used to run the experiments. Results show that segment-STC can effectively reduce the number of distortion elements of cover and improve the undetectability of the stego. Segment-STC algorithm can reduce the distortion over 24%, compared with the original STC algorithm. It also has a better imperceptible performance compare with other similar audio steganography algorithms.

Key words: segment-STC, cover-message allocation, optimal submatrix, WAV steganography

收稿日期: 2018-10-30; 修回日期: 2019-04-20

基金项目: 国家自然科学基金资助项目 (No.U1736215, No.61672302); 浙江省自然科学基金资助项目 (No.LZ15F020002, No.LY17F020010); 宁波市自然科学基金资助项目 (No.2017A610123); 宁波大学学科基金资助项目 (No.XKXL1509, No.XKXL1503); 浙江省移动网应用技术重点实验室开放基金资助项目 (No.F2018001)

Foundation Items: The National Natural Science Foundation of China (No. U1736215, No.61672302), The Natural Science Foundation of Zhejiang Province of China (No.LZ15F020002, No.LY17F020010), Ningbo Natural Science Foundation of China (No. 2017A610123), Ningbo University Fund (No.XKXL1509, No.XKXL1503), Mobile Network Application Technology Key Laboratory of Zhejiang Province (No.F2018001)



1 引言

信息隐写作为大数据安全的主要组成部分，其主要功能在于将秘密信息通过某种方式藏入数字多媒体中，使得该媒体在公共信道中传输却不被发现。其中的关键在于降低隐写前后多媒体载体的失真数量，使得传递密信具有足够的安全保证。参考文献[1]中指出，目前最安全的隐写方案是内容自适应方案，它们倾向于将秘密信息嵌入具有复杂性的内容区域中，使得失真检测变得更加困难。随着Fridrich结合卷积编码提出STC^[2-3]以来，在它的设计框架下产生了很多优秀的算法。在图像方面，嵌入痕迹不易被检测到的空间域隐写例子有HUGO^[4]、WOW^[5]和S-UNIWARD^[6]。

相较于图像的隐写方案，音频方面的隐写方案并不多见。其简单的发展过程为：从早期的WAV音频到压缩域音频（MP3、AAC等），从单一的采样点最低有效位替换到压缩领域编码参数自适应方案。尽管音频方面方案的数量不是非常庞大，但是其基本设计思路与图像一致。在WAV音频中，邹明光等^[7]设计出了一种基于振幅修改的隐写算法，通过比较原始音频每个采样点分组中振幅之间的关系，结合密信进行嵌入，取得大容量嵌入的突破。在AAC领域中，Luo等^[8]利用AAC编码与原始WAV音频的残差作为载体，利用STC进行了信息隐藏。在MP3领域中，Kim等^[9]利用MP3颗粒的大值区进行限定，对码流中的linbits位进行简单的LSB（least significant byte，最低有效位）替换嵌入。但是由于linbits位数量有限，对该方法的嵌入量有一定影响，同时LSB替换算法会造成载体音频的较大失真，降低算法的安全性。参考文献[10-11]利用MP3编码过程中窗口切换规则提出了一种隐写方法，该方法通过建立密信位和编码参数之间的映射关系，即窗口类型来执行嵌入。

尽管上述算法的侧重各有不同，但不难发现，所有设计者在设计算法的时候，考虑的载体均为

一维线性载体流，在整个载体流上进行嵌入算法的研究。在所有基于STC的隐写方案中，STC仅仅作为一种嵌入方法而存在，载体也仅仅只有一个。对于STC中子校验矩阵的选择、大小的设置均没有比较说明。参考文献[2]中，通过大量的实验给出了若干条子校验矩阵的设计原则和参数选择范围。但其实验是建立在随机产生的隐写载体和密信之上的，具有一定的普遍性。当载体、密信呈现一定分布特征的时候，参考文献[2]中所提供的建议就不具备最优性了。

本文通过对子校验矩阵的选取、排布做出分析，并研究其与载体、密信之间的联系，给出了适合于WAV音频的隐写算法。实验结果表明，在相同载体和密信的嵌入条件下，本文算法有效减少了隐写后载体的失真元素个数。

2 传统 STC 的模型框架

STC是Fridrich^[2]根据卷积编码和维特比算法所提出的一种信息隐藏算法。Fridrich假定各个载体元素之间的失真是加性的，随后并通过设计启发性的失真代价函数去衡量算法的失真程度，最后通过子校验矩阵实现在子块上对密信的连续嵌入。

传统的STC嵌入公式如式（1）：

$$\text{Emb}(x, m) = \arg \min_{P(y) \in C(m)} D(x, y) \quad (1)$$

其中，Emb(·)表示密信嵌入函数， x 表示原始载体向量， y 表示隐写后载体向量， m 表示秘密信息向量， $D(x, y)$ 表示密信嵌入前后载体的汉明距离，即失真（变化）元素个数。式（1）表示传统STC框架下，隐写模型的目标函数为嵌入前后载体的失真最小。在这个模型中，前后载体失真量的衡量方式如式（2）（亦为失真代价的普适公式）：

$$D(x, y) = \sum_{i=1}^n \rho_i |x_i - y_i| \quad (2)$$

其中， ρ_i 表示为当前元素的失真权重， n 表示载体

长度, i 表示当前载体位置。在传统的STC框架下, 密信提取计算式如式(3)所示:

$$\begin{aligned} \text{Ext}(y) &= Hy \\ \text{Ext}(y) &= \text{Ext}(\text{Emb}(x, m)) = m, \forall x \in X, \forall m \in \{0, 1\}^m \end{aligned} \quad (3)$$

其中, $\text{Ext}(\cdot)$ 表示密信提取函数, x 表示原始载体向量, y 表示隐写后载体向量, m 表示秘密信息向量, H 表示校验矩阵。式(3)表示密信的提取方式, 是通过校验矩阵于隐写后载体相乘得到的(校验矩阵不同于子校验矩阵, 其长度是子校验矩阵的倍数, 一般倍数与密信长度相当)。在STC隐写框架下, 通过密信提取函数可以将密信完全还原出来。

3 分段思想

Fridrich在参考文献[2]中设计此方法时考虑的是更为普适的情况, 对载体和密信均采用随机生成的方式进行考虑, 文献中没有任何直接的计算关系式可以用来描述载体、密信、完整校验矩阵与失真代价之间的关系:

$$\text{Cost} = f(x, m, H) \quad (1)$$

即式(4)所表示的定量关系并没有被明确。因此在衡量具体失真的时候, 绝大部分的隐写算法都是间接地用定性手段去衡量STC的隐写效果。本文将通过研究这四者的关系, 进一步确定其相互作用的方式, 并在获得这关系之后来设计新的隐写算法。

对此, 提出了“最佳子校验矩阵思路”——在一段载体密信的搭配下, 不同的子校验矩阵会产生不同的载体失真元素个数。也就是说, 在同一种规格的子校验矩阵集中, 至少存在一个子校验矩阵, 使得当前这组载体密信隐写完成后的失真元素个数最少。

较长的载体密信匹配起来十分复杂, 同时会消耗较长的时间。所以提出了载体密信匹配分段的方案, 以缩小其长度、加快其匹配速度。因为匹配是在STC框架下进行的, 一定长度的载体会

对应一定长度的密信。在分段后, 载体密信的0-1个数比将会不再按正常的接近1:1比值分布了。

当0-1个数比值远离1:1的时候, 使用最佳子校验矩阵进行STC嵌入, 失真元素个数会有明显下降。

$$\sum_{i=1}^n \text{cost}_i = \sum_{i=1}^n f(\hat{H}_i, m_i, x_i) \ll \text{Cost} = f(x, m, H) \quad (5)$$

其中, $x = [x_1, x_2, \dots, x_n]$, $m = [m_1, m_2, \dots, m_n]$, n 的取值可以根据密信的分段长度进行自定义。不等式两边的载体密信是完全相同的。不同的是使用STC时载体密信的长度、子校验矩阵的选取。不等式的左边表示利用分段思想, 对载体进行密信嵌入后, 每个分段失真元素个数的总和。不等式的右边表示传统的STC在同样的载体密信下所产生的失真元素个数。对比两者发现, 左边的失真元素个数一直小于右边的数值。可以说, 式(5)是分段思想提出的依据。

在分段之后, 需要为每一段匹配的载体密信寻找到一个最佳子校验矩阵。它将使得这一段载体在隐写后的失真元素个数最小。一般情况下, 规格越大时, 同规格子校验矩阵的个数也会越多, 且数量呈指数增长。例如规格为 hw 的子校验矩阵 $\hat{H}^{hw}$ 。理论上其可能出现的子校验矩阵数目为 2^{hw} 个。在如此庞大的选择范围中挑选出最佳的子校验矩阵是非常困难的。所以, 将通过对子校验矩阵特征的分析, 约束最佳子校验矩阵的选择范围。

4 最佳子校验矩阵的约束条件

作为STC算法的“灵魂”, 子校验矩阵会对这一过程产生巨大的影响。当其大小规格一定时, 子校验矩阵会有庞大的选择范围。通过对以下特征的分析, 将形成最佳子校验矩阵的约束条件, 以便更快地寻找到最佳子校验矩阵。

(1) 稀疏度约束

一个矩阵里面的零元素个数 $n_{x=0}$ 与所有元素个数 N 的比值可以用稀疏度来表示。本文采用式(6):



$$\eta = n_{x=0} / N \quad (6)$$

表示子校验矩阵的稀疏程度，稀疏度越大，说明矩阵中零元素个数越多。同规格下，子校验矩阵的稀疏度越低，失真元素越少。同时还发现失真个数的下降是波动的。分析原因发现是列稀疏度的突然改变，导致了失真元素个数陡然变化。

(2) 每列奇偶性约束

本文对子校验矩阵的列奇偶性定义如下：每列由上至下其权重分别为 $2^i (i=0, 1, \dots, n)$ ，将这些权重相加可以得到当前列的奇偶性（其本质是子校验矩阵首行是否置 1）。当每列权值为奇数时，子块编码后状态可以遍历到所有的状态；而当每列权值为偶数时，子块编码后状态仅仅只能遍历所有的状态的一半。由于可编码状态锐减一半，偶性的子校验矩阵其灵活性和可变性都大打折扣；相反状态遍历充分、路径选择越多时，就越有可能筛选出失真最小的嵌入路径（或者说最佳子校验矩阵）。

(3) 每行 0-1 和约束

众所周知在信息论中，状态转换使用的是按位异或运算。利用“位异或”对子校验矩阵每行的元素进行了运算。发现每行的值不同，也会产生不同的失真效果。当行和为 1（或者说该行 1 的个数是奇数）时，子块编码后其状态在保证输出的密信期望可变的情况下，可以遍历到所有的状态；当行和为 0（个数为偶数）时，子块编码后的状态无法遍历到所有状态。尽管此两种情况下，输出的密信期望 0 或者 1 都可以。但是行和为 0 时，由于状态遍历范围和路径选择范围均减少了一半，失真元素个数无法向最小值有效收敛。

(4) 末行置 1 约束

在子校验矩阵中，末行代表了状态值的最高位。当末行全部置 0 时，子块就自动失去了高位一半的编码位置，减少了可编码空间以及路径的选择范围（实际上换一个角度，末行置 0 就是将子校验矩阵的规格进行了一次调整——行的减

少）。这也是在Fridrich的原则^[2]中要求末行置 1 的原因。

综上约束条件，给出了一定规格下最佳子校验矩阵应具备的条件，首先子校验矩阵的规格不应过小，即 $h \geq 5, w \geq 5$ ，同时一般情况下 $|h - w| \leq 2$ ；其次需要保证子校验矩阵的每一列都不相同；再次根据“稀疏度约束”应保证每列的稀疏度最低（即每列的“1”要尽可能的多）；随后根据“每列奇偶性约束”应保证“首行置 1”；接着“每行 0-1 和约束”应尽可能保证“行和为 1”；最后根据“末行置 1 约束”应在其他约束条件不被破坏时，保证“末行置 1”。满足这些条件后，可以得到更小的子校验矩阵范围为 $w!$ 个，远小于 2^{hw} 个。

5 信息隐藏及提取

5.1 预处理

出于对时间成本的考虑，采用 5×6 、 6×6 两种规格（以下简称 56、66 规格）的子校验矩阵进行分段STC实验；且根据前期相关实验，密信分段长度 100 ~ 300 bit。之所以采用这样的规格和密信的长度，是因为考虑到在实际的嵌入过程中，分段STC方法存在着筛选最佳子校验矩阵的过程，这个筛选的范围已经通过最佳子校验矩阵约束条件进行了缩小，使用“暴力”搜索依旧会产生一定的时间成本。过大的子校验矩阵规格会使得时间成本呈指数趋势上升，故而选用相对较小的规格。

同时，密信的长度决定了这段密信所使用的完整子校验矩阵 H 的长度。当将分段密信的长度控制在 100 ~ 300 bit 时，每段的完整子校验矩阵 H_i 的生成时间总和 $T' = \sum_{i=1}^n t_i$ 与整段密信的完整校验矩阵 H 生成时间 T 基本相当。

5.2 密信隐藏

由于一般情况下读取音频时域采样点的值时，该值为正负十进制数，而STC嵌入操作要求载体一般为 0、1。故此根据十进制和二进制的转

化规则,对时域采样点进行二进制转换。并将每个采样点二进制后的LSB位作为嵌入的载体流。在此基础上,密信隐藏的具体流程如图1所示(j 为最佳子阵在集合中的编号,示意图仅举例说明,此处 $n=10$)。

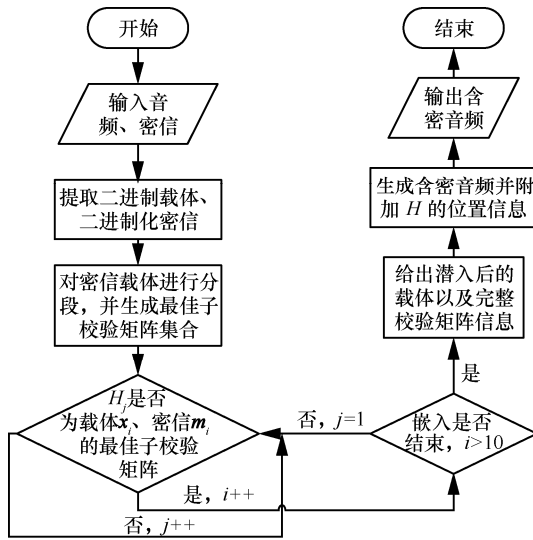


图1 分段STC隐写流程

首先对音频和载体进行二进制化并提取LSB载体流,并对用于信息隐藏的载体 x 、密信 m 进行匹配分段,共分为 n 段:

$$[x_1, x_2, \dots, x_n] = x \quad (7)$$

$$[m_1, m_2, \dots, m_n] = m \quad (8)$$

随后,分段匹配后的每对载体密信进行最佳子校验矩阵的匹配:

$$\begin{aligned} \min \sum_{i=1}^n \text{cost}_i &= \sum_{i=1}^n f(\hat{H}_i, m_i, x_i) \\ \text{s.t.} \quad &\begin{cases} \hat{H}_i \in \{\hat{H}\}^J \\ 10 \leq n \leq 20 \end{cases} \end{aligned} \quad (9)$$

其中, $\hat{H}_i$ 表示第 i 段载体密信所使用的子校验矩阵,从大小为 J 的 $\{\hat{H}\}$ 子校验矩阵集合中以失真元素个数最小为目标得到最佳子校验矩阵。该步骤在图1中体现为:当 $\hat{H}_j$ 不是当前第 i 段密信载体的最优子校验矩阵时,利用 $j++$ 换取下一个子校验矩阵进行判断;如果是,则相当于完成当前第 i 段

的密信嵌入,此时 $\hat{H}_i = \hat{H}_j$ 第 i 段的最佳子校验矩阵为 $\hat{H}_j$;随后判断的是,全部密信(共 $n=10$ 段)是否完成嵌入,如果没有,在 i 已经自加时, j 恢复到1,开始第 $i+1$ 段的最佳子校验矩阵判断。

然后,对各段载体密信分别实施STC嵌入,得到输出载体后合并,并输出完整载体 y :

$$y_i = \text{Emb}(x_i, m_i) \quad (10)$$

$$y = [y_1, y_2, \dots, y_n] \quad (11)$$

通过式(7)~式(11),成功地完成了秘密信息的分段嵌入。

5.3 密信提取

为了有效提取密信,音频时域采样值的LSB位载体流中,将下列基本信息用“直接替换”的方式放入载体:由密信起始位置、 $\hat{H}$ 排列信息和密信提取位置。有些情况下,这些信息通过保密信道传输,不直接进入载体,所以在提取密信的过程中,仅需要提取这些信息,随后构建传统STC解码框架即可。

密信提取的详细流程如图2所示。

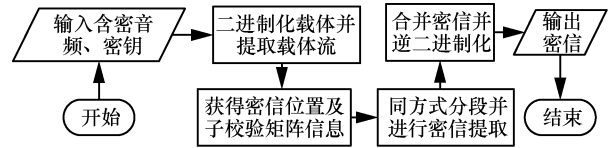


图2 密信提取流程

首先对含密音频二进制化(假设得到的是完整音频,因此需要二进制转换以得到含密载体流),并根据基本信息中的分段标准,提取隐写载体进行分段:

$$y_i = \{y_1, y_2, \dots, y_n\} \quad (12)$$

其次,根据密钥找到第 i 段载体所对应的子校验矩阵 $\hat{H}_i$,并生成完整的校验矩阵 H_i :

$$H_i = \begin{bmatrix} \hat{H}_i & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \hat{H}_i \end{bmatrix} \quad (13)$$

随后根据密信提取公式对每段载体进行密信



提取:

$$m_i = \text{Ext}(y_i) = H_i y_i \quad (14)$$

最后, 按照密钥中保存的密信顺序信息, 将密信拼接完整即可:

$$m = [m_1, m_2, \dots, m_n] \quad (15)$$

6 实验与分析

6.1 实验说明

本实验采用的密信一共有 3 种: 1 000 bit、5 000 bit、10 000 bit, 密信是文本格式; 采用的载体为 5 000 首随机 WAV 音频, 长度 10 s, 采样率为 44.1 kHz (样本库 1); 同时由于隐写领域没有成熟的公开语音音频样本库, 采用现有的、公开的 TIMIT 语音库进行了数据库的横向对比实验。由于 TIMIT 数据库中语音的长度是不固定的, 从 3 s 到 13 s 不等。为保证实验质量和实验结果的可对比性, 从 TIMIT 库中选取了所有大于 6 s 的语音片段进行实验 (样本库 2)。选用 56、66 两种规格的子校验矩阵。在分段的过程中, 为了避免段数过多造成隐写成本增加, 所以在这个实验中约定 n 的范围为 $10 \leq n \leq 20$ 。在此范围内可以保证分段 STC 相对于传统 STC 有充分的优化, 同时不会增加过多的密钥传输成本。本实验所采取的横向对比算法为: F5^[12]、匹配 LSB、传统 STC。

本实验采用的衡量指标为 ODG (模拟人耳听觉感知的指标)、SNR。这两个指标常用于衡量音频隐写算法的不可感知性。ODG 指标一般在 $(-4, 0)$, 其值越大说明人耳可辨程度越低, 一般 ODG 指标在 -1 以上说明人耳可以接受; 当其大于零时, 则说明两音频基本一样, 仅存在极其细微的差别。

SNR 是信噪比, 其计算式如下:

$$\text{SNR} = 10 \cdot \lg \left(\frac{\sum_{n=0}^{N-1} x^2(n)}{\sum_{n=0}^{N-1} [\tilde{x}(n) - x(n)]^2} \right) \quad (16)$$

其中, $x(n)$ 和 $\tilde{x}(n)$ 分别为原始音频载体和含密音频载体, N 为样本点个数。SNR 可以反映音频载体整体的失真, 例如有时在主观上不会感知到音频质量的下降, 但 SNR 数值会发生剧烈下降。另一个原因是从信息论的角度来看, 密信嵌入类似于一种加噪的过程, 故而通过对比信噪比可以从一定角度反映隐写算法的好坏。一般地, 信噪比越高, 则说明音频的不可感知性能越强。

6.2 实验结果与分析

隐写前后的音频已不可被人耳听觉、人眼视觉感知了。在此给出了直观的音频波形对比, 原始音频波形如图 3 所示, 分段 STC 隐写如图 4 所示。

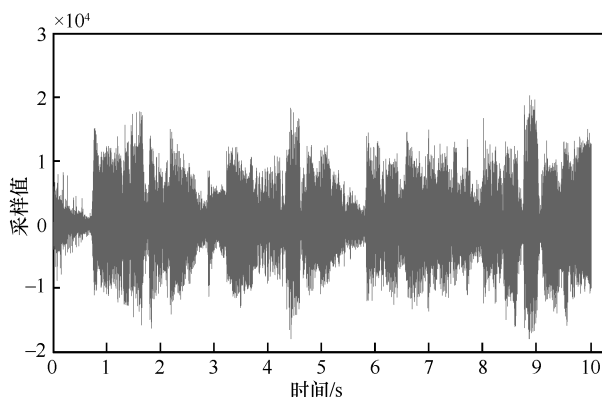


图 3 原始音频波形

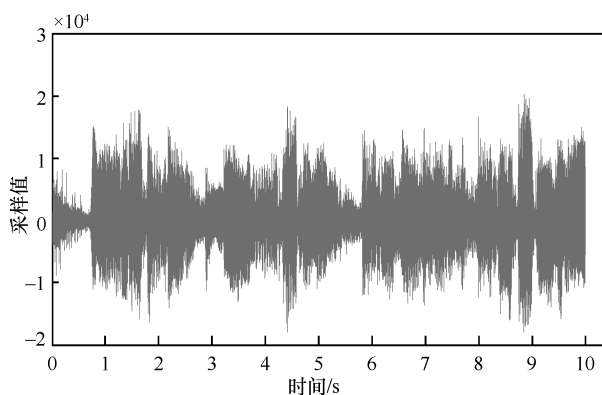


图 4 分段 STC 隐写后音频 (10 000 bit)

从图 3、图 4 两个音频波形对比来看, 在肉眼上无法发现其有明显失真, 证明了分段 STC 拥有出色的人耳不可感知性。同时为进一步衡量隐写方案的安全性, 通过数字音频分析手段给出了在

两个不同的样本库上的ODG指标和SNR指标。得到的ODG平均值结果见表1~表4（其中Original表示原始音频自比较）。

表1 不同密信长度下不同方案的ODG指标(56、样本库1)

ODG	10 000	5 000	1 000
LSB	0.202 1	0.203 3	0.204 1
F5	0.202 8	0.203 5	0.204 0
STC	0.203 0	0.203 5	0.204 9
分段 STC	0.203 3	0.203 8	0.205 1
Original	0.208 0	0.208 0	0.208 0

表2 不同密信长度下不同方案的ODG指标(66、样本库1)

ODG	10 000	50 000	1 000
LSB	0.197 7	0.198 8	0.200 5
F5	0.197 6	0.199 0	0.200 1
STC	0.198 5	0.199 9	0.200 4
分段 STC	0.199 9	0.200 2	0.200 6
Original	0.204 2	0.204 2	0.204 2

表3 不同密信长度下不同方案的ODG指标(56、样本库2)

ODG	10 000	50 000	1 000
LSB	0.176 6	0.179 9	0.193 5
F5	0.167 5	0.168 4	0.179 1
STC	0.193 1	0.193 3	0.193 6
分段 STC	0.194 1	0.194 7	0.195 3
Original	0.196 6	0.196 6	0.196 6

表4 不同密信长度下不同方案的ODG指标(66、样本库2)

ODG	10 000	50 000	1 000
LSB	0.176 6	0.179 9	0.193 5
F5	0.166 6	0.167 5	0.179 9
STC	0.190 3	0.192 2	0.193 5
分段 STC	0.193 9	0.194 4	0.194 9
Original	0.196 6	0.196 6	0.196 6

表1~表4显示了在56、66两种规格下的ODG指标。可见不管是在自制的容量为5 000首音频的

样本库中，还是在成熟的TIMIT的样本库中，分段STC隐写方案都具有最佳的听觉感知特性。其模拟人耳听觉感知得分最高，最接近于原始音频的ODG得分。

实验得到的SNR指标见表5~表8。

表5 不同密信长度下不同方案的SNR指标(56、样本库1)

SNR	10 000	5 000	1 000
LSB	65.093 5	67.383 3	74.402 2
F5	69.840 1	72.271 1	79.104 0
STC	69.276 0	71.653 0	78.451 3
分段 STC	69.946 1	72.510 1	79.485 5

表6 不同密信长度下不同方案的SNR指标(66、样本库1)

SNR	10 000	5 000	1 000
LSB	64.946 5	67.345 3	74.222 1
F5	69.673 3	72.190 2	79.151 1
STC	69.192 0	71.574 1	78.451 1
分段 STC	69.983 3	72.369 0	79.350 7

表7 不同密信长度下不同方案的SNR指标(56、样本库2)

SNR	10 000	5 000	1 000
LSB	66.262 5	68.716 9	75.134 9
F5	58.327 2	58.497 0	65.300 2
STC	73.399 1	75.749 9	82.199 1
分段 STC	73.700 6	76.180 8	82.985 1

表8 不同密信长度下不同方案的SNR指标(66、样本库2)

SNR	10 000	5 000	1 000
LSB	66.151 4	68.607 0	75.005 9
F5	57.952 6	58.097 0	64.900 3
STC	73.198 5	75.823 5	81.276 9
分段 STC	73.694 4	76.296 1	82.941 5

表5~表8显示了在56、66两种规格下的SNR指标。在两种不同的子校验矩阵规格和两种不同的样本库下，均是分段STC的指标最为优秀——



计算所得的信噪比值最大。从实验结果数据上看, ODG指标和SNR指标均充分说明了在上述所有算法中, 本文算法的不可感知性能是最优的。同时上述数据也可以证明分段STC方法比其他传统方法具有更好地隐藏效率和更接近原始音频质量的输出能力。

7 结束语

本文以最小元素失真个数为目标, 提出了“最佳子校验矩阵思路”, 通过约束条件进一步缩小了最佳子校验矩阵的选择范围; 并通过分段思想进一步突出了载体密信的分段匹配能力, 减少了最佳子校验矩阵的搜索时间。对比传统的隐写算法优化思路, 本文从STC本身的角度提供了新的优化方向, 为STC隐写算法优化策略提供了一个全新的角度。

同时, 也要指出, 在密信使用分段STC嵌入之后, 为了保证密信的100%完整提取, 需要记录分段子校验矩阵的排列信息。排列信息一般有两种处理方式: 一种以另一种密信的形式, 附进载体音频中(由于其体量极小, 篡改痕迹可忽略不计); 另一种方式则是单独利用保密信道进行加密传输。从现实使用场景角度来看两种方案各有利弊: 前者减少了敏感信息的暴露, 但是极小量地增加了载体失真, 且该信息的位置一般是固定的; 后者虽然可以不再给载体带来其他失真, 但是增加了密信相关信息的外露, 一定程度上降低了安全性。

本文提出的分段STC方法目前只在WAV音频上进行了实现和对比。但是从其本质上来说, “分段STC”是一种广义的针对传统STC隐写方法的优化, 可以应用在多种媒体载体、多种媒体参数上进行信息隐藏。倘若结合多载体分段的形式, 可以预见其会具有更强大的信息隐藏能力。在未来的工作中, 将会注重在压缩音频领域, 如主流的MP3、AAC两种压缩格式上尝试分段STC隐写算

法。同时也会针对压缩音频的种种特性, 进一步优化以期获得一种更为高效、优秀、隐蔽的隐写算法。

参考文献:

- [1] NI J, YE J, YI Y. Deep learning hierarchical representations for image steganalysis[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2545-2557.
- [2] FILLER T, JUDAS J, FRIDRICH J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(3): 920-935.
- [3] FILLER T, JUDAS J, FRIDRICH J. Minimizing embedding impact in steganography using trellis-coded quantization[C]//International Conference on Multimedia Computing and Systems, April 14-16, 2014, Marrakesh Morocco. Piscataway: IEEE Press, 2014.
- [4] PEVNY T, FILLER T, BAS P. Using high-dimensional image models to perform highly undetectable steganography[J]. Lecture Notes in Computer Science, 2010(6387): 161-177.
- [5] HOULUB V, FRIDRICH J. Designing steganographic distortion using directional filters[C]//IEEE International Workshop on Information Forensics and Security, December 2-5, 2012, Costa Adeje-Tenerife, Spain. Piscataway: IEEE Press, 2012: 234-239.
- [6] HOLUB V, FRIDRICH J, DENEMARK T. Universal distortion function for steganography in an arbitrary domain[J]. EURASIP Journal on Information Security, 2014, 1(1): 1-13.
- [7] 邹明光, 李芝棠. 基于振幅值修改的 WAV 音频隐写算法[J]. 通信学报, 2014 (s1)
ZOU M G, LI Z T. WAV-audio steganography algorithm based on amplitude modifying[J]. Journal on Communications, 2014(s1).
- [8] LUO W, ZHANG Y, LI H. Adaptive audio steganography based on advanced audio coding and syndrome-tcoding[J]. International Workshop on Digital Watermarking, 2017(10431): 177-186.
- [9] KIM D H, YANG S J, CHUANG J H. Additive data insertion into MP3 bitstream using linbits characteristics[C]// IEEE International Conference on Acoustics, Speech, and Signal Processing, May 21-23, 2014, Montreal, Que, Canada. Piscataway: IEEE Press, 2014: 181-184.

- [10] YAN D Q, WANG R D, YU X, et al. Steganography for MP3 audio by exploiting the rule of window switching[J]. Computers & Security, 2012, 31(5): 704-716.
- [11] 严迪群. 压缩域音频隐写与隐写分析中若干问题的研究[D]. 宁波: 宁波大学, 2012.
- YAN D Q. Research about several problems of steganography and steganalysis in audio compressed domain[D]. Ningbo: Ningbo University, 2012.
- [12] 刘昌鑫, 朱平, 夏春和. F5 隐写算法及其隐写分析研究[J]. 计算机工程与设计, 2007, 28(4): 884-887.
- LIU C X, ZHU P, XIA C H. Research on F5 steganography algorithm and its steganalysis[J]. Computer Engineering and Design, 2007, 28(4): 884-887.

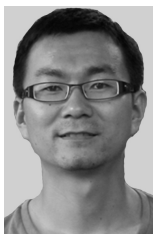
[作者简介]



张雪垣(1994-), 男, 宁波大学信息科学与工程学院硕士生, 主要研究方向为多媒体通信、信息安全、信息隐写与隐写分析等。



王让定(1962-), 男, 博士, 宁波大学高等技术研究院教授、博士生导师, 主要研究方向为多媒体通信与取证、信息隐藏与隐写分析、智能抄表及传感网络技术。



严迪群(1979-), 男, 博士, 宁波大学信息科学与工程学院副教授、硕士生导师, 主要研究方向为多媒体通信、信息安全、基于深度学习的数字语音取证等。



林昱臻(1994-), 男, 宁波大学信息科学与工程学院硕士生, 主要研究方向为多媒体通信与信息安全等。