

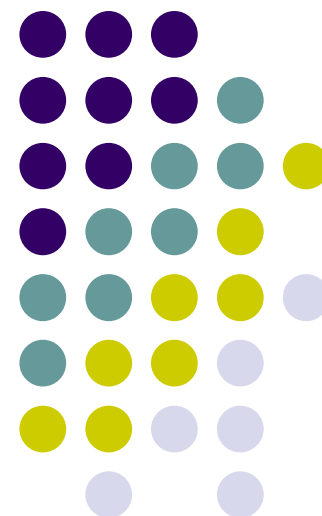
# 信息隐藏与数字水印

## 第一讲：概论与基础

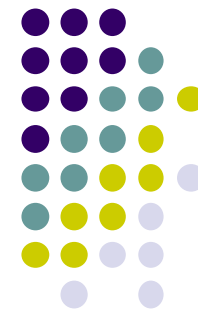
(Information Hiding)

周琳娜

2023.03.29



# 教师简介



- 周琳娜
- 网络空间安全学院 综合楼403室
- [zhoulinna@bupt.edu.cn](mailto:zhoulinna@bupt.edu.cn)
- 13121068100





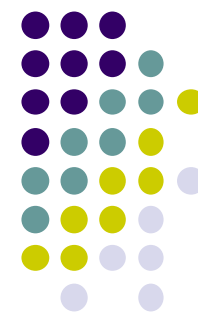
# 课程概论

- 1、技术背景(定义)
- ✦ 2、发展中的信息隐藏(历史)
- 3、信息隐藏与密码术
- 4、信息隐藏与数字水印(学术分支)
- 5、对抗中的信息隐藏
- 6、信息隐藏范例(视频)



# 信息隐藏的历史

- 古代信息隐藏技术
  - 信息隐藏起源于古老隐密术（Steganography，其原形为 Steganographia，源于希腊文  $\sigma\tau\epsilon\gamma\alpha\nu\acute{o}-\zeta$ ， $\gamma\rho\alpha\phi-\epsilon\iota\nu$ ，其字面含义是“covered writing”。
  - 希腊历史学之父Herodotus写于公元前400 多年前的《历史》一书中就描述了许多关于信息隐藏的经典事例。
  - 新长出的头发掩盖刺在头皮上的密文
  - 蜡板传书
  - 中国古代的“藏头诗”



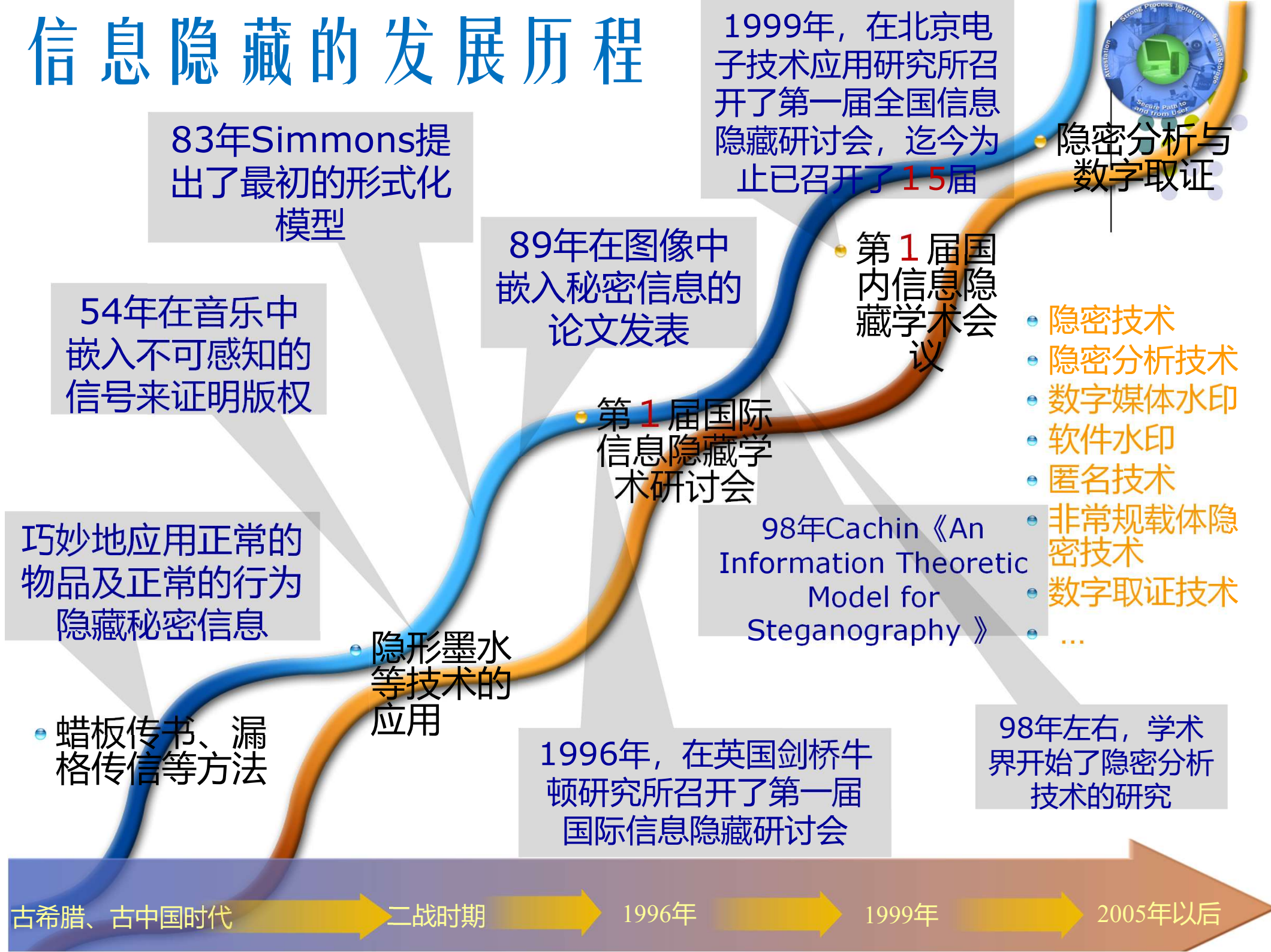
# 信息隐藏的历史

- 近代信息隐藏技术

近代的隐蔽通信很多都采用信息隐藏技术手段

- 信鸽传书
- 隐形墨水
- 缩微摄影
- 语义隐藏
- 扩频通信
- 流星余迹散射通信

# 信息隐藏的发展历程



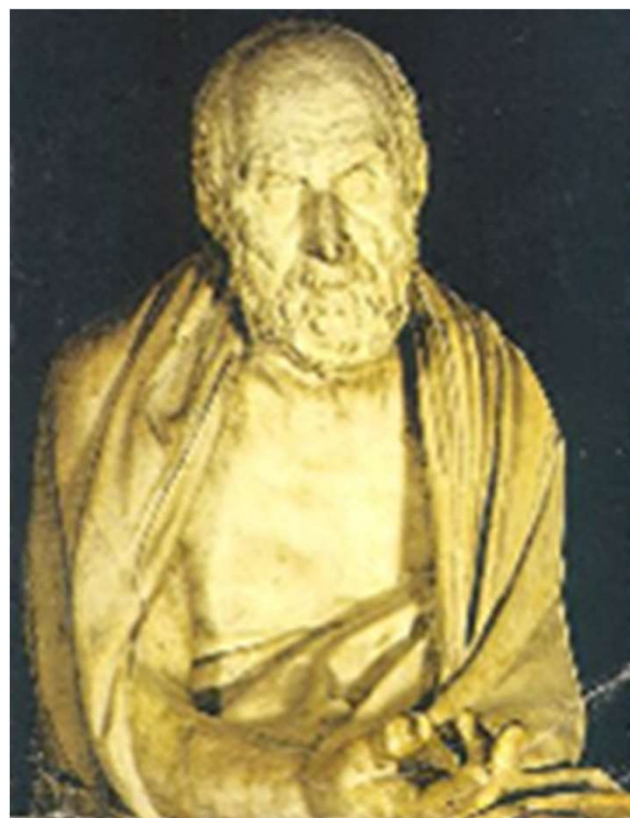


# 古代隐密术

早在公元前440年，**隐密术**就已经被应用

历史上关于隐写术的最早的记载可以在古希腊历史学家希罗多德(公元前**486~425**)的著作中找到

- ❑ 古西腊-奴隶的头皮上写字;
- ❑ 反抗波斯国王入侵-涂蜡板上写字



# 古代隐密术



**隐写术（信息隐藏）**类似于生物学上的保护色，它将主体(某一机密信息)秘密隐藏于外界环境(某公开载体)中，然后通过公开媒体来传输隐藏的机密信息。

- **Stegnography:**

由Johannes Trithemius于1499年将“steganos”与“graphein”两个希腊字根结合，表示“Covered Writing”，意指**隐藏消息的存在性**(Existence)

- **Cryptography:**

由Thomas Browne于1658年创造，表示“Secreted Writing”，意指**隐藏消息的意义**(Meaning)



# 古代隐密术



- 技术性的隐写术
- 语言学中的隐写术
- 用于版权保护的隐写术



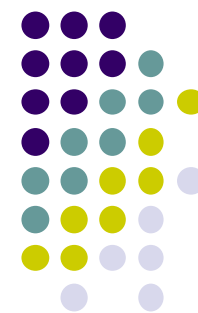
# 古代隐密术—技术性的

- 用头发掩盖信息
  - 将消息写在头皮上，等到头发长出来后，消息被遮盖，这样消息可以在各个部落中传递（公元前440年）
- 使用书记板隐藏信息
  - 首先去掉书记板上的腊，然后将消息写在木板上，再用腊覆盖，这样处理后的书记板看起来是一个完全空白的
- 将信函隐藏在信使的鞋底、衣服的皱褶中，妇女的头饰和首饰中等



# 古代隐密术—技术性的

- 在一篇信函中，通过改变其中某些字母笔划的高度，或者在某些字母上面或下面挖出非常小的孔，以标识某些特殊的字母，这些特殊的字母组成秘密信息
- 采用无形的墨水在特定字母上制作非常小的斑点（17世纪）
- 微缩胶片（1860年）
  - 信鸽传递
  - 粘贴在无关紧要的杂志等文字材料中的句号或逗号上



# 古代隐密术—技术性的

- 使用化学方法的隐写术
  - 用笔蘸淀粉水在白纸上写字，然后喷上碘水，则淀粉和碘起化学反应后显出棕色字体
  - 化学的进步促使人们开发更加先进的墨水和显影剂
  - 但随着“万用显影剂”的发明，此方法就无效了。其原理是，根据纸张纤维的变化情况，来确定纸张的哪些部位被水打湿过，这样，所有采用墨水的隐写方法，在“万用显影剂”下都无效了。
- 在艺术作品中的隐写术
  - 在一些变形夸张的绘画作品中，从正面看是一种景象，侧面看又是另一种景象，这其中就可以隐含作者的一些政治主张或异教思想

# 古代隐密术——语言的



- 藏头诗

豆在山脚下，  
月亮半天挂，  
打柴不见木，  
王里是一家

**化**工何意把春催？  
**缘**到名园花自开。  
**道**是东风原有主，  
**人**人不敢上花台。



**芦**花丛中一扁舟，  
**俊**杰我从此地游，  
**义**士若能知此理，  
**反**躬难逃可无忧。

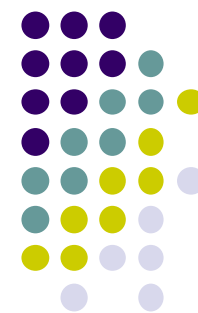
**黄**帝示程书山行，  
**天**籁相伴入翰林，  
**笑**迎万卷七彩路，  
**翌**日神州成精英

# 古代隐密术—语言学的



## 语言学中的信息隐藏

- ◆ 第二次世界大战德国间谍发出的信息：
- ◆ President's embargo ruling should have immediate notice. Grave situation affecting international law. Statement foreshadows ruin of many neutrals. Yellow journals unifying national excitement immensely.
  - Pershing sails from NY June 1.
  - (潘兴号于6月1日从纽约启航。)

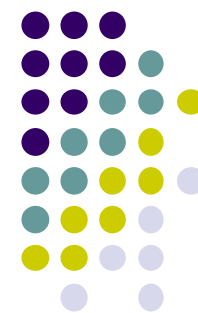


# 古代隐密术—语言学的

- 乐谱

- **在音乐乐谱中隐藏消息，每个音符对应于一个字符**

- 第二次世界大战期间，一位热情的女钢琴家，常为联军作慰问演出，并通过电台播放自己谱写的钢琴曲。由于联军在战场上接连遭到失败，反间谍机关开始怀疑到这位女钢琴家，可一时又因找不到钢琴家传递情报的手段和途径而迟迟不能决断。原来，这位德国忠实的女间谍，从联军军官那里获得军事情报后，就按照事先规定的密码巧妙地将其编成乐谱，并在电台演奏时一次次公开将重要情报通过悠扬的琴声传递出去。



# 古代隐密术—语言学的

- 卡登格子

- 中国古代设计的信息隐藏方法中，发送者和接收者各持一张完全相同的、带有许多小孔的纸，这些孔的位置是被随机选定的。发送者将这张带有孔的纸覆盖在一张纸上，将秘密信息写在孔的位置上，然后移去上面的纸，根据下面的纸上留下的字和空余位置，编写一段普通的文章。接收者只要把带孔的纸覆盖在这段普通文字上，就可以读出留在小孔中的秘密信息
- 在16世纪早期，意大利数学家Cardan(1501-1576)也发明了这种方法，这种方法现在被称作卡登格子法





# 古代隐密术—用于版权保护

- 核对校验图（作品的摘要）
  - Lorrain(1600-1682)是17世纪一个很有名的风景画家，创作了一本称为《*Liber Veritatis*》的书，目的是为了保护自己的画免遭伪造。事实上，只要在素描和油画作品之间进行一些比较就会发现，前者是专门设计用来作为后者的“核对校验图”，并且任何一个细心的观察者根据这本书仔细对照后就能判定一幅给定的油画是不是赝品
- 纸张中的水印

对打

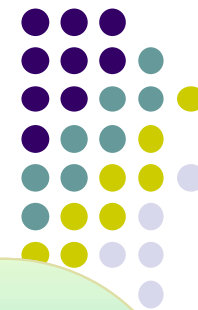
将军问：木兰，听说你出征前，东市买骏马，西市买鞍鞯，南市买辔头，北市买长鞭，你是女扮男装吧？木兰惊问：你怎么发现的？将军道：男人是不会为了买这些东西逛四个集市的...

姜

更



# 对抗是信息隐藏发展的主旋律



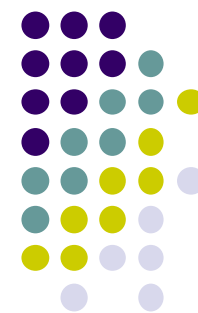
## 三个层次的安全性对抗

破坏秘密信息（鲁棒性对抗）

发现秘密信息（隐蔽性对抗）

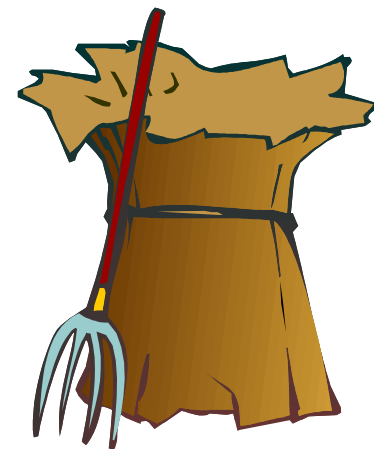
从内容安全  
到行为安全

提取秘密信息（取证性对抗）



# 现代隐密术--在干草堆中藏针

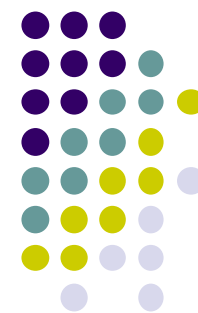
- 公共和私人的网站
- Email
- Newsgroups
- FTP sites
- Peer-to-peer 软件
- Instant messaging (即时通信)
- TCP/IP networking
- Shared file systems
- 互联网这个干草堆可以隐藏大量没有通过检测的数据。



# 信息掩密术的基点



- 隐蔽通信的基点是人类能力的不足
  - 视觉感知
  - 听觉能力
  - 系统设计先天不足
  - 安全性无意识
  - 分析能力
  - 数据冗余的存在



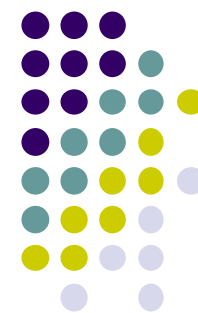
# 信息掩密术的基点

- 利用人类感知系统的冗余
  - **人类感知系统的分辨能力是有限的，对某些频段具有一定的掩蔽效应，比如，人眼对灰度的分辨率只有几十个灰度级别，听觉系统也有类似的局限性。**
- 利用计算机处理系统的冗余
  - **多媒体数据本身存在着很大的冗余。从信息论的角度看，未压缩的多媒体信息的编码效率是很低的，所以将消息嵌入到媒体数据中进行秘密传送是可行的**
- 利用各种潜信道
- 技术上是可行的

# 课程概论



- 1、技术背景(定义)
- 2、发展中的信息隐藏(历史)
- ✦ 3、信息隐藏与密码术
- 4、信息隐藏与数字水印(学术分支)
- 5、对抗中的信息隐藏
- 6、信息隐藏范例(视频)



# 信息隐藏相关学科

利用以

- 数字信号处理理论（图像信号处理、音频信号处理、视频信号处理等）
- 人类感知理论（视觉理论、听觉理论）
- 现代通信技术
- 密码技术

等为代表的伪装式信息隐藏方法来研究信息的保密和安全问题

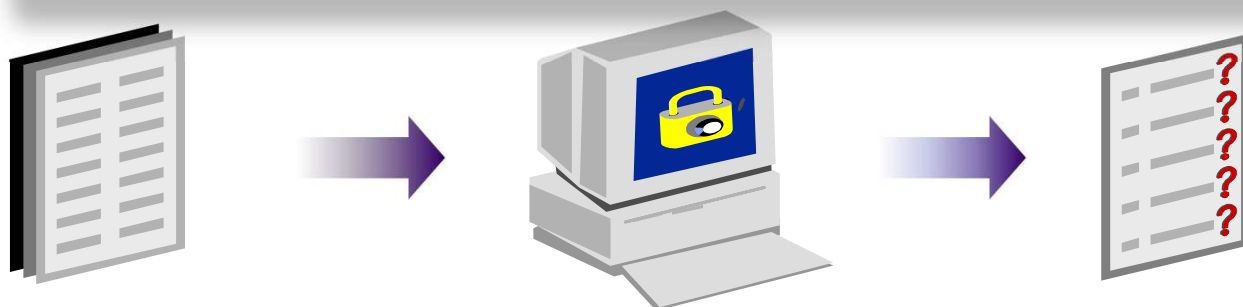


# 信息隐藏相关学科



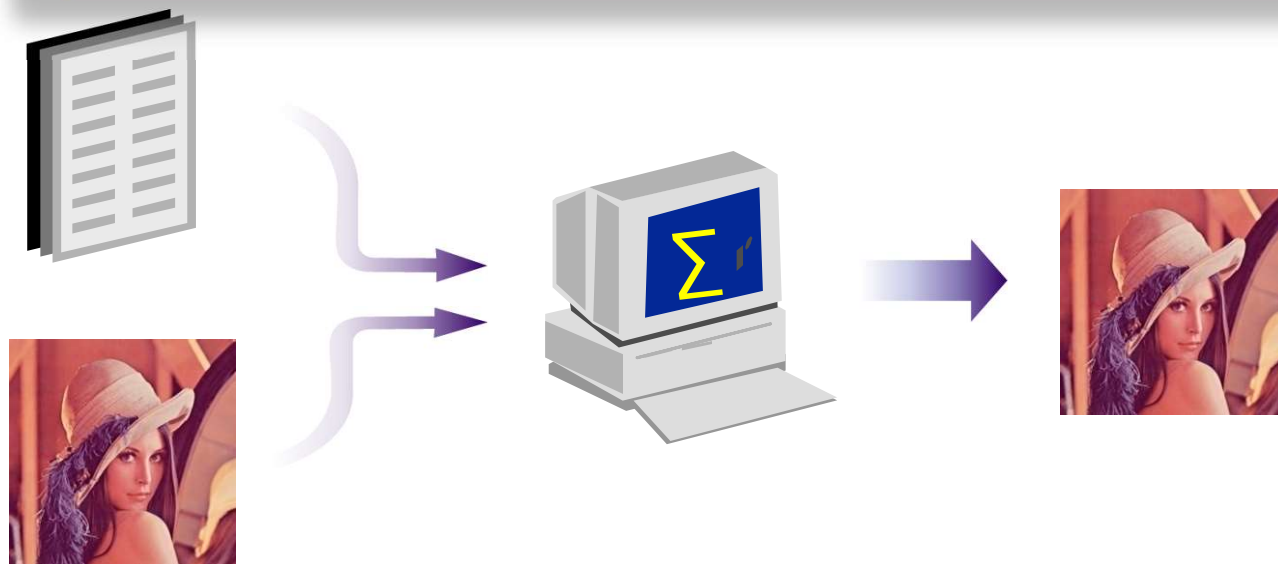
- 信息隐藏与密码学

加密术局限性：明确提示攻击方哪些是重要信息



密码学保护的是  
秘密通信的内容

隐密术：混迹于海量日常数据而不被察觉



信息隐藏保护的  
秘密通信的存在

# 信息隐藏相关学科

- 隐写术**vs**密码术

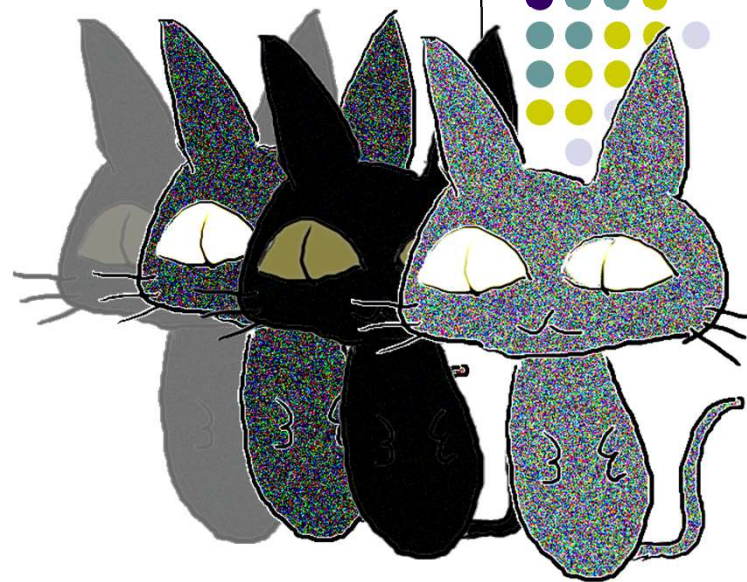


Steganography  
信息“不可发现”

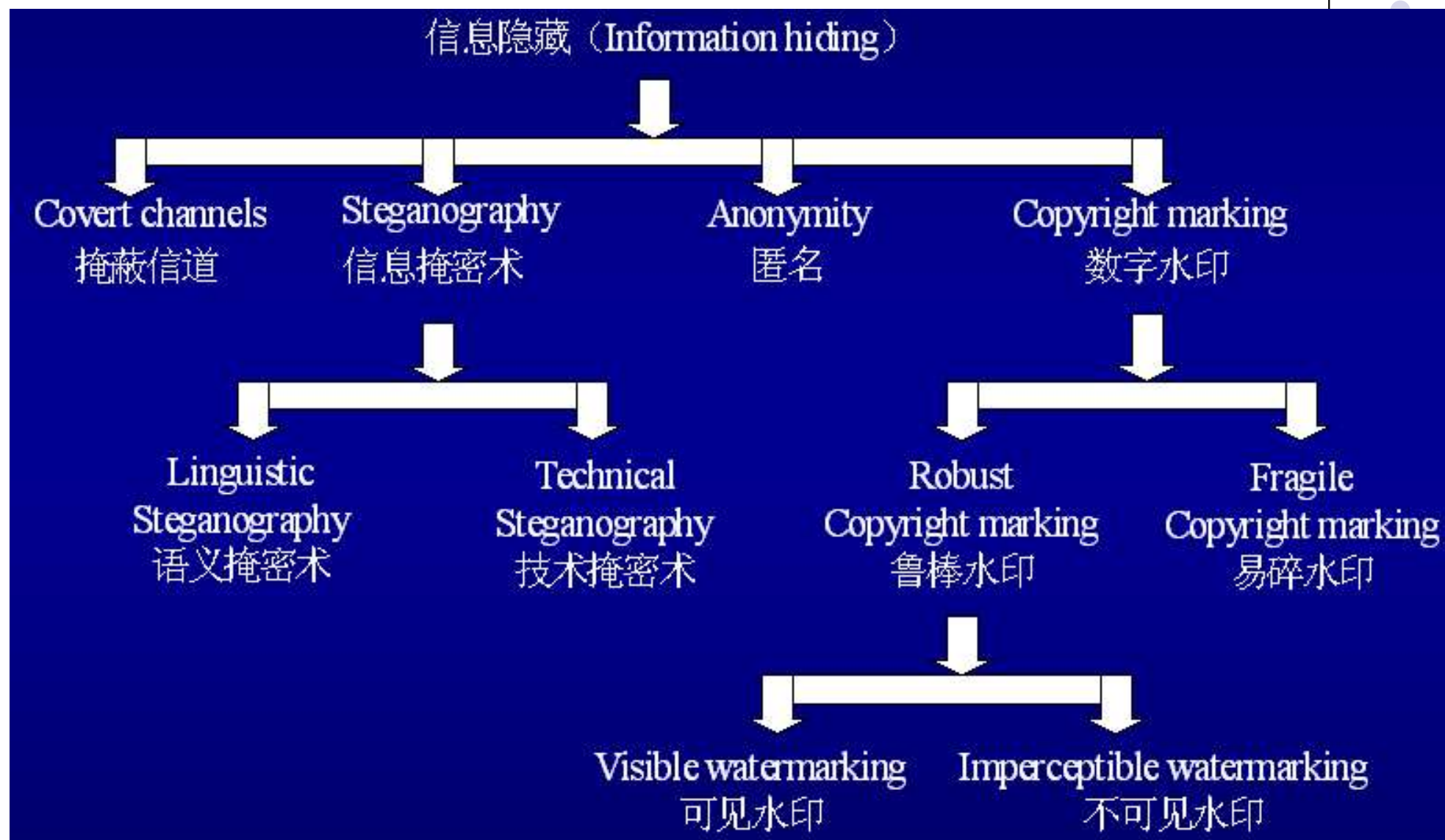
自信、张扬

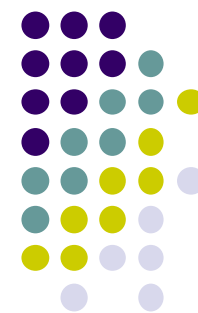
Cryptography  
信息“不可读”

谨慎、内敛



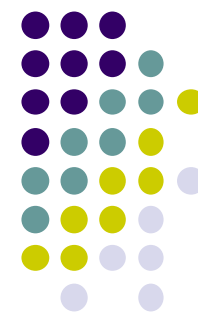
# 信息隐藏的学术分支





# 课程概论

- 1、信息隐藏技术背景(定义)
- 2、发展中的信息隐藏(历史)
- 3、信息隐藏与密码术
- ✦ 4、信息隐藏与数字水印(学术分支)
- 5、对抗中的信息隐藏
- 6、信息隐藏范例(视频)



# 信息隐藏的学术分支

- 两个主要分支

- 隐密术

- 伪装式隐蔽通信

- 数字水印

- 数字产品的版权保护（数字版权管理**DRM**）

- 两个主要方面

- 守—隐写术

- 尽可能多地将信息隐藏在公开消息之中

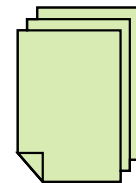
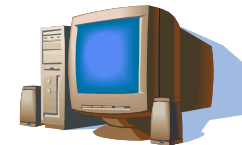
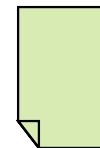
- 尽可能不让对手发现任何破绽

- 攻—隐写分析

- 尽可能地发现和破坏对手利用信息隐藏技术隐藏在公开消息中的机密信息

# 掩密术的类型

- Steganography
- multimedia
  - Images /video/ Audio / Exe
- Network Based
  - TCP / IP Channels
- Text Manipulation
  - Word Manipulation/Substitution
- Operating Systems
  - Data Hiding/Alternate Data Streams

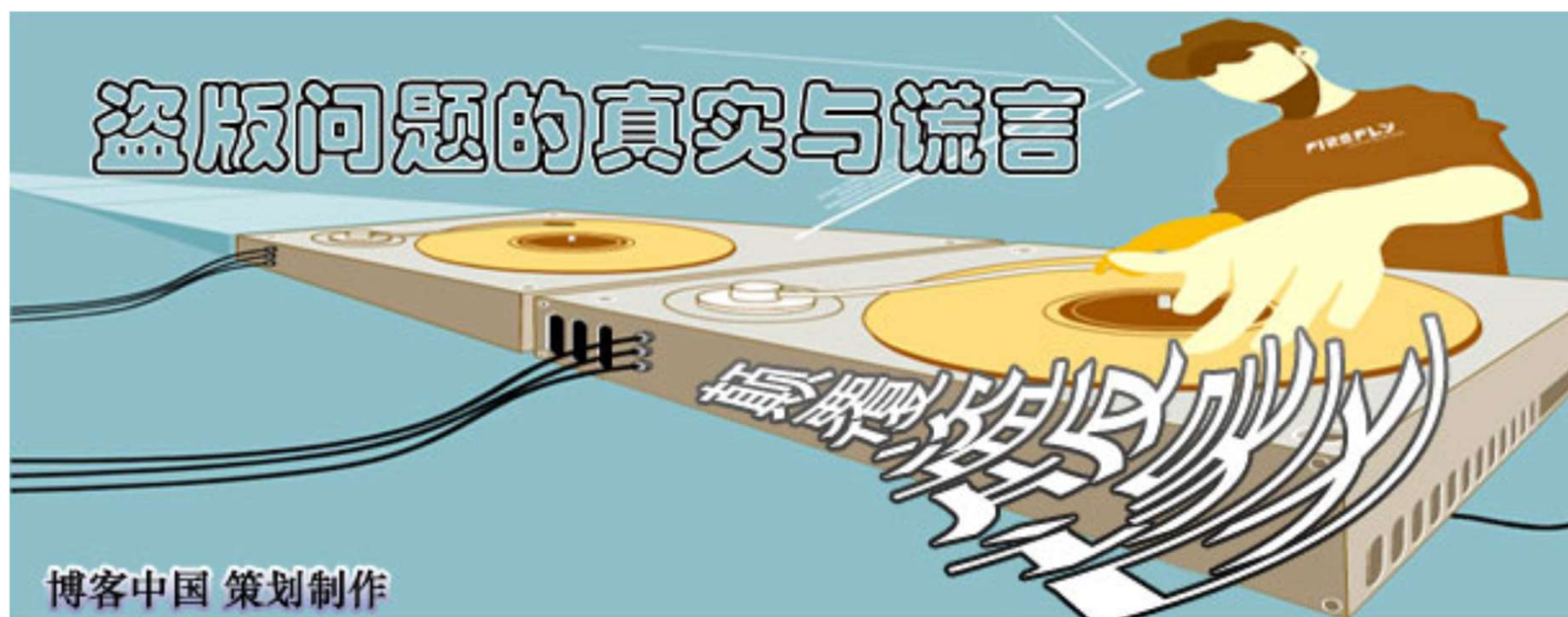






# 数字水印—知识产权保护技术

- 知识产权保护
  - 数字化的全透明性和易操作性为人们带来便利的同时，也使得盗版行为更为容易。
  - 数字水印一种知识产权保护的新技术





# 信息隐藏的应用与发展

## —— 隐密术应用

- 军事和情报部门
  - 现代化战争的胜负，越来越取决于对信息的掌握和控制权
  - 军事通信中通常使用诸如扩展频谱调制或流星散射传输的技术使得信号很难被敌方检测到或破坏掉
  - 伪装式隐蔽通信正是可以达到不被敌方检测和破坏的目的





# 信息隐藏的应用与发展

## — 隐密术应用

- 需要匿名的场合
  - 包括很多合法的行为，如公平的在线选举、个人隐私的安全传递、保护在线自由发言、使用电子现金等
  - 非法的行为，如诽谤、敲诈勒索以及假冒的商业购买行为



# 信息隐藏的应用与发展

## — 数字水印应用

- 用于**版权保护的数字水印**：将版权所有者的信息，嵌入在要保护的数字多媒体作品中，从而防止其他团体对该作品宣称拥有版权
- 用于**盗版跟踪的数字指纹**：同一个作品被不同用户买去，售出时不仅嵌入了版权所有者信息，而且还嵌入了购买者信息，如果市场上发现盗版，可以识别盗版者
- 用于**拷贝保护的数字水印**：水印与作品的使用工具相结合（如软硬件播放器等），使得盗版的作品无法使用

## 隐密术 vs 数字水印

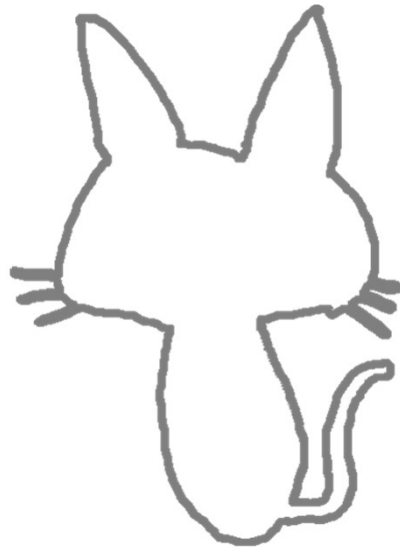


- 保护的目的地不同
  - 信息隐密保护的是内嵌的秘密信息
  - 数字水印保护的是携带载体本身
- 具体应用不同
  - 信息隐密主要应用于隐蔽通信
  - 数字水印主要应用于知识产权保护
- 实现的方式不同
  - 信息隐密在秘密信息提取时一般不需要原始载体信息
  - 数字水印在水印认证时有时需要原始信息有些甚至需要提供水印信息

# 隐密术 vs 数字水印



**Covert  
communication  
invisible**

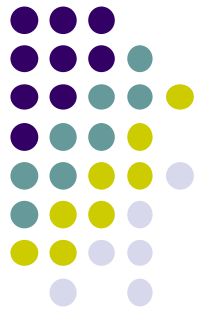


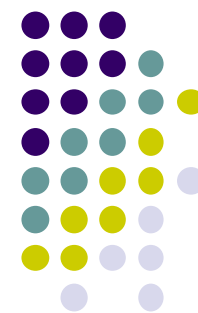
**Watermark**

**“non-distortion”**



休息中。。。○ ○ ○





# 课程概论

- 1、技术背景(定义)
- 2、发展中的信息隐藏(历史)
- 3、信息隐藏与密码术
- 4、信息隐藏与数字水印(学术分支)
- ✦ 5、对抗中的信息隐藏
- 6、信息隐藏范例(视频)

# 隐密术的两个对立面-攻与守



- 守—隐写术
  - 尽可能多地将信息隐藏在公开消息之中
  - 尽可能不让对手发现任何破绽
- 攻—隐写分析
  - 尽可能地发现和破坏对手利用信息隐藏技术隐藏在公开消息中的机密信息

# 隐密术--守



被卫星收集到的苏联战略轰炸机  
(卫星数据)

+



用S-Tools工具隐藏机场图片  
(载体为名画)



隐藏后的图像  
(感知无差别)

机密信息的隐蔽分发



# 隐密分析--攻

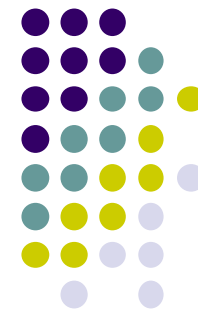


- 《今日美国》文章摘要：

美国政府官员和专家说（密写）是本·拉登及其亲信使用的最新通信手段。



# 隐密分析--攻



- 在隐密术的应用中，使用者的伦理道德水平并不是很清楚，尤其是使得部分不法分子有机可乘

2001

穆斯林恐怖分子，今日美国发表文章；“9.11”事件治之后，纽约时报等

2006

印度媒体报道孟买火车爆炸案中使用了隐密术

2007

美国NBC报道了伊斯兰恐怖组织“基地”对隐密术的使用

2010

美国FBI破获情报网络，文件显示间谍嫌犯使用数字隐密术进行通信

2011

Google新闻报道南美洲毒贩利用数字隐密术传递信息

隐密术的对立面—隐密分析技术，刻不容缓



# 对抗中的现代隐密术



1、一个基本模型-囚徒模型

- 2、两个重要指标:隐蔽性和容量

- 3、三重对抗境界

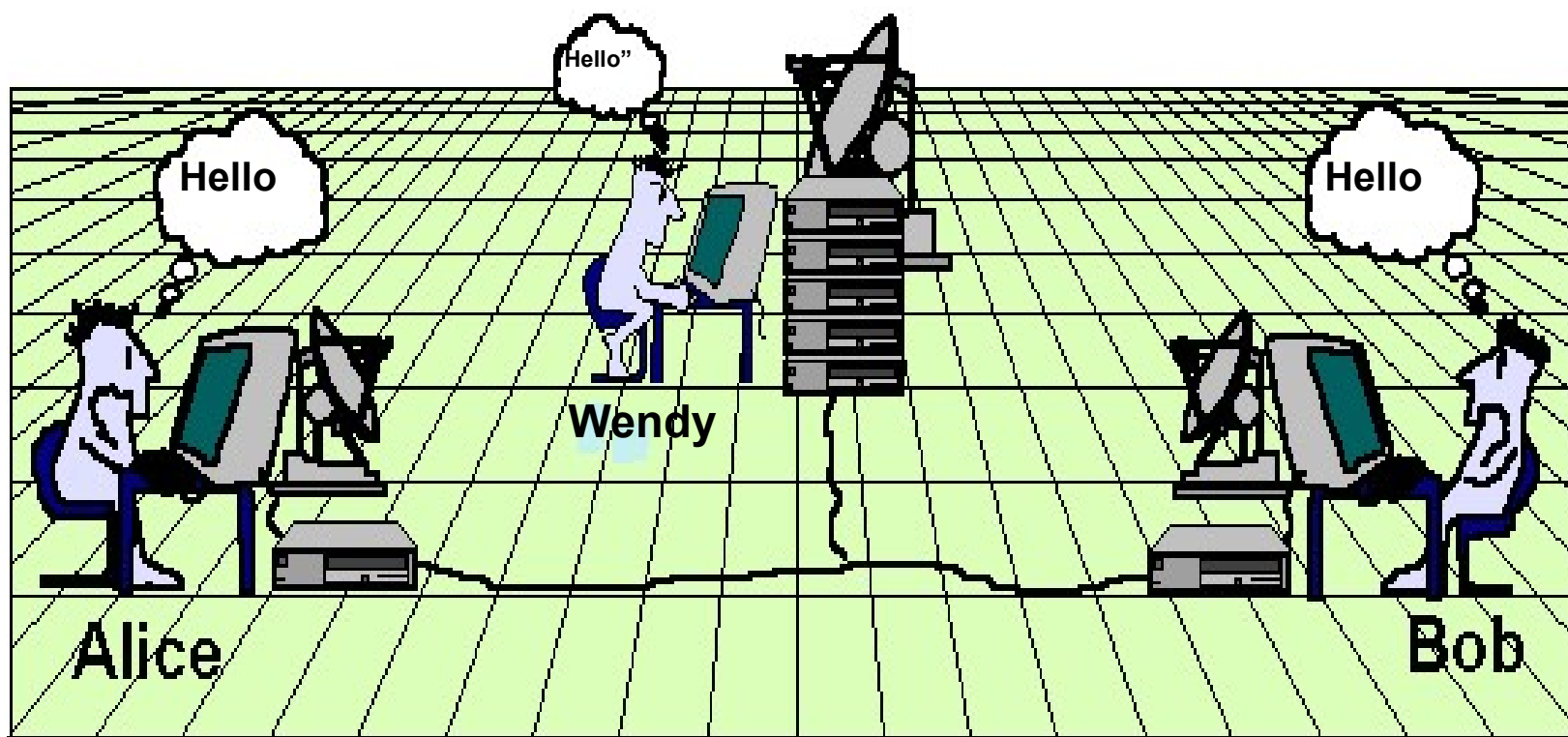
- 见招拆招

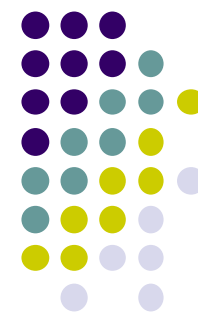
- 一招制胜

- 无招胜有招

# 一个基础模型

## 不可视通信模型（囚犯问题）





# 一个又一个模型

- 信号处理为基础模型

- 以失真为约束的模型

- 以信息论为基础模型

- 以互信息为约束的模型
- 以相对熵为约束的模型

$$d(x, y) = 1/n \sum_n (x_i - y_i)^2 = \varepsilon$$

$$I(M, X) = \varepsilon$$

- 以博弈论为基础模型

$$D(P_C | P_S) = \varepsilon$$

- 把隐藏者和攻击者看成博弈双方，利用博弈论在特定的约束下，求解隐藏容量。

- 以认知论为基础模型

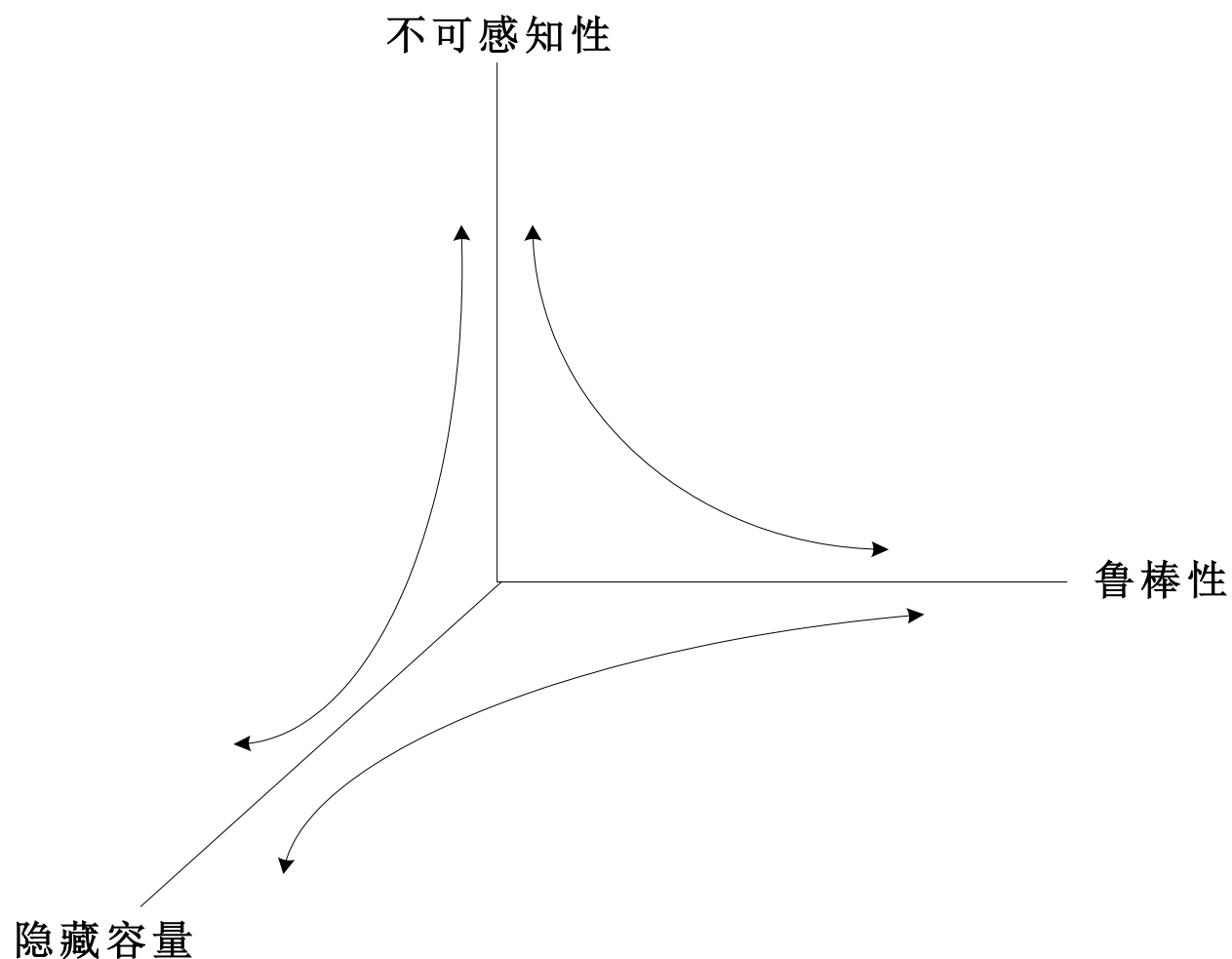


# 对抗中的现代隐密术

- 1、一个基本模型-囚徒模型
- ★ 2、两个重要指标:隐蔽性和容量
- 3、三重对抗境界
  - 见招拆招
  - 一招制胜
  - 无招胜有招

# 三个特性中的两个重要指标

不可感知性、鲁棒性与隐藏容量之间的关系

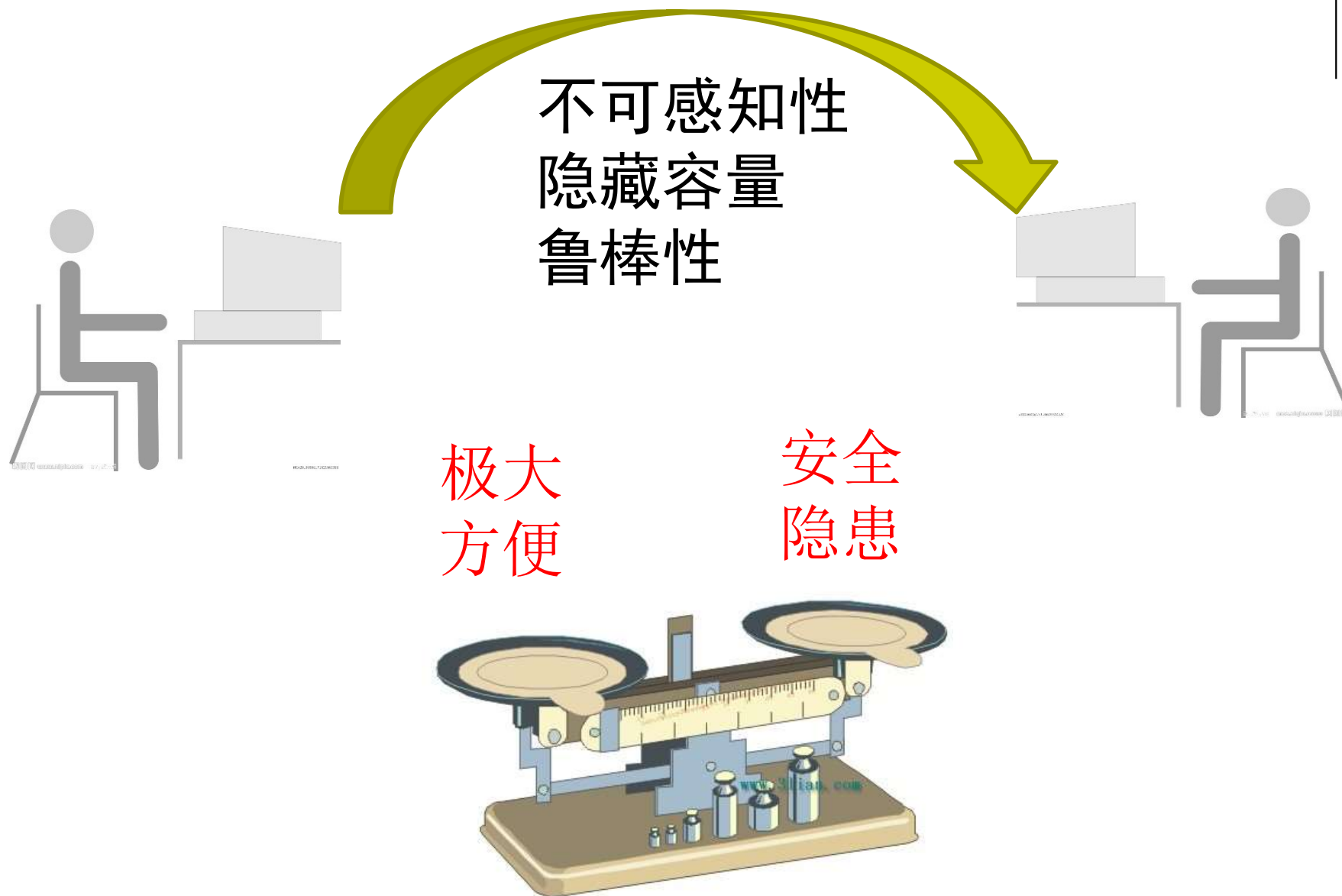


信息隐密三个指标  
重要程度排序为：  
不可感知性、隐藏  
容量、鲁棒性

数字水印三个指标  
重要程度排序为：  
不可感知性、鲁棒  
性、隐藏容量



# 三个特性的关系(权衡与折中)







# 对抗中的现代隐密术

- 1、一个基本模型-囚徒模型
- 2、两个重要指标:隐蔽性和容量
- 3、三重对抗境界



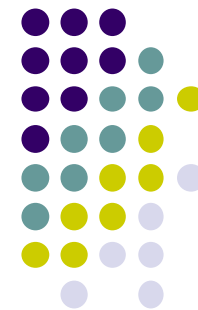
见招拆招(隐密和隐密分析技术)

- 隐密算法-分析算法-抵抗分析算法的隐密算法-对应的分析算法
- 一招制胜
- 无招胜有招

# 对抗第二境界：一招制胜

## ----通用性统计检测

- 信息隐藏盲检测
  - 特征+分类器
  - 先学习后检测.

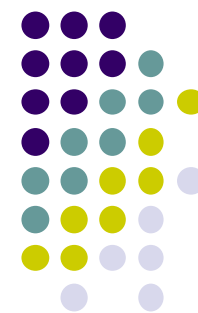




# 对抗的最高境界:无招胜有招

## ----对抗通用性统计检测

- 筛选隐藏法
  - 先隐藏
  - 后检测
  - 保证无疑



# 对抗的最高境界:无招胜有招

## ----对抗通用性统计检测

- **藏和变的问题**

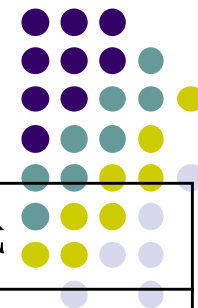
- 藏：需要冗余
- 压缩和压缩同分一块蛋糕
- 变的可行性
  - 七巧板方法
  - 三角剖分发
  - 数系的变换
  - DNA隐藏
  - 藏头诗

# 公开的多媒体信息隐藏技术

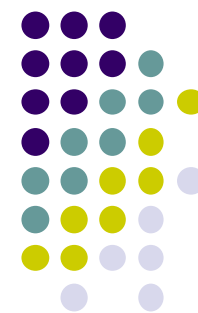


- 信息隐藏的算法已有许多，如图像为载体的有：最低有效位替换、多位平面替换、随机调制(扩频)、调色板隐写、基于DCT系数和小波系数的隐写等。
- 以现有的隐写技术为基础，互联网上有许多可免费下载的数字隐写软件，如Johnson N在其个人网站上列出了一百多种隐写软件。
- <http://www.jjtc.com/Steganography/toolmatrix.htm>

# 互联网上常见的图像隐写软件



序号	工具	作者及网址	主要方法	图像格式
1	BMP Secrets	<a href="http://www.pworlds.com">http://www.pworlds.com</a>	空域替换方法	JPEG, GIF, BMP等
3	DCT-Steg (DCT-Jpeg)	Stefan Katzenbeisser <a href="http://www.dbai.tuwien.ac.at/staff/katzenb/stego/robust-st.html">http://www.dbai.tuwien.ac.at/staff/katzenb/stego/robust-st.html</a>	DCT系数修改	JPEG
4	EzStego	Romana Machado <a href="http://www.stego.com">http://www.stego.com</a>	LSB方法	GIF
5	F5 v0.9	Andreas Westfeld (Dresden, Germany) <a href="http://www.inf.tu-dresden.de/~aw4">http://www.inf.tu-dresden.de/~aw4</a>	修改量化后的DCT系数	BMP, GIF, JPEG
6	Hide and Seek	Colin Moroney	空域LSB方法	BMP
7	JP Hide and Seek	Allan Latham, <a href="http://linux01.gwdg.de/~alatham/-stego.html">http://linux01.gwdg.de/~alatham/-stego.html</a>	修改量化后的DCT系数	JPEG
8	JPHSWin	Allan Latham <a href="http://linux01.gwdg.de/~alatham/stego.html">http://linux01.gwdg.de/~alatham/stego.html</a>	修改量化后的DCT系数	JPEG
9	JSteg Shell	John Korejwa <a href="http://www.tiac.net/users/korejwa/jsteg.htm">http://www.tiac.net/users/korejwa/jsteg.htm</a>	修改量化后的DCT系数	输出JPEG
10	JSteg-Jpeg	Derek Upham <a href="http://linkbeat.com/files/">http://linkbeat.com/files/</a>	修改量化后的DCT系数	输出JPEG
11	Mandelsteg	Henry Hastur	LSB算法	GIF
12	OutGuess	Niels Provos <a href="http://www.outguess.org/">http://www.outguess.org/</a>	修改量化后的DCT系数	JPEG, PNM
13	S-Tools v4.0 (stools)	Andy Brown, <a href="ftp://ftp.demon.net/pub/-mirrors/crypto/idea/code/s-tools4.zip">ftp://ftp.demon.net/pub/-mirrors/crypto/idea/code/s-tools4.zip</a>	LSB算法	BMP, GIF
14	White Noise Storm	Ray (Arsen) Arachelian	扩频+LSB	PCX
15	Steganos Security Suite III	DEMCOM, Fabian Hansmann <a href="http://www.steganography.com">http://www.steganography.com</a>	LSB算法	BMP, DIB



# 课程概论

- 1、技术背景(定义)
- 2、发展中的信息隐藏(历史)
- 3、信息隐藏与密码术
- 4、信息隐藏与数字水印(学术分支)
- 5、对抗中的信息隐藏
- ✦ 6、信息隐藏范例(藏与变)

1 我在这个世界上生活了十几年，虽总在加强情操的培养，但是有的时候，仍然很难做一些性命悠关的大决定。生存，还是毁灭，这是个问题。莎士比亚的这个疑问困扰了古代无数的哲人。

2 他人的利益重要，还是自己的利益重要？为了祖国是不是该牺牲个人的利益？为人民服务的宗旨是不是要坚持？这是我们的品德教育用了十年，才使我们彻底弄清的问题。革命先烈用八年抗战，为我们做出了最好的回答。我们这代人是跨世纪的一代，将来会面对更多的诱惑。正因为如此，我们必须从小就树立一切为了他人的崇高信念。

3 生命是人最宝贵的财富，但是在重要的时候，个人利益必须牺牲。\*\*\* 在刺骨的冰水中救孩子，这是他心灵的选择。他牺牲自己，让孩子的生命得到延续。而在我们的生活中，大多没有这么极端的情况。但也不能有一点危险就屁滚尿流。做出牺牲自己的选择，不只是象用眼睛看来那么简单的。我们必须时时反省自己，只有时刻严格要求自己，才可能成为一个完整的人。

4 个人的利益首先还要服从集体利益，就像当年一个人再怎么成功，其力量也不能改变国家孱弱的现实。个人的智慧再强大，也比不上

集体智慧。是全  
穷二白的面貌，  
奋斗痴心不悔，  
雷锋像，我们就  
事迹逼自己努力  
不是神。做出牺  
然要经历的。这  
排除病态的极端  
自己，做出正确  
5 一个人的力  
伟目标。所以如  
时刻准备，甚至  
能象猪一样，只  
样抛头颅，洒  
自己。只有人  
才能还我国以  
好。不过，让  
但是如果我  
到从我做起，  
实现的。

6 大的理想  
起，便容易成  
只是有崇高的  
保持头脑的清  
铭记脑海。太  
强大。

數學老師與老婆離婚  
臨走女方在離婚書背後  
寫著：

$$145 \times 154 \div 4 (1+1) 80$$

事後，老教授用盡各種  
數學專業，仍苦思不得  
其解。索性上課時在黑  
板要求學生解答，某學生  
脫口而出～

一事無成 一無是處 死玉八星

譚浪手抄



➤ 反躬难逃可无忧

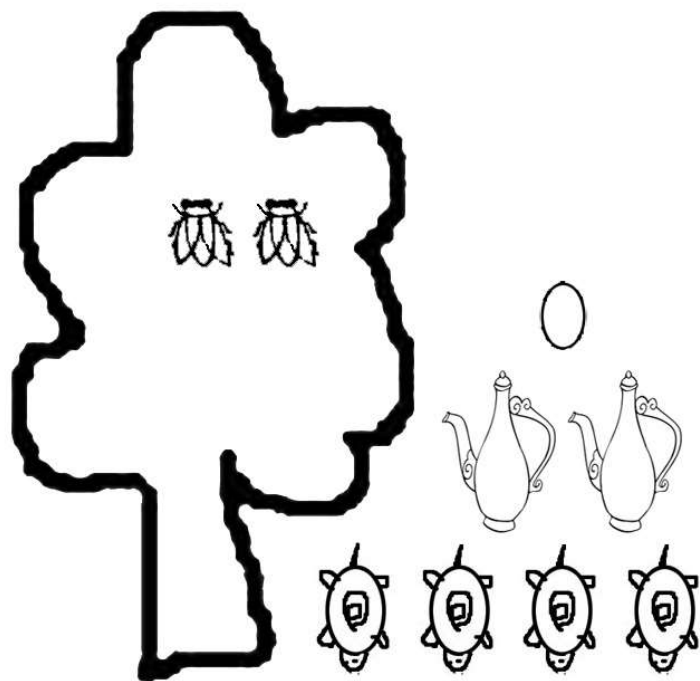




# 信息隐藏典型范例

## —— 隐密术（“藏”）

- 2、山西家书



银子 银子 有数

$$4 \times 8 = 32$$

$$2 \times 9 = 18$$

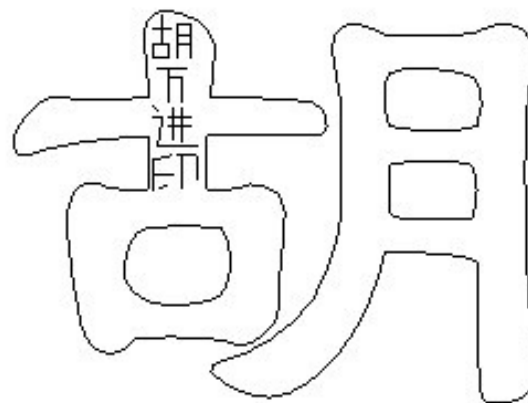
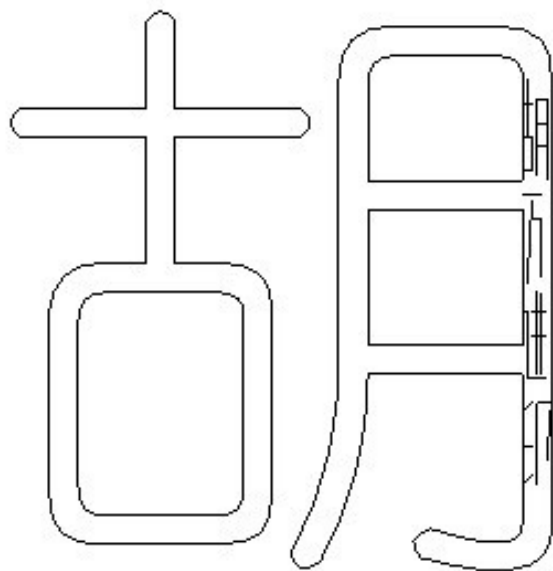
$$32 + 18 = 50 \bigcirc$$



# 信息隐藏典型范例

## —— 隐密术（“藏”）

- 3、word 的字中有字



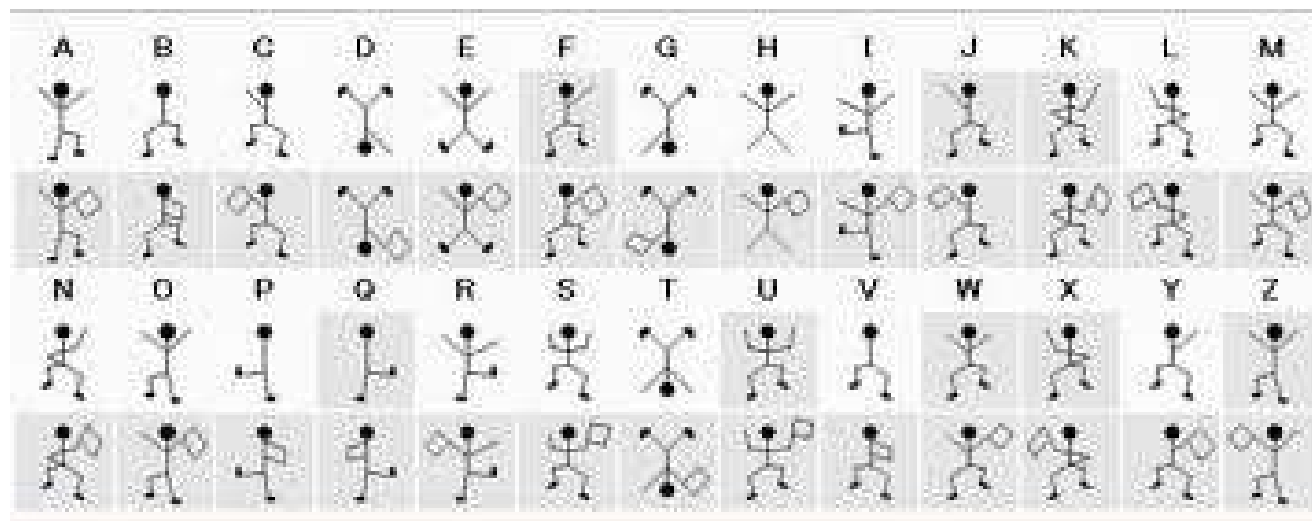


# 信息隐藏典型范例

## — 隐密术 ( “变” )

### ● 1、跳舞的小人

福尔摩斯探案集第 2 集





# 信息隐藏典型范例

## —— 隐密术（“变”）

- 2、二战中土著语与方言讲课

好莱坞影片《风语者》，纳瓦霍密码；

卧春

暗梅幽闻花

卧枝伤痕底

遥闻卧似水

易透大春绿

岸似绿

岸似透绿

岸似透黛绿



我蠢

俺没有文化

我智商很低

要问我是谁

一头大蠢驴

俺是驴

俺是头驴

俺是头呆驴

# 信息隐藏典型案例

## — 圈子里需要认识的几个人

- 1、Lena—国际标准测试图







# 信息隐藏典型案例

## — 圈子里需要认识的几个人

### ● 2、Jessica Fridrich

是世界上最快的、使用最广泛的  
魔方解法的发明人。她的方法是  
基于层先方法的，使用量最小的



2023/6/6

#### Jessica Fridrich

Professor

SUNY Binghamton

Department of Electrical and Computer Engineering

T. J. Watson School of Applied Science and Engineering

Binghamton, NY 13902-6000

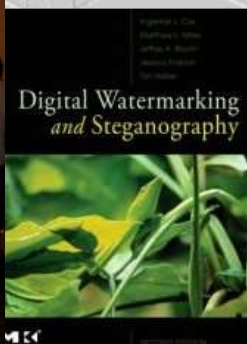
Phone: (607) 777-6177, Fax: (607) 777-4464

URL: <http://www.ws.binghamton.edu/fridrich>

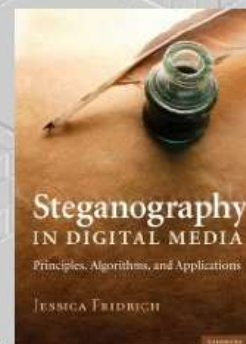
E-MAIL: [fridrich@binghamton.edu](mailto:fridrich@binghamton.edu)

#### Research

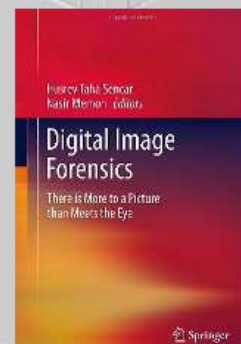
I specialize in data hiding applications in digital imagery, including steganography and steganalysis, forensic analysis of digital images (sensor fingerprints), and advanced image processing. My earlier research interests were in chaotic nonlinear dynamical systems and dynamical systems modeling and encryption. I work with a team of my graduate students at Binghamton University. Our research is mostly funded by the AFOSR, NSF, and the AFRL.



Errata



Errata



# 信息隐藏典型案例

## — 圈子里需要认识的几个人

### ● 3、施云庆





# 信息隐藏典型范例

## — 圈子里需要认识的几个人

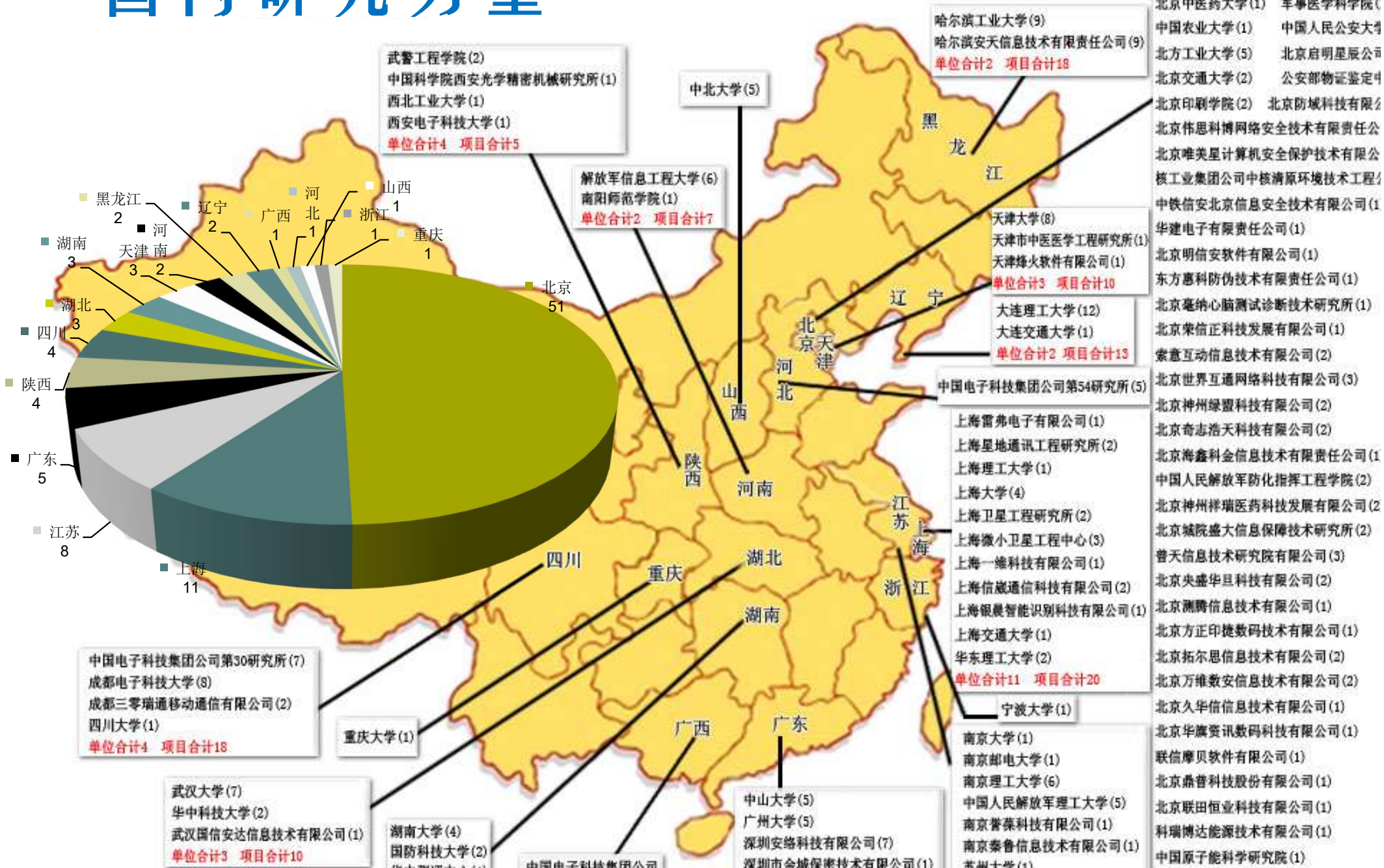
### ● 4、郭云彪

北京电子技术应用研究所所长，全国信息隐藏暨多媒体信息安全大会程序委员会主席





## 国内研究力量







# 学术制高点

## 全国信息隐藏暨多媒体信息安全学术大会

- 99年始，电子学会通信学分会的重要学术会议，共举办十二届
- 由何德全，周仲义，蔡吉人三位院士倡导，一所(北京电子技术应用研究所)牵头
- 全国范围，年投稿单位达70余家，年参会单位达80余家，年参会人员近300名





# 需掌握的内容

- 什么是信息隐藏
- 什么是数字水印
- 什么是隐密术
- 数字水印与隐密术的区别与联系
- 信息隐藏与密码学的区别与联系





欢迎大家继续讨论！

