网络安全中图像隐写术的分析与检测方法

王莹莹，李旋
（公安部第三研究所，上海 200031）

摘 要： 图像隐写是网络空间安全领域一个重要的研究方向，已经有大量的隐写以及隐写分析方法提出。为了解决图像隐写的检测问题，使用实验的方式对文中介绍的图像隐写方法中的拼接和LSB隐写进行分析和测试，结果表明，文中的实验方法能够有效地对图像隐写的隐藏信息进行分析和提取，同时提供了图像隐写在检测中的一般思路。

关键词： 图像隐写；网络空间安全；检测
中图分类号： TP391 **文献标识码：** A

Analysis and test methods of image steganography in cyberspace security

Wang Yingying, Li Xuan
(*The Third Research Institute of Ministry of Public Security, Shanghai 200031*)

Abstract: Image steganography is an important research direction in the field of cyberspace security. A large number of steganography and steganalysis methods have been proposed. In order to solve the problem of image steganography detection, experimental methods are used to analyze and test the collage-based steganography and LSB steganography in the image steganography method introduced in this article. The results show that the experimental method in the paper can effectively analyze and extract image steganography information. Provides general ideas for image steganography detection.

Key words: steganography; cyberspace security; test

1 引言

隐写术是不让计划外的任何接收者知道信息传递事件和隐藏的信息内容的一门科学与技术，通过将秘密数据隐藏在像图像这样的载体文件中，可以实现信息隐写，隐写是一种不可见的通信方式。隐藏秘密数据后，载体文件应该看起来是正常社交通信，以便隐藏嵌入数据的存在。通常隐写术主要分为三类：（1）图像中的隐写术；（2）音频中的隐写术；（3）视频中的隐写术。

然而，随着研究的深入，文字等其它隐写术也已经被提出。在图像隐写术中，秘密消息以无法注意到的图像质量（或者大小）变化的方式隐藏在图像内部。在音频隐秘术中，秘密消息隐藏在诸如歌曲或音乐之类的音频文件中，而不会改变其原始质量。在视频隐写术中，秘密消息隐藏在视频文件中，而不会影响视频的原始质量。在文本隐写术中，秘密消息隐藏在文本文件中，而不会更改其含义。图像隐写技术可以分为两大类，如图1所示的空间域技术和频域技术。在空间域技术中，通过对图像的不同像素进行一些操作，秘密消息被隐藏在图像内部。在频域技术中，通过应用像离散小波变换这样的变换将图像变换为另一种形式，然后通过应用任何常用的嵌入技术来隐藏消息。隐

藏秘密消息的图像称为隐秘图像[1~3]。

本文针对图像隐写术，对其研究，以期分析出图像隐写的通用检测方法。在本文的第2章节中，说明了图像隐写的方法和分析介绍；在第3章节中，通过实验的方法对基于图像隐写的图像进行检测分析；最后在第4章节中得出结论。

2 图像隐写和隐写分析介绍

2.1 图像隐写方法

目前针对图像隐写的方法多样，在空间域中有不同类别的方法：（1）基于拼贴的隐写；（2）最低有效位（LSB）隐写；（3）基于RGB的隐写；（4）像素值差分隐写；（5）基于映射的隐写；（6）基于调色板的隐写；（7）扩频隐写；（8）基于代码的隐写；（9）其他。本文后续章节将对基于拼贴的隐写和LSB隐写进行介绍，其他的隐写方法本文不做解释和分析。

Shahreza[4]提出了一种称为拼贴隐写术的新型隐写术，其中信息通过更改外观而不是其特征而隐藏在图像内部。在这种方法中，将多个对象的图像放在一起以形成新图像。然后，通过更改每个对象的位置和类型，信息将隐藏在图像中。在基于拼贴隐写术中，最简单实现的隐写方式是图像附加，即把隐藏图像附加在载体信息的后面，从而不改变载体信息的像素等特征将隐藏信息添加进去，然而这种方法的问题在于会改变图像的大小，而且使用简单的文件分析工具（如Binwalk等）即可将隐藏信息分析出来，同样基于拼贴的图像隐写都存在数据帧分析以及图像异或等运算问题。

目前，最流行的图像隐写方法是最低有效位（LSB）替换。通过直接替换最低有效位，将消息嵌入到封面图像中。通过在每个像素中使用多达4个最低有效位可以增加隐藏容量。当覆盖载秘样本值的LSB与消息位完全相等时，载秘信息不进行任何更改。否则，样本值不对称地变化。这种不对称性可以通过简单的隐写分析程序捕获。

图1 原图1.jpg

2.2 图像隐写分析

与图像隐写种类繁多一样，隐写分析方法也种类颇多，主要包括通用的隐写分析方法和专用的隐写分析方法。通用隐写分析方法一般包括特征提取和训练分类器两个步骤。其中，隐写分析中的特征是对正常图像和载密图像具有区分能力的统计量。而分类器则是机器学习中常用的SVM、集成分类器（Ensemble Classifier）等可训练优化的类别判别工具。两个步骤中，特征表达是研究中的关键问题，其对检测性能起到决定性的作用。

在传统的方法中，特征表达主要依赖于人工设计，且特征设计的基本思想是找到隐写操作前后图像中具有明显差异的统计量；而专用的隐写分析方法则针对具体的隐写技术，如针对最低有效位隐写，它直接用秘密信息位替换载体图像像素（或JPEG压缩域的量化系数）的最低位。

在空域中，通过分析像素最低位的某些异常特性可以很容易对其进行检测。因为图像最低位并不总是0和1的均匀随机分布，在某些区域呈现与内容有关的结构，LSB替换会破坏这种结构。本文后续章节将使用实验的方法对LSB隐写进行分析[5]。

3 图像隐写和检测

3.1 基于拼接的隐写

3.1.1 拼接隐写

如第2章节所述，基于拼接的隐写是将多个

对象的图像放在一起以形成新图像，本节以信息附加的方法将隐藏信息直接附加在载体文件的尾部，因未改变载体文件的外在特征，因此该隐写方法不易在通信中被发现。该拼接隐写实验步骤如下：

（1）选择一张JPG格式的图像，如图1所示，命名为1.jpg，将需要被隐藏的图像（或文件）命名为2.jpg；

（2）使用二进制的文件拼接命令，Copy /b 1.jpg+2.jpg 3.jpg，将2.jpg文件以二进制的形式添加到1.jpg文件的文件尾，并生成了一张名为3.jpg的新图像，如图2所示。

新生成的图像3.jpg和图像1.jpg除了在文件大小上存在差异之外（差异取决于待隐藏文件的大小），因为没有对图像像素做任何改动，因此外观上无法察觉其是否带有隐藏信息。通过本实验，就把一张图像文件隐藏进了另一张图像中，这是基于拼接的隐写，这是拼接隐写的简单实现方式。

图2 带有载秘信息的图像3.jpg

3.1.2 拼接隐写分析

紧接上节的示例，当拿到一张图像时，需要分析或检测其是否已拼接隐写的方式进行了信息隐藏，可以有四种分析方法：一是查看该图像的属性，若图像大小明显大于一张正常图像的大小，或者使用图像读取工具通过像素等尺寸信息，得出与图像的实际大小不符，则可能使用了拼接隐写；二是使用binwalk文件分析工具，对图像进行分析，查看该图像是否还有其他文件，若含有其他文件，则可能使用了拼接隐写；三是使用StegSlove图像分析工具，通过分析文件格式以及对图像帧进行分析，对图像进行检测；四是使用WinHex数据处理软件，根据文件头、文件尾以及偏移等信息对图像进行判断。下面以第三和第四种分析方法为例，检测上一节中的图像3.jpg是否以图像拼接的方式隐藏了信息以及发现隐藏信息的内容的分析方法。

（1）Stegsolve

Stegsolve软件是一个图像分析工具，该软件功能丰富，后面在分析LBS隐写时还会用到该软件，该软件的特点就是对图像中的信息进行分析挖掘。该软件是一个jar包，不需要安装即可以使用该软件，但是在使用之前需要先配置Java环境变量等系统的基本信息。打开该软件后，选择打开需要被分析的图像文件，使用在Analyse主菜单下的File Format文件类型菜单，对图像文件进行类型分析，可生成一个文件类型的报表，报表的内容涵盖该图像文件的类型、文件头、大小等信息，图像信息显示完后，在End of Image下方，显示了一个额外的附加信息，同样通过内容，可发现另外一张图像，该图像即为被隐藏的图像。再使用该软件Analyse主菜单下的Frame Browser功能，可以看到该图像包含2个数据帧，数据帧2则为被隐藏的信息，如图3所示的第一帧和第二帧。

（2）WinHex

WinHex是一款功能强大的以16 进制编辑器为核心，用来进行计算机取证、数据恢复、低级数据处理、以及 IT 安全性等各种紧急情况的高级工具。同样，基于其丰富的功能，可以使用该工具进行图像分析，分析出隐藏在文件中的信息。使用WinHex软件打开需要被分析的图像文件，找出该图像文件的结束符，本实验分析的jpg文件结束符是FF D9，在该结束符后，还有一部分信息，从结束符可以看出该部分仍然以FF D9结束，如图4所示。选中该区域，选择编辑菜单，将该部分内容另存为新文件，并保存为jpg格式，即可得到隐藏的文件，如图5所示。

至此，以拼接隐写的方式在图像后添加文件进行隐写的方法和主要的分析检测手段做了简

图3 使用Stegsolve软件检测结果

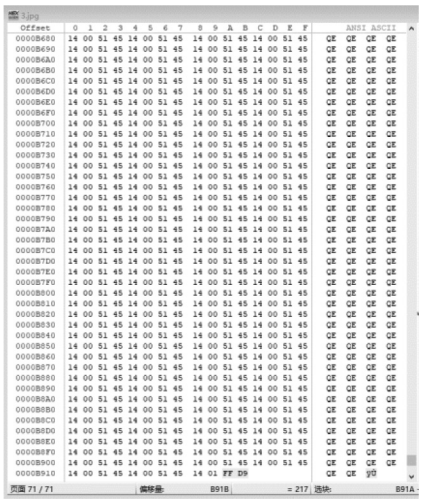

图4 使用WinHex检测结束符图

图5 使用WinHex检测分析结果

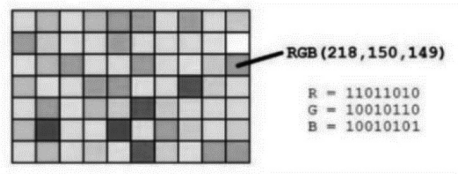

图6 像素的三原色

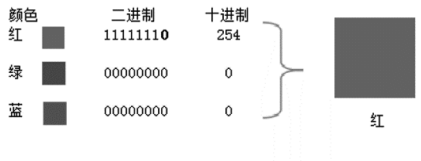

图7 像素中红色分量的最低位变化

要介绍，其他格式的隐藏信息以及载秘文件的不同存在方式，可以使用以上介绍的方式进行检测、分析[6,7]。

3.2 LSB隐写

3.2.1 LSB隐写简介

LSB（Least Significant Bit），即最低有效位，通过直接替换最低有效位，将消息嵌入到图像中，在每个像素中使用多达4个最低有效位可以增加隐藏容量。通常图像中的像素是由红绿蓝三种颜色组成，由这三种颜色可以组成其他各种颜色，如图6所示。以bmp格式的图像为例（因bmp格式的图像未经过压缩），在bmp格式图像的储存中，每个颜色会有8bit，LSB隐写就是修改了像素中的最低的1bit（当最低位不够用的时候，可依次使用高位，但载秘图像会因此变得失真），因此就可以把信息隐藏进来。例如，如果需要把字符‘A’隐藏进来，如图7所示，就可以把A转成16进制的0x61再转成二进制的01100001，再修改红色通道的最低位为这些二进制串，将A写进红色通道的最低位中[8]。

3.2.2 LSB隐写方法

在使用LSB隐写方法进行信息隐写时，可以借助LSB-Steganography工具，该工具的做法是将数据存储在每一个颜色像素（RGB）的第一比特位上。除此之外，如果无法在每一个像素的第一个比特位中存储有效载荷所有的数据，该工具就会使用到第二个比特位，以此类推。

LSB-Steganography工具最基本的指令是LSBSteg.py encode -i -o -f，-i代表输入文件，即载体文件；-o代表输出文件，即含有有效载荷的载秘文件；-f代表有效载荷。使用该条指令即可完成文件的隐写。此外，该工具还提供了隐写信息的提取功能，使用的指令是上条指令的逆过程LSBSteg.py decode -i -o，使用该指令即可在文件操作的路径下生成隐写文件。

本节的第一个实验中以bmp后缀图像为例，使用隐写指令，将00.txt文件中的内容（内容为this is secret）写进in.bmp图像中，生成out.bmp图像，可以使用解码指令检查隐写的正确性，如图8所示。从图中可以看出有效载荷被成功的编码和解码了。

本节第一个实验中将文件内容写入到了图像的最低位中，为了进一步验证该方法的有效性以及写入信息的多样性，在本节的第二个实验中尝试将一张图像写入至另一张图像的最低有效位中，写入方法与第一个实验类似，将图像2.bmp写入1.bmp中，生成3.bmp，因1.bmp的大小（1.2MB）远大于2.bmp（44KB），因此，图像被写入后，不会存在严重的失真，即通过观察，难以察觉图像的不同[9,10]。

3.2.3 LSB隐写检测方法

在上节中，介绍了LSB隐写的手段和实现方法，那么当获取到一张疑似使用了LSB隐写的图像时，应怎样检测出该图像的最低位、次低位甚至其他位是否会有信息被写入。此处，可以继续使用Stegsolve软件，该软件能够对图像按位进行提取，首先选择需要被检测的图像，在Analyse主菜单下选择Data Extract，在该页面中可以选择按行或者列进行像素提取，可选择像素的排序方式，如RGB或者BGR等等，选择待提取的像素位，使用预览或者保存就可以展示已选择出的像素位的信息，针对前一节的第一个实验的实验后生成的图像，选择合适的提取方式（需要进行不同组合方式的尝试），即可将隐写信息提取出来，如图9所示[11,12]。

针对上节中第二个实验得出的图像继续使用上述分析方法，还无法找出被隐写的图像2.bmp，此时可以将图像3.bmp的最低有效位使用Save Bin功能菜单，如图10所示，将最低有效位保存到文件（文件4），用前面介绍的WinHex软件分别打开图像2.bmp和文件4，可以看出文件4从偏移量00000008到偏移量0000AEF1处与图像2.bmp一致，如图11所示。因此可以猜测该部分即是被隐写到图像1.bmp的图像2.bmp，借助3.1.2中的图像分析方法，将文件4该部分偏移量另存为5.bmp，则可还原出被隐藏的图像2.bmp。此处为了更直观的展示文件4即是还原出来的图像2.bmp，在使用WinHex软件时与图像2.bmp进行了对比，在实际检测过程中，无法提前拿到图像2.bmp，可通过分析文件4的文件头以及文件尾等信息确定文件格式，且文件4的特征明显，为BMP文件。

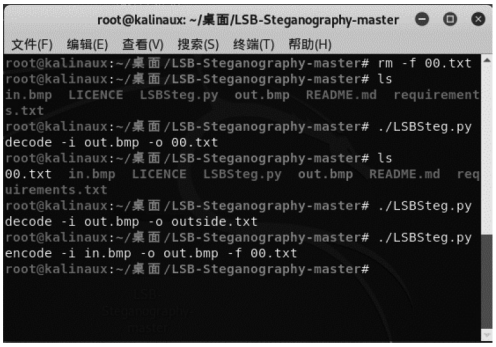

图8 LSB-Steganography信息隐藏和提取

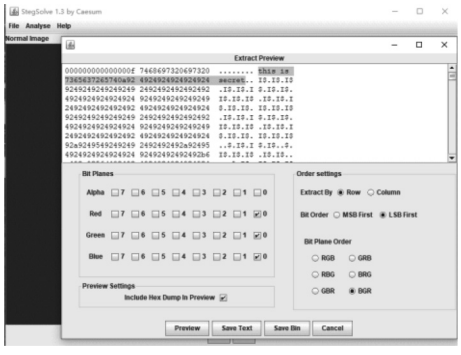

图9 LSB隐写分析和检测

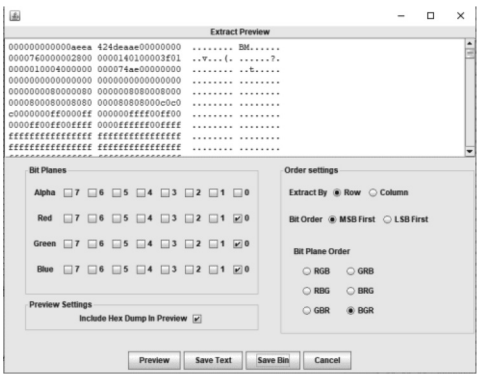

图10 Stegsolve隐写信息提取

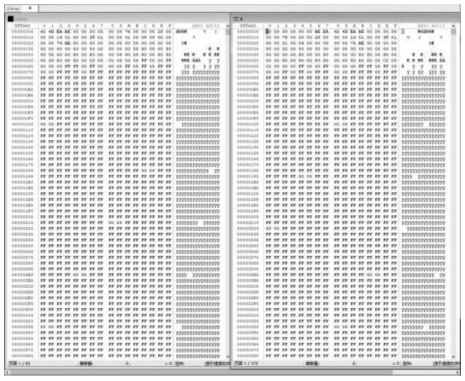

图11 WinHex二进制文件比对

4 结束语

本文介绍了图像隐写技术以及图像隐写的分析检测方法，针对目前图像隐写的特点，总结出图像隐写常用的使用工具和方法，通过实验对真实的隐藏图像进行分析，能够很好地分析出图像中的隐藏信息，归纳出针对特定隐写算法的有效的检测方法，解决了图像隐写术在测试过程中遇到的问题，对图像隐写的测试进行了探索。

基金项目：

国家重点研发计划项目（项目编号：2018YFC0824800）。

参考文献

[1] N. Tiwari, M.Shandilya.Secure RGB image steganography from pixel indicator to triple algorithm-an incremental growth[J]. International Journal of Security and Its Applications, vol.4, no.4, pp.53-62, 2010.

[2] Fridrich J.Steganography in digital media: principles, algorithms, and applications[M].Cambridge: Cambridge University Press, 2010.

[3] 沈昌祥,张焕国,冯登国,等.信息安全综述[J].中国科学E辑:信息科学, 2007, 37(2): 129-150.

[4] 陈嘉勇,王超,张卫明,等.安全的密文域图像隐写术[J].电子与信息学报,2012, 34(7):1721-1726.

[5] C. Cachin. An Information-theoretic model for steganography[A]. In: Proceedings of 2nd International Workshop on Information Hiding, LNCS 1525[C]. Portland, Oregon, USA1998: 306-318.

[6] Gandharba Swain, Saroj Kumar Lenka.International Journal of Computer Science & Engineering Technolog [J].2014,5(3):219-232.

[7] 张军,熊枫,张丹.图像隐写分析技术综述[J].计算机工程,2013,39(4):165-168.

[8] 包震坤,罗向阳.JPEG图像隐写关键问题研究[D].郑州:战略支援部队信息工程大学, 2018. 1-5.

[9] 王朔中,张新鹏,张卫明.以数字图像为载体的隐写分析研究进展[J].计算机学报, 2009, 32(7): 1247-1263.

[10] Nissar A,Mir A H.Classification of steganalysis techniques: A study[J].Digital Signal Processing,2010, 20(6):1758-1770.

[11] 陆兴,黄方军.基于二维直方图修改的JPEG图像可逆信息隐藏[J].网络空间安全, 2019,10(08),55-64.

[12] 陈旖旎,李千目,吕超贤,等.不可见字符的文本安全隐藏算法研究[J].网络空间安全, 2019,10(05),88-96.

作者简介：

王莹莹（1988-），女，汉族，上海人，武汉大学，硕士，公安部第三研究所，实习研究员；主要研究方向和关注领域：通信与信息系统。

李旋（1987-），男，汉族，安徽蚌埠人，兰州理工大学，硕士，公安部第三研究所，助理研究员；主要研究方向和关注领域：网络空间安全。