

语音流隐写分析

原创

noobme 于 2019-11-22 17:10:48 发布 746 收藏 4

分类专栏: # 语音隐写分析

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/sleepinghm/article/details/103203428>

版权



[语音隐写分析 专栏收录该内容](#)

6 篇文章 2 订阅

订阅专栏

第 31 卷第 3 期

重庆邮电大学学报(自然科学版)

Vol.31 No.3

2019 年 6 月 Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition)

Jun.2019

DOI: 10.3979/j.issn.1673-825X.2019.03.017



IP 语音隐写及隐写分析研究

刘小康, 田 晖, 刘 杰, 卢 璿

(华侨大学 计算机科学与技术学院 厦门 361021)

<https://blog.csdn.net/sleepinghm>

1. 隐写

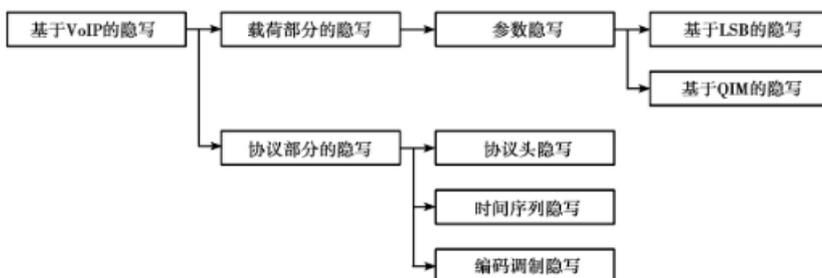


图 1 基于 VoIP 的隐写分类

VoIP 的编码器都使用代数码本激励线性预测 (ACELP) 编码规则编码, 这是一种混合编码形式。

主流方案是基于 VoIP 编码器编码过程中的冗余提出的隐写方案:

1. 在编码中检测某些参数属于最低有效位, 然后篡改秘密信息这种属于最低有效位 LSB 隐写,
2. 而利用 VoIP 编码器的码本编码特性划分码本来隐藏信息的方法叫做量化索引调制 QIM 隐写: 按照语音编码本来的原则将码本以某种规则划分并选择次优参数来嵌入秘密信息。

2.隐写分析

在参数隐写的分类上按照编码参数种类进行分类

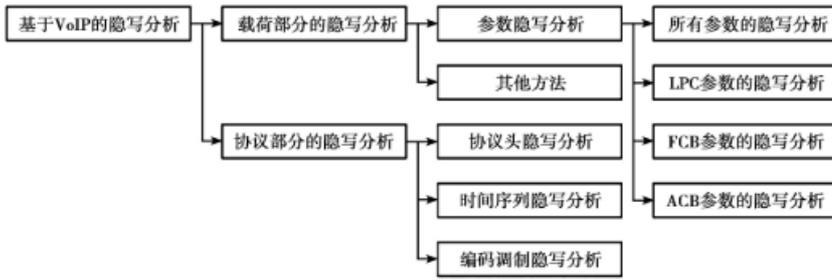


图 2 基于 VoIP 的隐写分析分类

编码之后得到的参数有线性预测(LPC) 参数, 固定码本(FCB) 参数, 自适应码本(ACB) 参数..

LPC, FCB, ACB 参数编码都是使用码本的参数编码, 所以既可以使用 LSB 方式隐写又可以根据 QIM 方式隐写

对于隐写, 提出的隐写方案更加侧重于隐写方法, 其目的在于如何使提出的方法能够提高隐 蔽性和隐藏容量。所以按照隐写手段来分类。

对于检测, 不论使用的是何种方法, 重要的是将其检 测出来并且最好知道隐写的位置, 因此, 隐写分析会 按照参数位置来分类。

3.隐写分析算法

文献	检测的隐写方法	检测的隐写域	分类方法	是否提升检测精度
文献[66]	LSB	协议头	基于统计	是
文献[67]	LSB	SIP 协议头	基于统计	—
文献[68]	时间序列	TCP/IP	特征和分类器	是
文献[69]	Transcoding	载荷	基于统计	—
文献[70]	Transcoding	载荷	基于统计	是
文献[71]	编码速率跳变	载荷	特征和分类器	是
文献[72]	QIM	LPC 编码参数	LSTM 神经网络	是
文献[73]	QIM	LPC 编码参数	贝叶斯网络	是
文献[74]	QIM	ACB 编码参数	特征和分类器	是
文献[75]	QIM	ACB 编码参数	特征和分类器	是
文献[76]	QIM	FCB 编码参数	特征和分类器	是
文献[77]	QIM	FCB 编码参数	特征和分类器	是
文献[78]	QIM	FCB 编码参数	特征和分类器	是

[66] HUANG Y, TANG F. Detection of covert voice-over Internet protocol communications using sliding window-based steganalysis [J]. Iet Communications, 2011, 5 (7): 929-936.

[67] ZHAO H, ZHANG X. SIP Steganalysis Using Chaos Theory [C]//Proceedings of International Conference on Computing, Measurement, Control and Sensor. New York: IEEE Press, 2012: 95-100.

[68] ZHAO H AND SHI Y, Detecting Covert Channels in Computer Networks Based on Chaos Theory [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(2): 273-282.

[69] ZHAO H, ANSARI N. Detecting covert channels within VoIP[C]//Proceedings of 35th IEEE Sarnoff Symposium IEEE. New York: IEEE Press, 2012: 1-6.

[70] JANICKI A, MAZURCZYK W, SZCZYPIORSKI K. Steganalysis of transcoding steganography [J]. Annals of telecommunications-Annales des télécommunications, 2014, 69(7-8): 449-460.

[71] TIAN H, SUN J, CHANG C C, et al. Detecting Bitrate Modulation Based Covert Voice-over-IP Communication [J]. IEEE Communications Letters, 2018, 22(6): 1196-1199.

[72] LIN Z, HUANG Y, WANG J. RNN-SM: Fast Steganalysis of VoIP Streams Using Recurrent Neural Network [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(7): 1854-1868.

[73] YANG J, LI S. Steganalysis of Joint Codeword Quantization Index Modulation Steganography Based on Codeword Bayesian Network [J]. Neurocomputing, 2018 (313): 316-323.

[74] 李松斌, 贾已真, 付江云, 等. 基于码书关联网络的基音调制信息隐藏检测 [J]. 计算机学报, 2014, 37(10): 2107-2117.

LI S B, JIA Y Z, FU J Y, et al. Detection of Pitch Modulation Information Hiding Based on Codebook Correlation Network [J]. Chinese Journal of Computers, 2014, 37(10): 2107-2117.

[75] REN Y, YANG J, WANG J, et al. AMR Steganalysis Based on Second-Order Difference of Pitch Delay [J]. IEEE Transactions on Information Forensics & Security, 2017, 12(6): 1345-1357.

[76] REN Y, CAI T, TANG M, et al. AMR Steganalysis Based on the Probability of Same Pulse Position [J]. IEEE Transactions on Information Forensics & Security, 2015, 10(9): 1801-1811.

[77] TIAN H, WU Y, CHANG C C, et al. Steganalysis of adaptive multi-rate speech using statistical characteristics of pulse pairs [J]. Signal Processing, 2017, 134(C): 9-22.

[78] TIAN H, SUN J, HUANG Y, et al. Detecting Steganography of Adaptive Multirate Speech with Unknown Embedding Rate [J]. Mobile Information Systems, 2017, 2017(3): 1-18.

QIM思想: 将量化码本分组, C分为C1,C2 (无交集), C1=比特0, C2=比特1.嵌入为0时在分组码书C1中选取最佳量化值, 嵌入1时在分组码书C2选择最佳量化值。接收方根据所接收的量化结果中的索引值是 属于C1、C2 来恢复机密信息比特。

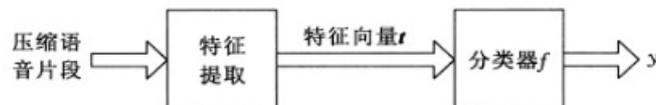


图 4 压缩语音片段隐写检测过程

隐写检测的关键是确定特征向量t和分类器f.

1.特征向量的提取必须首先对压缩语音片段进行解码，其后基于解码获得的语音数据计算基于MFCC的统计特征向量，这种特征提取方法需要进行解码操作，甚为耗时。上一节中我们介绍了本文的特征提取方法，该方法不需要对压缩语音进行解码，**直接在压缩域抽取特征向量**，计算速度较快。为此，本文将上节给出的**音素分布特性量化向量H作为特征向量t**。

2.关于分类器的设计，现有研究中，不同的对象分类识别系统有不同的训练方法，这些方法大致可分为两大类：判别法和生成法。判别法可以灵活地选择用来识别的特征，检测速度也较快，为此本文采用基于判别法的分类器。在判别型分类器中，由于支持向量机比较适合小样本训练的情况，本文考虑到训练时间和训练样本量，使用支持向量机作为分类器。SVM分类器是一种监督学习分类器，它是通过使用某些已标注类别的样本进行训练获得的。

对于特征向量t,分类器f的训练和预测步骤如下:

1. 获取尽可能多的cover类别低速率压缩编码语音片段，并使用QIM嵌入方法（分组码本使用[8]算法进行优化划分）进行隐写以获得cover类别中每个样本对应的stego样本，并做好标注；
2. 抽取上一步骤所获得的两类样本的特征向量t，标记每个向量的类别；
3. 训练分类器：使用上一步骤获得已标记类别的特征向量集合训练分类器，获得分类器 f
4. 使用分类器 f 对未知类别样本进行隐写检测：对于未知类别样本首先抽取特征向量t，将t作为分类器f的输入，分类器输出即为隐写检测结果。LIBSVM是一个优秀的SVM工具，本文基于 LIBSVM进行分类器的训练和预测。

实验：[8]CNV算法对G.729进行矢量量化时的3个分裂矢量码本进行优化划分，获得进行QIM嵌入的分组码本。再次对每个PCM格式的语音样本进行基于G.729标准的编码压缩，并且，在对每个帧的LPC系数进行矢量量化时使用QIM机制嵌入机密信息，获得包含隐藏信息的500个G.729压缩语音流片段，这些压缩语音片段组成隐写类别(S类)样本，C类及其对应的S类压缩语音流片段构成进行分类器训练和预测时的CM数据集。同理可得CW、EM和EW数据集,这4个数据集的所有样本构成混合数据集.因此，本文在5个不同的数据集上评估了算法性能。

4.基于语音载荷的隐写分析

4.1针对最低有效位LSB的隐写分析 4.2-4.4针对量化索引调制QIM的隐写分析

4.1所有参数的隐写分析

[80]采用了二次检测和回归分析，不仅能够检测嵌入在互联网协议(VoIP)语音中的隐藏消息，而且能够准确地估计嵌入消息的长度。

[81]提出了一种能够捕获Internet上的VoIP语音流并检测其中实时隐蔽信道的模型。

[82]提出了一种在VoIP语音的分布式隐写分析方法。每个可用于隐藏信息的语音参数被设计成利用相应的最佳检测特征独立地检测。

[83]提出了一种基于二阶导数语音信号小波包系数的马尔可夫双向转移矩阵的隐写检测算法。此类检测方法具有一定的通用性，但是针对一些复杂的隐写方案并不能有效地检测。

5.2 线性预测参数LPC隐写分析

LPC广泛应用于语音信号建模是VoIP编码器中重要的组成部分。

在LPC编码中，对LPC系数进行转换成线谱频率系数。

基于LPC参数的QIM隐写就是在量化LSF的过程中划分码本并嵌入秘密信息。

[84]提出了一种改进的QIM隐写算法用于G.729A压缩语音流中的有效信息隐藏。

[85]基于量化指标序列中各量化指标(码字)的分布具有不平衡性和相关性的特点，提出检测G.723.1比特流QIM隐写的方法。[86]采用音素分布特征用来检测QIM隐写术。

[87]针对LPC上的隐写，观察到线性预测编码滤波器系数的分裂矢量量化码字的相关特性在QIM隐写之后发生了变化，基于此，构造量化码字相关网络模型。值得注意的是，利用深度学习来构建隐写分析算法不仅在准确率而且在实时性上都优于传统算法。

[72]提出了一种有效的隐写分析方法来检测QIM隐写术。为了提取这些相关特征，提出了基于递归神经网络的码字相关模型。实验结果表明，在短时间内这个隐写分析方法达到了非常好的效果。

[73]提出了一种基于码字贝叶斯网络的隐写分析方法。

5.3 固定码本参数FCB隐写分析

在编码中通过深度优先树获得固定码本向量。但是这个结果是次优的，因此，对于所需的码本向量还有其他替代方案。利用这一特性，现有的隐写方法将隐写操作结合到码本搜索中实现信息嵌入。**对于这种隐写方法的检测往往是根据脉冲之间的一些特性来区分原始样本和隐写样本。**

[88]提出了一种基于脉冲位置参数直方图特征的合成压缩语音隐写分析方法。

[89]认为脉冲位置等参数的取值存在一定的局限性，基于此提出一种针对 G.723.1 网络语音协议(VoIP) 压缩语音的隐写分析方法。

[90]针对固定码本上的隐写提出了2种隐写分析方法: ①利用马尔科夫转移概率来估计轨迹中脉冲位置之间的关系; ②使用联合熵与条件熵来测量脉冲位置的不确定性。

[76]提出基于相同脉冲位置概率的隐写分析特征的隐写分析方法。

[91]提出利用脉冲位置的概率分布和语音信号的短时不变特性，提取脉冲位置的马尔可夫转移概率，并采用联合概率矩阵来表征脉冲-脉冲相关性，提出一种新的隐写分析方法。

[77]又使用脉冲对的概率分布和脉冲对的马尔科夫转移概率矩阵以及脉冲对的联合概率矩阵作为轨道与轨道相关性特征，使用 AdaBoost 进行特征筛选精简得到的特征分类结果优于现有的检测方法。

针对 FCB 隐写率未知的问题，Tian 等 [78] 提出了 3 种基于支持向量机的隐写分析方法，然后提出了一个混合隐写分析方案，并提供一个综合的检测结果。目前，基于 FCB 参数隐写的检测方法在检测精度上已经达到较好的效果，但是在可拓展性和通用性上仍有提升的可能。

5.4 自适应码本参数ACB隐写分析（难）

自适应码本搜索的目的是预测基音周期，基音周期是VoIP编码器中一个很重要的参数。由于编码的冗余，很多隐写方法使用LSB 或者QIM 方法将原值修改嵌入信息。针对这类的隐写分析难度较大。

基音调制信息隐藏是在基音预测中嵌入秘密信息，在低比特率语音编解码器中能以较高的隐蔽性和带宽来隐藏信息。

但是，压缩语音流中相邻语音帧自适应码本具有一定的相关特性。根据这一发现

[74]采用码本相关特性作为基音调制隐写检测的特征，并设计了码本相关网络模型得到较好的实验效果。

[75]提出了一种新的 AMR 音频隐写检测方案，基于原始的与隐写的 AMR 音频对相邻音高延迟连续性的区别，通过计算马尔科夫转移概率，提出音调延迟二阶差分矩阵(matrix of the second-order difference of pitch delay, MSDPD) 隐写分析特征矩阵，再通过校准MSDPD 得到C-MSDPD，实验证明 C-MSDPD 的效果要优于 [74]的效果，是已知最优的检测方法。

5.提升

1) 提高隐写分析检测准确率：从提高分类器的性能出发也是 升检测效果的方向。将深度学习方法应用到隐写分析中并且达到了较好的效果，检测准确率仍然有上升的空间。

2) 隐写分析的通用性。通用不仅仅要做到对某一类型的隐写方法的检测(其中包括未知隐写方法的检测)，而且做到要对不同编码环境下隐写的检测。除此之外，由于样本集大小的限制，一般隐写分析算法可能对一些样本集并不能达到较好的效果，这些都是通用的范围。一方面需要研究提高分类器的泛化能力，另一方面需要研究组建针对不同条件的集成分类器。