

Design and Implementation of Information Hiding Function Based on Sipdroid Platform

Qianqian Xu, Kaiyang Cheng, Xingjie Wen, Zhuang Wang, Yuxin Zhou, Meiling Yan, Hongguang Zhao

Computer and Information Engineering College, Henan University, Kaifeng Henan
Email: 955918996@qq.com, 437934160@qq.com

Received: Nov. 17th, 2017; accepted: Nov. 30th, 2017; published: Dec. 7th, 2017

Abstract

VoIP has the advantages of low cost, easy operation, high platform compatibility and other advantages, getting the rapid development and the favor of the vast number of consumers. Sipdroid is an open source Internet phone software and it is easy to use. Its use of the Sip protocol has the advantages of simple structure, to support multimedia business, with the Internet network structure, good expansibility, flexible application and so on. Sipdroid is based on the Android platform, and it has good open source and compatibility. When the network provides people with information sharing, it also causes a threat to the security of information. In this article, in order to further improve the security of transmission information, we analyze and design, based on Sipdroid system and add information hiding module, real-time voice calls at the same time, to achieve the hidden information embedded, transmission and extraction. The test results show that Sipdroid still has good usability after adding information hiding function.

Keywords

Sipdroid, Analysis and Design, Information Hiding

Sipdroid平台下的信息隐藏功能设计与实现

徐茜茜, 程开洋, 温兴杰, 王 壮, 周玉欣, 闫美玲, 赵红光

河南大学计算机与信息工程学院, 河南 开封
Email: 955918996@qq.com, 437934160@qq.com

收稿日期: 2017年11月17日; 录用日期: 2017年11月30日; 发布日期: 2017年12月7日

摘 要

网络电话具有资费低、易操作、平台兼容性高等优点, 因此得到迅速发展并获得广大消费者的青睐。

文章引用: 徐茜茜, 程开洋, 温兴杰, 王壮, 周玉欣, 闫美玲, 赵红光. Sipdroid 平台下的信息隐藏功能设计与实现[J]. 软件工程与应用, 2017, 6(6): 163-171. DOI: 10.12677/sea.2017.66018

Sipdroid是一款开源且使用简便的网络电话软件,其采用的Sip协议具有结构简单、支持多媒体业务的开展、符合互联网网络结构、可扩展性好、应用灵活等优点。基于的Android平台具有良好的开源性和兼容性。网络在为人们提供信息共享的同时,对信息的安全性也造成了一定的威胁。本文为了进一步提高传输信息的安全性,在Sipdroid系统的基础上进行分析设计,添加信息隐藏模块,在实时语音通话的同时,实现了隐藏信息的嵌入、传输与提取。测试结果表明,在加入信息隐藏功能之后Sipdroid仍具有良好的使用性。

关键词

Sipdroid, 分析与设计, 信息隐藏

Copyright © 2017 by authors and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

网络电话依托现有的互联网,利用协议来实现语音的实时传递,这成为了新一代网络时代最具代表性和发展前景的应用技术之一。网络电话在使用时处于开放的网络环境下,用户的信息容易暴露在外界环境中,对于银行、政府等一些对数据安全性要求较高的行业,更要保证数据不被窃取,因此网络电话的安全性引起了人们的高度重视。为了保证传输信息的安全性,采用不同于加密技术的信息隐藏技术,结合网络电话和信息隐藏技术两方面的技术优点,实现在进行实时语音通话的同时传输秘密信息[1]。传统的加密技术在保护秘密信息的同时也暴露了秘密信息传输的存在,被加密的信息很容易引起攻击者的注意,而信息隐藏技术隐藏了秘密信息的“存在性”,即使窃听者监听到了传输的语音数据,也无法直接判断其中是否有秘密信息的存在,这在一定程度上提高了秘密信息的隐蔽性[2]。同时,基于流媒体的信息隐藏技术引起了国内外专家学者的普遍重视,它作为一种实时传输载体,将会给信息安全传递提供更好的隐蔽性以降低秘密信息被攻击的概率[3]。

从现有的文献来看,目前信息隐藏的载体已经从静态媒体如文本、图像等转向动态流媒体如语音、视频等[4]。本文是以VoIP (Voice over Internet Protocol)语音为载体,在语音数据编码后进行插入隐藏信息进而将隐藏信息发送到接收端。基于VoIP语音通话采用的是IP分组封装,当秘密信息被提取后,语音信息在播放后将会被后面紧随的语音信息覆盖,因此攻击者只能对整个通话信息进行盲检测,难度很大,因而在很大程度上提高了秘密信息的安全性。在VoIP中应用较多的隐藏算法有LSB (Least Significant Bit)算法和DWT (Discrete Wavelet Transform)算法。为了增强LSB算法的鲁棒性,Kratzer等人[5]提出在LSB信息隐藏后再进行加密,虽然有效的提高了信息的安全性但是由于加密技术的影响也带来了很大的通信延迟,一定程度上也损伤了语音的质量,这也容易暴露隐藏信息的存在。为增强语音载体信息隐藏的容量及鲁棒性,Wu等人提出一种基于小波变换的音频隐藏新方法,通过调节语音段小波变换的中高频系数,进而改变每级小波变换高频系数前后两部分的能量状态来隐藏二进制机密信息[6]。虽然算法具有良好的隐蔽性和鲁棒性,但是由于算法实现复杂,也会对实时语音通信造成一定影响。本文使用G.711语音编解码结合LSB算法,按照每八位二进制流进行替换最不重要位的原则,算法实现简单,实验结果表明本方法对实时语音传输影响小。

2. Sipdroid 信息隐藏功能分析与设计

2.1. 整体需求分析

基于Sipdroid系统要实现的主要功能:在现有Sipdroid系统的基础上,为了提高传输信息的隐蔽性

和安全性,在语音通话模块加入信息隐藏模块。在不影响语音通话质量的前提下,实现秘密信息的传输。本文实现基于的载体是语音,要传输的秘密信息是文本。

发送端: SIP 账号的登录,根据当时的网络环境以及对要传输秘密信息的安全性和其他条件选择调用的信息隐藏算法,本文实现以 LSB 算法为例。SIP 账号的拨打,建立连接,语音通话,在通话界面输入秘密信息。

传输过程:对采集编码之后的语音流调用隐藏嵌入算法,把要传输的秘密信息隐藏在实时的语音流中,对带有秘密信息的语音流进行封装,使其随语音流的传输到达接收方。

接收端:接受方收到来自网络的数据包之后调用信息隐藏提取算法,提取出嵌入在语音流中的秘密信息,并保存在相应的位置提示接收方进行检查。

其相应的处理流程如图 1 所示。

2.1.1. 用户界面

信息隐藏算法的选择界面。

在设置界面增加信息隐藏算法的选择功能。用户可以根据所在网络环境的状况、发送信息的容量、信息隐藏算法实现的难易、要传输的秘密信息的形式等,来选择相应的隐藏算法来实现秘密信息的隐藏和提取功能。

界面如图 2 所示。

2.1.2. 通话界面

发送方在语音通话界面点击“发送消息”完成秘密信息的输入,要发送的秘密信息随着语音流到达接收方,以震动的形式提醒用户收到信息,用户可以点击菜单选项,在弹出的界面上点击“收到信息”,查看提取出的秘密信息。

通话界面如图 3 所示。

2.2. 信息隐藏功能需求分析与设计

用户在使用 Sipdroid 之前要根据不同的使用情况,在用户界面去选择相应的隐藏算法来实现秘密信息的嵌入和提取。信息隐藏算法主要有基于时间域信息隐藏和基于变换域的信息隐藏两类。

时间域信息隐藏算法的特点是算法复杂度低容易实现,但是鲁棒性差;变换域信息隐藏算法是对语音载体进行频域变换之后得到的系数进行修改实现信息隐藏,其具有较好的鲁棒性,但是提高了算法的

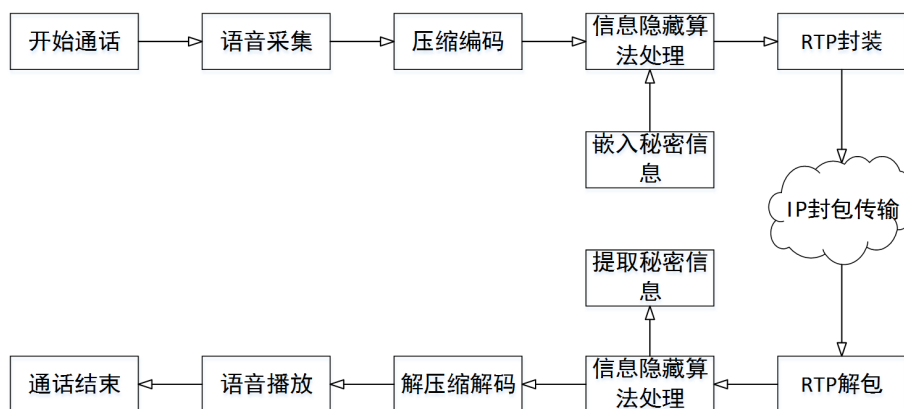


Figure 1. Information hiding process flow chart

图 1. 信息隐藏处理流程图

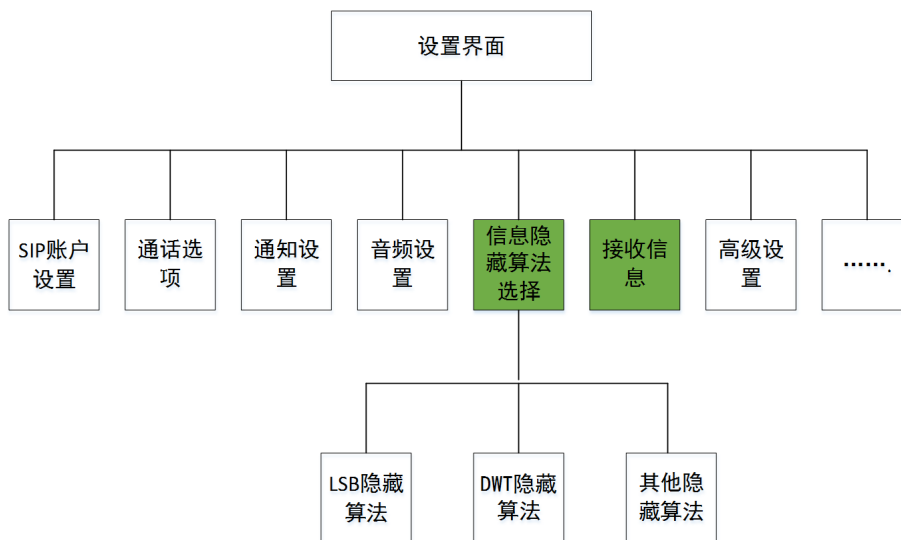


Figure 2. User interface
图 2. 用户界面

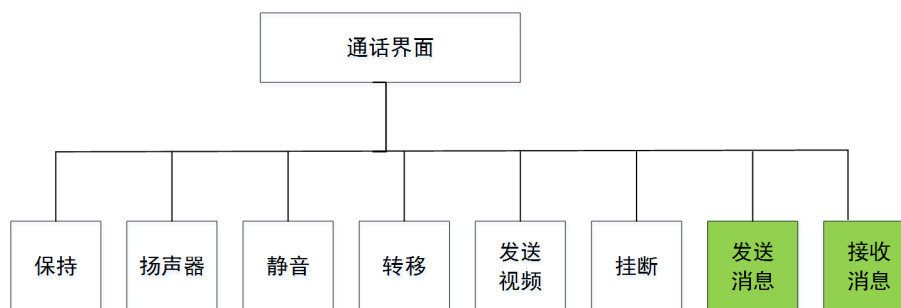


Figure 3. Call interface
图 3. 通话界面

复杂度[7]。由于语音载体对实时性要求比较高，与变换域相比 LSB 信息隐藏算法有较高的嵌入容量[8]。因此，本文选择经典时间域信息隐藏 LSB 算法的进行实现信息隐藏功能。

3. Sipdroid 信息隐藏功能实现

3.1. Sipdroid 信息隐藏功能的实现

1、在用户界面的设置界面下增加“信息隐藏算法设置”选项，用于实现信息隐藏算法的选择。信息隐藏算法选择界面实现主要代码如下：

```

android:entries 设置的内容是用户通过界面看到的内容。
android:entryValues 即保存在 preferences.xml 中的值。
在 values/strings.xml 添加定义的属性信息和键值对：
<string name="settings_secret">信息隐藏算法设置</string>
<string name="settings_secret_choose">信息隐藏算法选择： </string>
<string-array name="pref_secret_values">
<item>LSB 信息隐藏算法</item>
<item>DWT 信息隐藏算法</item>
    
```

<item>DWT 信息隐藏算法</item>

<item>...</item>

2、在实时语音通话界面实现秘密信息的输入和查看。在原有通话界面选项的基础上增加“发送消息”和“接收消息”选项。用户点击发送消息，弹出“发送秘密信息”文本框，在文本框中输入要传输的秘密信息，点击“发送”按钮发送要传输的秘密信息。

发送消息其具体的实现过程如下：

在 packageorg.sipdroid.sipua.ui.callscreen.java 里面添加如下代码在通话界面生成发送消息按钮。

```
public static final int SEND_MENU_ITEM = FIRST_MENU_ID + 11;
```

```
private static EditTexttransferText;
```

```
private EditTextScrectText; //要保存的文件名
```

```
private String fileName ="send secret";
```

以下代码实现的是将文本框中输入的隐藏信息以键值对的方式保存：

```
public void onClick(DialogInterface dialog, int which) {
```

```
String in= ScrectText.getText().toString();
```

然后在 RtpStreamSender 中调用键值对的值传入到隐藏信息 info 中，进行 lsb 算法的插入。

```
String info=pref.getString("Secretinfo", "");
```

```
byte[] msg=info.getBytes();
```

接收消息具体的实现过程如下：

在 RtpStreamReceiver 类中开始秘密信息的提取，并以震动的形式提醒用户收到秘密信息。

```
rtp_socket.receive(rtp_packet);/*提取信息*/
```

```
mess +=GetInfo.getInfo(rtp_packet.getPayload());
```

```
if(mess.endsWith("%%*%%*%%")){
```

```
editor.putString("receiver_Info", mess.substring(0, mess.length()-6));
```

```
editor.commit();
```

```
mess="";
```

```
VibratorUtil.Vibrate(Receiver.mContext,1000); //震动 100ms}
```

在 package org.sipdroid.sipua.ui.callscreen.java 里面添加如下代码在通话界面生成“接收消息”按钮，对提取的信息进行查看，主要代码如下：

```
case RECEIVER_MENU_ITEM:
```

```
finalAlertDialog.Builder dialog = new AlertDialog.Builder(this);
```

```
String receive_info=pref.getString("receiver_Info", "");
```

```
receiveText.setText(receive_info);
```

```
dialog.setCancelable(true)
```

```
.setTitle("接收秘密信息")
```

```
.setView(receiveText)
```

```
.setPositiveButton("确定", new DialogInterface.OnClickListener()
```

```
.setNegativeButton("取消", new DialogInterface.OnClickListener()
```

其中重新定义了一个 Vibrate 手机工具类来实现震动提醒。

根据使用要求和所处于的环境，本文在经典的时间域信息隐藏-LSB 算法的基础上对其进行改进来实现信息隐藏功能。信息隐藏算法的实现分为秘密信息的嵌入和秘密信息的提取。

秘密信息的嵌入步骤:

步骤 1: 设置一 byte 数组 data1 存放同步码 + 前标识 + 秘密信息 data0+后标识

步骤 2: 判断载体音频长度是否大于嵌入数据的位数, 即 $radio.length > data1.length * 8$ 。

步骤 3: 将 data1 和 radio 的每个字节转换成 8 位二进制的形式存储, 分别存储到一维数组 ch 和二维数组 chars2 当中。

步骤 4: 用 ch 的每一个元素替换 chars2 每个元素的最低位。

步骤 5: 将 chars2 转换成一个十进制数组, 再转换成 Byte 数组, 进行传输。

秘密信息的提取步骤:

步骤 1: 将音频的每个字节转换成 8 位二进制的形式存进二维数组 chars3 中。

步骤 2: 提取 chars3 每个元素的最低位保存进 chars4 中, 并转换成字符串 d6 中。

步骤 3: 循环判断, 从下标 $i(0-d6.length-1)$ 处开始, 判断第 i 项字符是否为 0。

步骤 4: 在前一步的基础上, 如果第 i 项字符为 0, 则判断判断 $i-(i+47)$ 是否为同步码(000011111111 000011111111000011111111000011111111), 若为真, 则继续判断 $(i+48)-(i+55)$ 是否为前标识(10010001)。

步骤 5: 在步骤 4 的基础上若为真, 则开始提取信息, 每次循环提取 8bit, 并且判断是否是后标识符(10010001)。

步骤 6: 在步骤 5 的基础上判断为真, 则停止提取, 将字符串 d6 转换成字节数组, 再转换成字符串 info 返回即为隐藏信息。

3.2. Sipdroid 信息隐藏功能测试结果分析

首先从语音通话质量、电话使用的流畅度来测试实现的效果。主要从主观角度对实现信息隐藏功能的 Sipdroid 进行整体评价即通过主观感知质量评价标准: 通过人耳对获得语音质量的主观感觉来判断语音隐藏功能实现的好坏, 比较语音信号嵌入秘密信息前后人耳对语音质量的感觉是否发生变化。采用的方法是: 随机选取若干实验者分别对语音信号的质量进行评分, 多次进行测试然后求其平均值得到主观平均分(MOS: Mean Opinion Source)。MOS 是一种绝对等级打分方法采用五级评分标准。MOS 评分方法的标准详见表 1。

进行主观测试的人员为 5 组共 10 人, 男、女各 5 人, 每组分别进行语音通话且每组通话时间不少于 3 分钟, 计算各自的得分并求其平均值, 如表 2 所示, 每隔 20 s 记录测试数据, 对比加入信息隐藏算法前后其中一组延迟率和丢包率变化情况, 结果如图 4、图 5 所示, 通过加入高斯噪声测试系统的鲁棒性, 分析噪声加入前后语音质量的变化。加入噪声前后其中一组的丢包率、延迟率变化情况如图 6、图 7 所示, 嵌入的秘密信息与提取的秘密信息内容如表 2 所示。

因为 Sipdroid 系统处于开放的网络环境下, 所以其使用情况与当时所处于的网络环境有关, 在使用

Table 1. MOS score criteria

表 1. MOS 评分标准

得分	质量级别(SOS)	失真级别(DMOS)
5	优	察觉不到
4	良	刚有察觉
3	中	有察觉, 稍微令人烦躁
2	差	明显察觉, 令人烦躁, 但可忍受
1	劣	不可忍受

Table 2. Information Hiding Implementing MOS Values Table
表 2. 信息隐藏实现 MOS 值表

语音载体		MOS 值						平均值
第一组	嵌入前	4.7	4.6	4.8	4.8	4.8	4.7	4.7
第一组	嵌入后	4.3	4.2	4.4	4.2	4.3	4.2	4.3
第二组	嵌入前	4.6	4.8	4.6	4.9	4.7	4.8	4.7
第二组	嵌入后	4.4	4.2	4.3	4.6	4.2	4.2	4.3
第三组	嵌入前	4.7	4.8	4.8	4.7	4.9	4.7	4.8
第三组	嵌入后	4.3	4.2	4.5	4.2	4.4	4.2	4.3
第四组	嵌入前	4.6	4.8	4.9	4.6	4.7	4.8	4.7
第四组	嵌入后	4.3	4.3	4.5	4.1	4.2	4.4	4.3
第五组	嵌入前	4.8	4.7	4.9	4.8	4.8	4.6	4.8
第五组	嵌入后	4.2	4.3	4.6	4.2	4.4	4.4	4.4

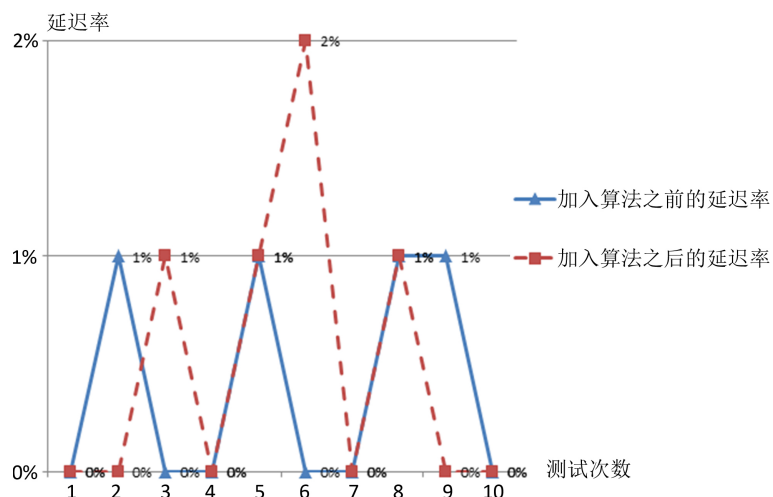


Figure 4. Change chart in the delay rate before and after the algorithm is added
图 4. 加入算法前后延迟率变化图

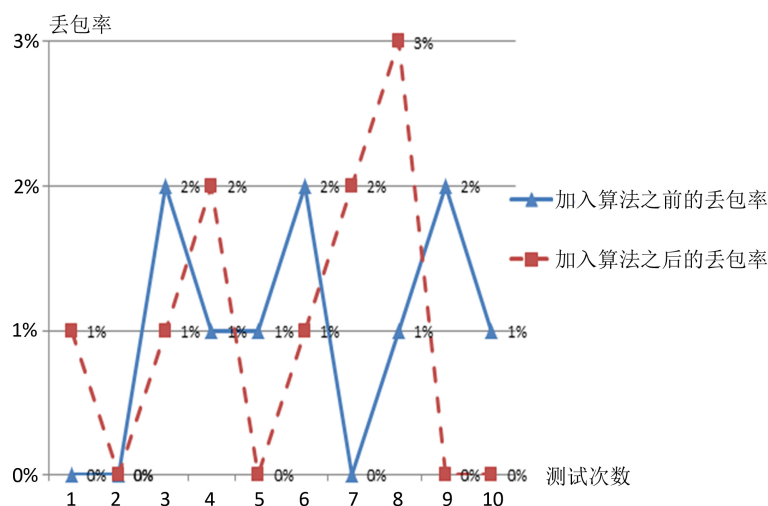


Figure 5. Change chart of the packet loss rate before and after the algorithm is added
图 5. 加入算法前后丢包率变化图

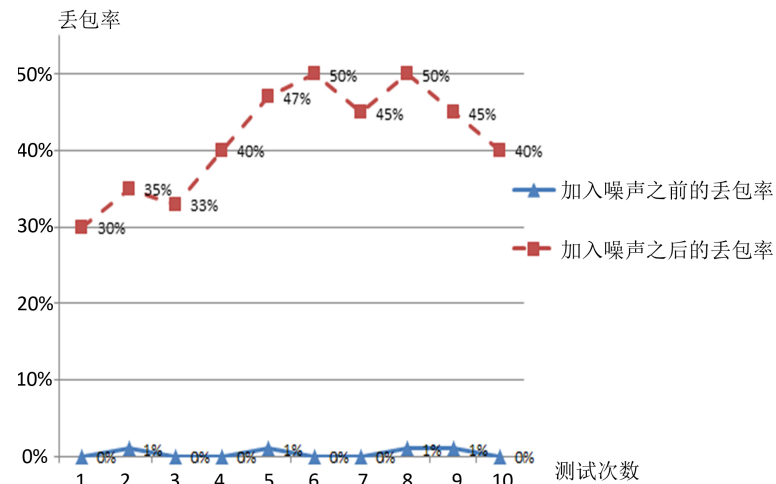


Figure 6. Change chart of the packet loss rate before and after the noise is added
图 6. 加入噪声前后丢包率变化图

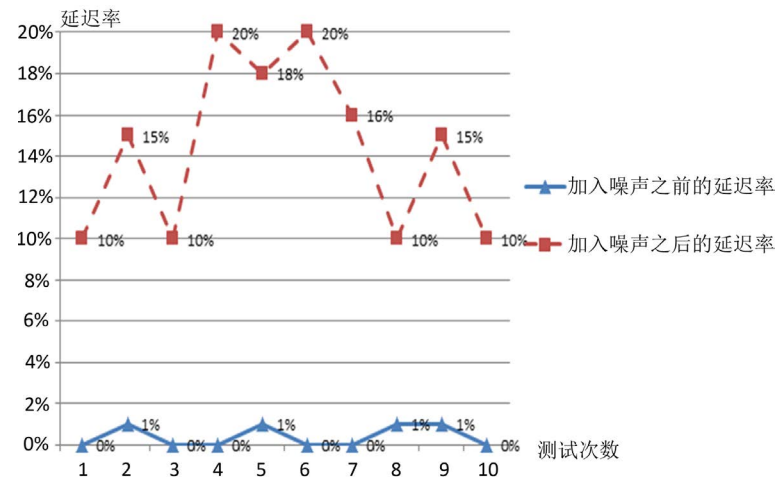


Figure 7. Change chart of the delay rate before and after the noise is added
图 7. 加入噪声前后延迟率变化图

Table 3. Information Hiding Interactive Data Sheets
表 3. 信息隐藏交互数据表

组别	嵌入的信息	提取的信息
第一组	下午 403 开会	下午 403 开会
第二组	我的生日 0101	我的生日 0101
第三组	密码 abc123	密码 abc123
第四组	快来救我	快来救我
第五组	我的邮箱是 123456789@qq.com	我的邮箱是 123456789@qq.com

时可能具有不稳定性。通过表 3 的结果可以得出加入信息隐藏功能的 Sipdroid 系统仍然具有良好的语音质量, 对比图 4、图 5 的丢包率和延迟率, 加入信息隐藏功能之后的 Sipdroid 系统其丢包率和延迟率变化较小, 说明加入信息隐藏算法之后对语音通话的质量影响较小, 说明了算法达到了不可感知性的要求。

由图 6 和图 7 得到, 加入噪声前后丢包率和延迟率的变化较大说明该隐藏算法的鲁棒性需要进一步的改进。由表 3 可以看出不管是使用汉字、英文、数字或者符号, 都能保证嵌入的信息与提取的信息相同, 在保证语音通话质量的同时实现了秘密信息的传递。

4. 结论

本文在开源的 Sipdroid 的基础上, 在语音通话模块中进行信息隐藏功能需求分析、设计、实现。相关功能测试的结果表明: 在进行语音通话的同时完成秘密信息的隐藏、传输, 保证了信息的安全性。在加入信息隐藏功能之后该软件仍然具有很好的使用性, 说明本文研究的内容具有一定的现实意义。

基金项目

河南省高等学校大学生实践创新项目。

参考文献 (References)

- [1] Tian, H., Sun, J., Chang, C.C., *et al.* (2017) Hiding Information into Voice-over-IP Streams Using Adaptive Bitrate Modulation. *IEEE Communications Letters*, **PP**, 1.
- [2] Mazurozyk, W. (2013) Voip Steganography and Its Detection: A Survey. *ACM Computing Surveys*, **46**, 20-26. <https://doi.org/10.1145/2543581.2543587>
- [3] 高振宇. 基于实时语音的信息隐藏的研究与实现[D]: [硕士学位论文]. 广州: 中山大学, 2012.
- [4] 黄永峰, 李松斌. 网络隐蔽通信及其监测技术[M]. 北京: 清华大学出版社, 2016.
- [5] Kratzer, C., Dittmann, J., Vogel, T., *et al.* (2006) Design and Evaluation of Steganography for Voice-over-IP. *Proceedings of the 19th IEEE International Symposium on Circuits and Systems*, **4**, 2397-2340.
- [6] Wu, Q. and Wu, M. (2016) Novel Audio Information Hiding Algorithm Based on Wavelet Transform. *Journal of Electronics & Information Technology*, **38**, 834-840.
- [7] Wang, X.Y. and Zhao, H. (2006) A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT. *IEEE Transactions on Signal Processing*, **54**, 4835-4840. <https://doi.org/10.1109/TSP.2006.881258>
- [8] Bassia, P. and Pitas, I. (2001) Robust Audio Watermarking in the Time Domain. *IEEE Transactions on Multimedia*, **3**, 232-241. <https://doi.org/10.1109/6046.923822>

知网检索的两种方式:

1. 打开知网页面 <http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD>
下拉列表框选择: [ISSN], 输入期刊 ISSN: 2325-2286, 即可查询
2. 打开知网首页 <http://cnki.net/>
左侧“国际文献总库”进入, 输入文章标题, 即可查询

投稿请点击: <http://www.hanspub.org/Submission.aspx>

期刊邮箱: sea@hanspub.org