07.0 隐写分析

钮心忻、杨榆、雷敏
北京邮电大学信息安全中心
yangyu@bupt.edu.cn

前言

- 隐写（steganography）
  - 目的：以表面正常的数字载体如静止图象、数字音频和视频信号等作为掩护，在其中隐藏秘密信息。额外数据的嵌入既不改变载体信号的视、听觉效果，也不改变计算机文件的大小和格式（包括文件头），使隐蔽信息能以不为人知的方式进行传输
- 隐写分析（steganalysis）

前言

- 早在2001 年初，震惊世界的9.11 事件发生半年多以前，美国报纸就曾刊登文章，指出本·拉登及其同伙可能利用某些网站上的大量数字图像秘密传递与其恐怖行动有关的信息如指令、地图、攻击目标的资料等
- 当时还有报道指出，一些著名的网站等已成为传播隐写信息的隐蔽渠道

前言

- 有报道称，首先将科学家在隐写研究中取得的早期成果用于实践的就有基地和哈马斯等国际恐怖组织
- 一些国家的警方也曾在恐怖组织的计算机内查获大量可疑图像和视频文件，据分析可能藏有与恐怖行动有关的信息

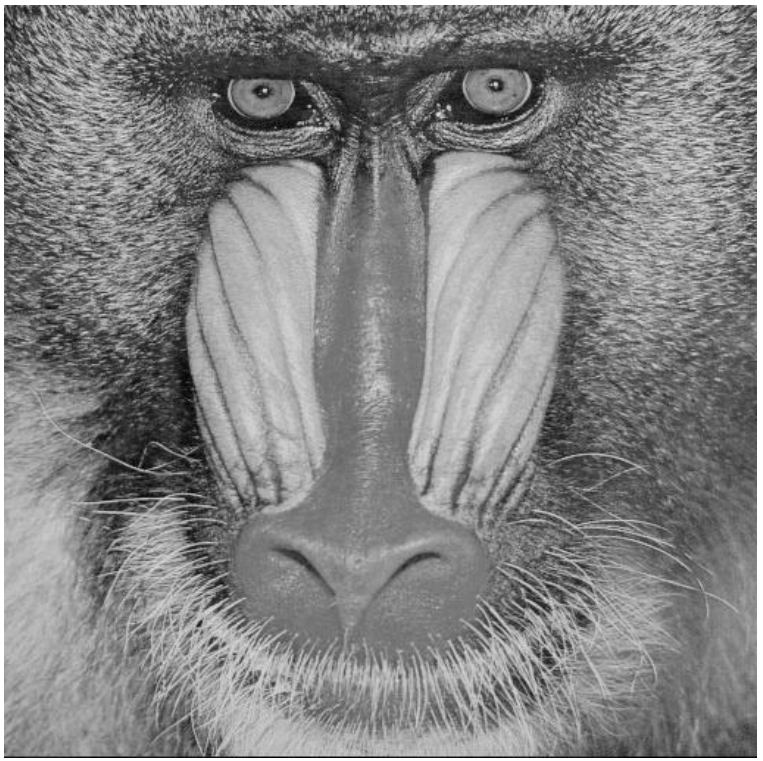
前言

- 一些研究者开始对著名网站上数以百万计的图像展开搜索和检测，试图寻找可能存在的敌对隐蔽信息
- 他们又用所谓字典式攻击法分析了USENET上数以百万计的文档
- 这些工作虽然未能找到隐蔽恐怖信息的确凿证据，却推动了隐写和隐写分析的研究

前言

- 隐写和隐写分析在军事、情报、国家安全方面的重要意义是不言而喻的
- 设计高度安全的隐写方法是一项富于挑战性的课题
- 对隐写的准确分析往往比隐写本身更加困难

隐写分析



隐写分析的目标

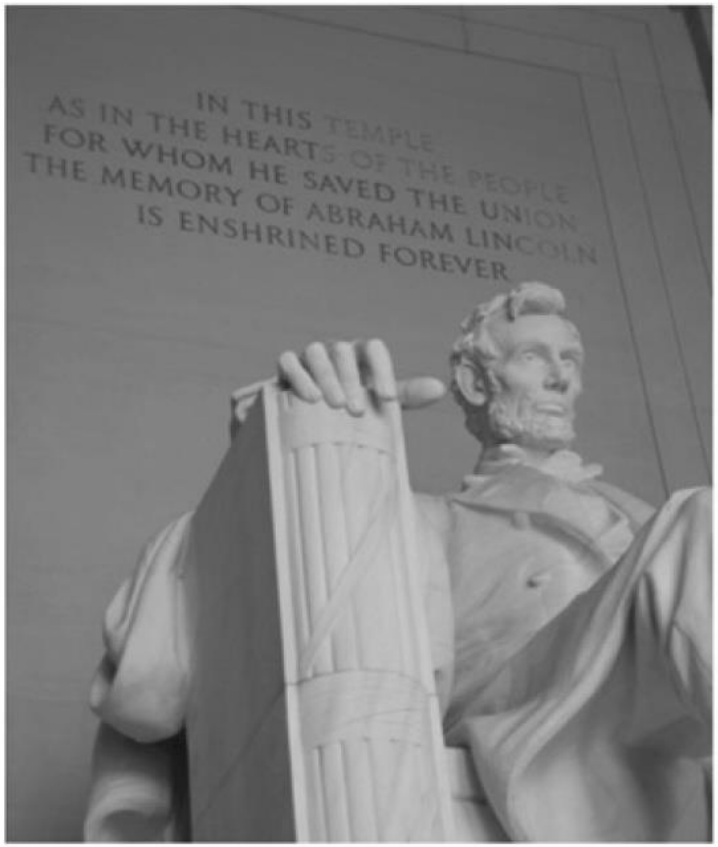
- 判断是否隐写
- 估计隐写量多少
- 提取隐藏信息

隐写分析的分类

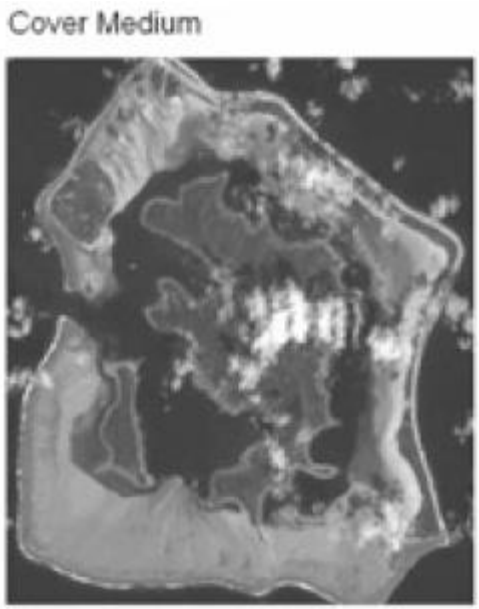
- Stego-only attack
- Known-cover attack
- Known-message attack
- Chosen-stego attack
- Chosen-message attack

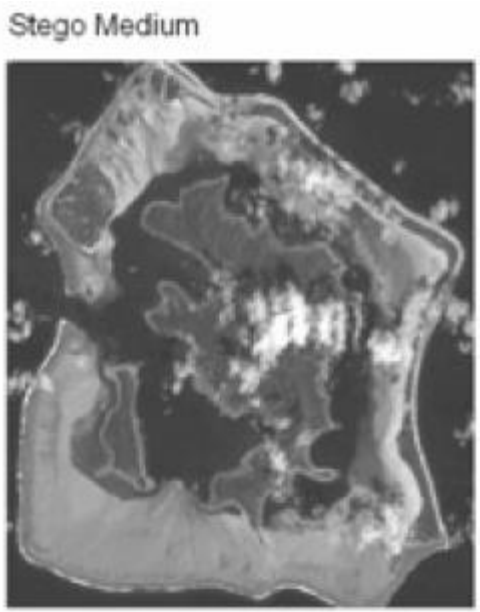
Stego-only attack

- Attack is one where we have only the stego-medium, and we want to detect and extract the embedded message



Known-cover attack





Attack is used when we have both the stego-medium and the cover-medium, so that a comparison can be made between the two

Known-message attack

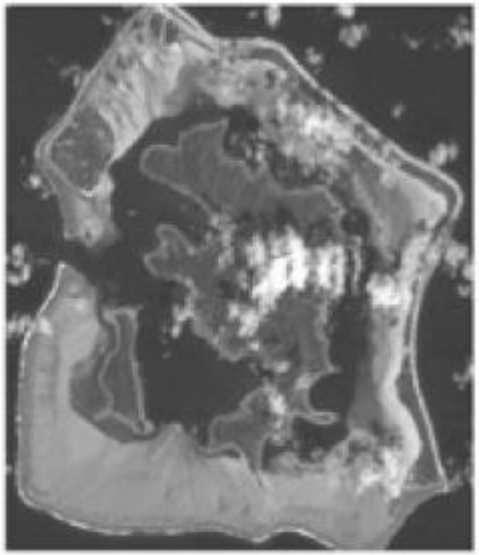
Message

ADDRESS DELIVERED AT THE DEDICATION

OF THE CEMETERY AT GETTYSBURG

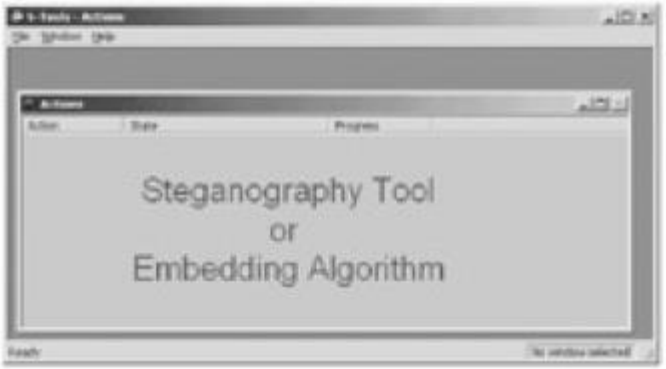
Four score and seven years ago our fathers br
on this continent, a new nation, conceived in Li
dedicated to the proposition that all men are cre
Now we are engaged in a great civil war, testi
that nation, or any nation so conceived and so ded
long endure. We are met on a great battle-field o
We have come to dedicate a portion of that field
resting place for those who here gave their live
nation might live. It is altogether fitting and pro
should do this.
But, in a larger sense, we can not dedicate—
consecrate—we can not hallow—this ground. The
living and dead, who struggled here, have consec
above our poor power to add or detract. The wor

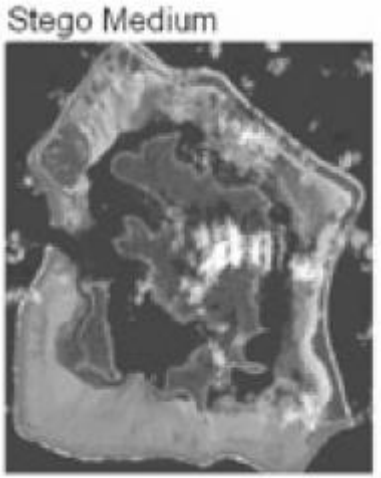
Stego Medium



Attack assumes that we know the message and the stego-medium, and we want to find the method used for embedding the message

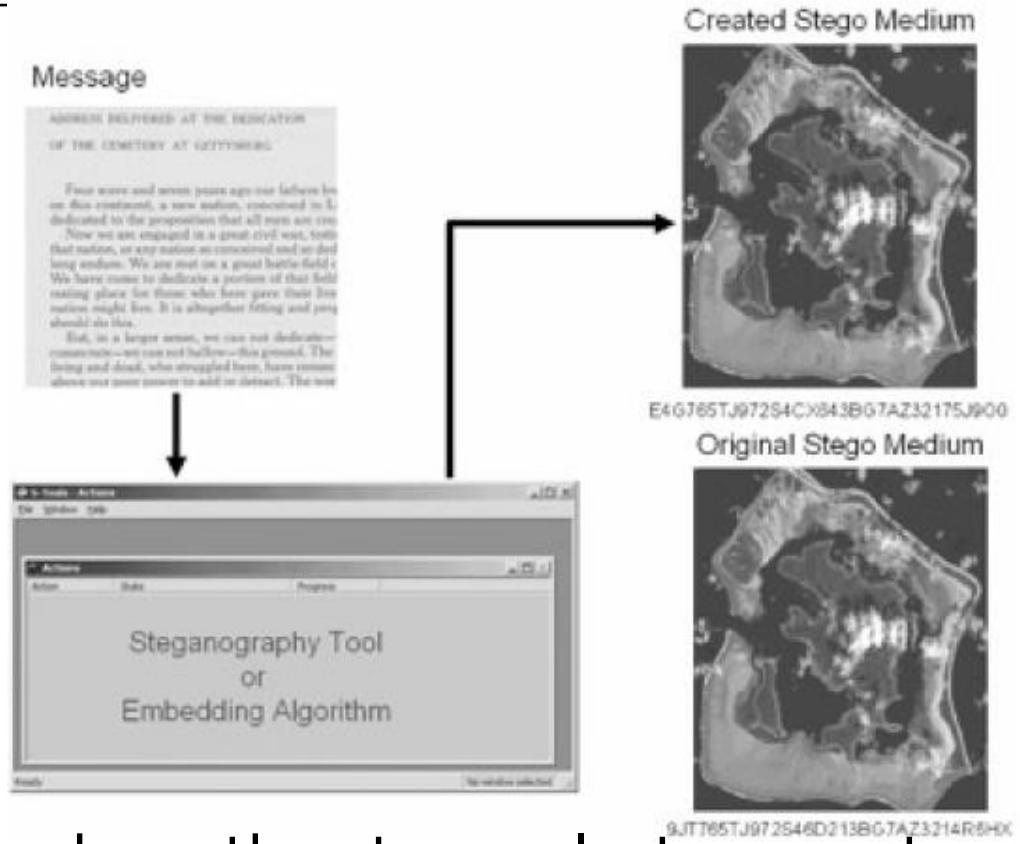
Chosen-stego attack





Attack is used when we have both the stego-medium and the steganography tool or algorithm

Chosen-message attack



Attack is one where the steganalyst generates a stego-medium from a message using a particular tool, looking for signatures that will enable the detection of other stego-media

隐写分析方法

- 感观分析
- 特征分析
- 统计分析
- 通用分析

感观分析

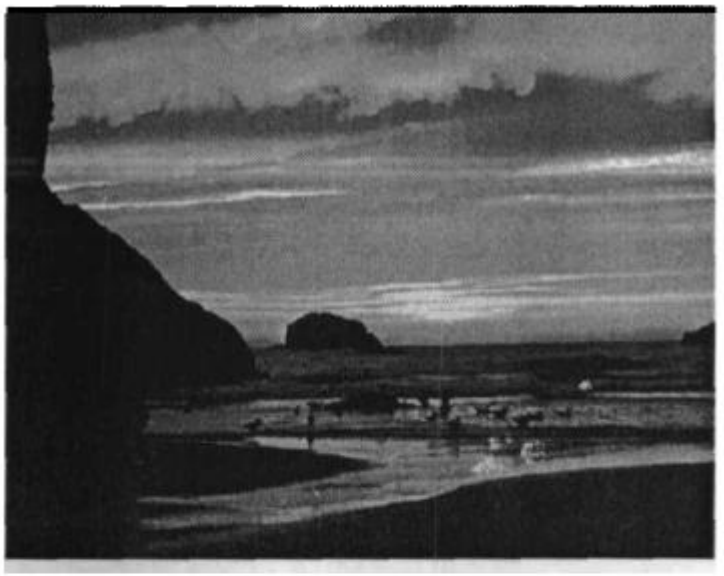
carrier-image

stego-image

the 1th plane of carrier-image

the 1th plane of stego-image

(a)



(b)

(c)

(d)

感观分析

- 优点
  - 简单、直观
- 弱点
  - 自动化程度弱
  - 可靠性弱

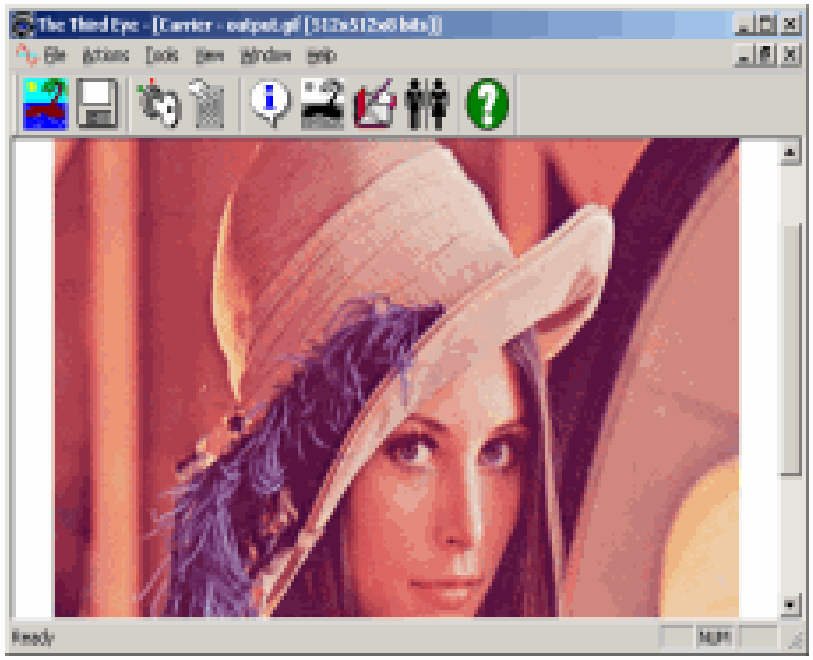
特征分析

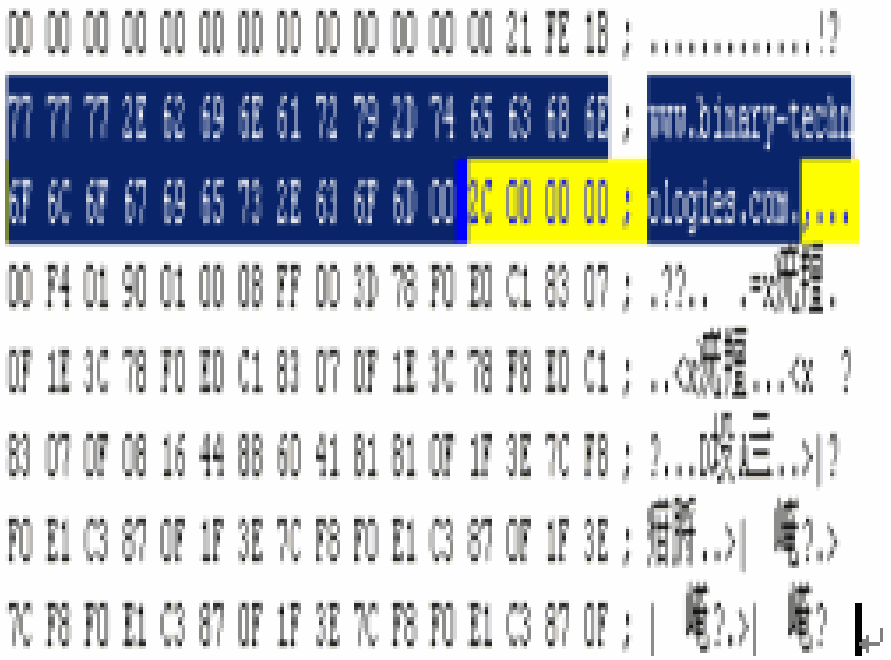
- 基于文件结构的隐写特征
  - 文件大小异常
  - 调色板中有像素没有使用的颜色
  - 。 。 。
- 软件特征
  - 2006年高清晰度DVD视频播放器面世时，使用了强度较高的加密算法。可仅仅6个月之后，系统就被破解了，问题不是出在算法之上，而是算法的实现，攻击者能从内存获取密钥。

特征分析

- 隐写软件特征例1

特征分析





隐写软件TheThirdEye的隐写标记：www.binary-techNologies.com

特征分析

- 隐写软件特征例3
  - 隐写软件Securengin3.0特征码
  - 0111 0000 1101 1110 1011 0010 0100 0110 1101 1010 1110 1111
  - 1111 0111 0100 0110 0011 1101 0010 0100 0001 1110 1010 1000
- 隐写软件特征例4
  - 早期F5算法总插入“JPEG Encoder Copyright 1998, James R. Weeks and BioElectroMech”，而普通图像编辑器几乎不会插入这条信息。

统计分析

- 载体感观效果没有变化，但统计特征改变
- 分析待检测载体的统计特征，可以判断载体是否经过隐写
- 典型方法：
  - 卡方、RS检测等
  - JPEG检测等

通用分析方法

- 通用分析方法
  - 统计分析法需要根据隐写算法原理“一对一”地设计检测特征，通用隐写分析期望提出适用于多种隐写技术的检测算法。
  - 当前研究阶段实现了“通用框架”。即运用同一套统计特征检测多种隐写算法。
    - 基于图像质量特征矩阵的检测算法是一种典型通用隐写分析方法。
    - 算法指出，自然信号与其去噪信号间的“距离”，隐写信号与其去噪信号的“距离”，存在统计差异。算法运用图像质量特征度量这一距离，得出对隐写敏感的特征向量。该方法可以检测多种空域和变换域隐写算法。

通用隐写分析方法

- 通用隐写分析方法一般分为两个步骤
  - 特征分析和设计
    - 利用特征向量来描述自然和隐写载体之间的差异。
    - 考虑到DWT的多分辨率辨析能力，图像常用特征向量包括DWT系数的均值、方差、偏度、和峰度等统计量。
    - 常用方差分析（ANOVA，analysis of variance）来选取特征（即找出对隐写和原始载体的差异最敏感的统计量）
  - 选定特征向量后，通用隐写分析就转变为一个分类问题

参考文献

- 陈铭，隐写与隐写分析算法及实践研究，北京邮电大学博士学位论文
- 《数字密写和密写分析——互联网时代的信息战技术》；王朔中，张新鹏，张开文；清华大学出版社
- 《Digital Watermarking and Steganography》, Ingemar J. Cox, Mathew L. Miller, Jeffey A. Bloom, Jessica Fridrich, Ton Kalker, Elsevier Inc. 2008