

01

第1章 概论



1.1 什么是信息隐藏



1.2 信息隐藏的历史回顾



1.3 发展现状和分类



1.4 信息隐藏算法性能指标



1.5 可视密码学与信息分存



1.6 叠像术



发展现状和分类



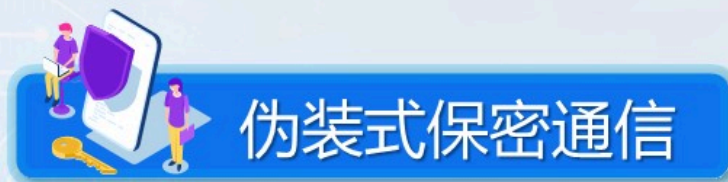
1.3.1 信息隐藏技术的发展现状



1.3.2 伪装式保密通信



1.3.3 数字水印



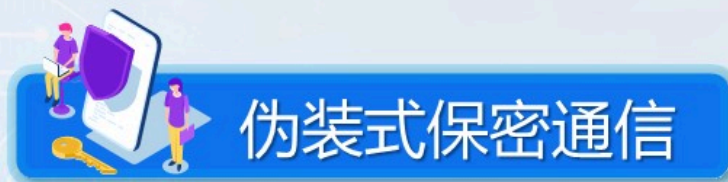
伪装式保密通信

伪装式保密通信，是古典隐写术与现代技术的直接结合。

越来越多的多媒体信息可以通过网络传输。

越来越多的机密信息需要保密。

信息的安全传输除了可以依靠传统的密码技术，还可以使用信息隐藏技术，更好地提高其安全性。

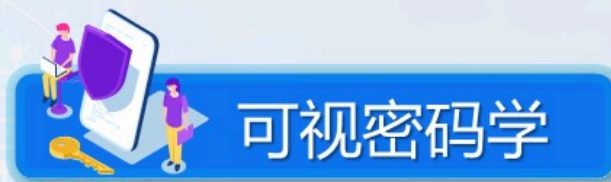


伪装式保密通信

隐藏载体：利用多媒体信息作为隐藏载体。

人的感觉系统对图像、视频、声音等的感知的精确度远远低于计算机的精确度，利用这一特点，发展出了伪装式保密通信这一研究领域。

目前这一研究领域主要研究图像、视频、声音以及文本中的隐藏信息。



可视密码学

1994年，M.Naor
和A.Shamir提出。

其思想是把要隐藏的密钥
信息通过算法隐藏到两个或多
个子密钥图片中，每一张图片
上都有随机分布的黑点和白点，
把所有的图片叠加在一起，则
能恢复出原有的信息。

主要特点：恢
复秘密图像时不需
要任何复杂的计算，
直接以人的视觉系
统就可以将秘密图
像辨识出来。

可视密码学举例1

密钥 (Secret image):

南开

子密钥1 (The first share):



子密钥2 (The second share):



解密结果 (Reconstructed image):

南开




可视密码的原理

原始文字是白底黑字，视为一个二值图像









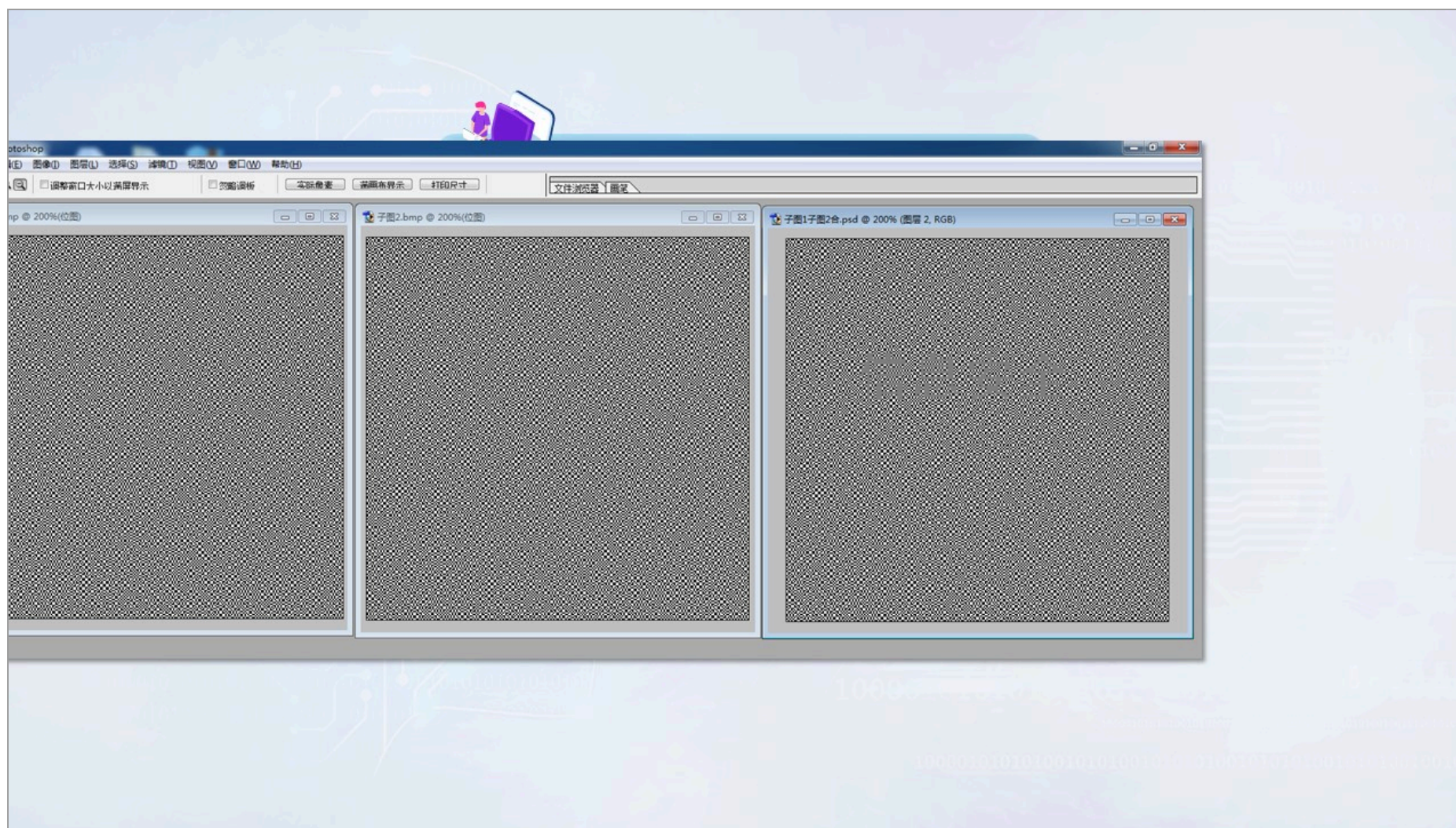
把每一个像素扩展为 2×2 （或 $n \times n$ ）的图块






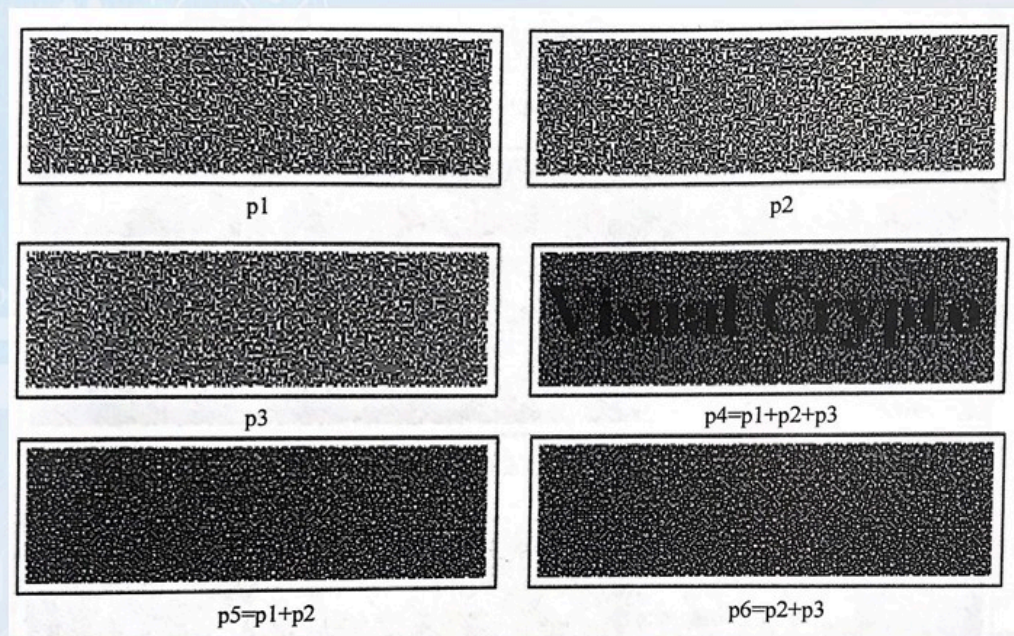
可视密码的原理

秘密图像的像素	黑	白
伪装图像1的像素 (部分)		
伪装图像2的像素 (部分)		
叠加后的像素		



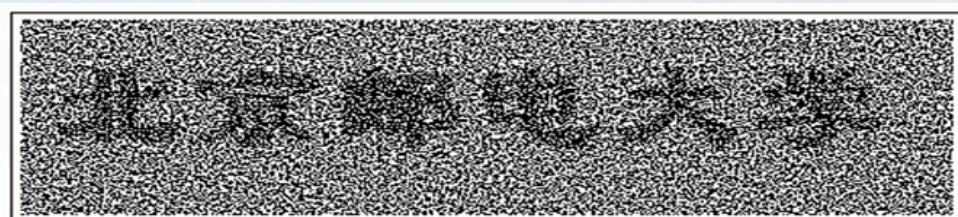


可视密码学举例3

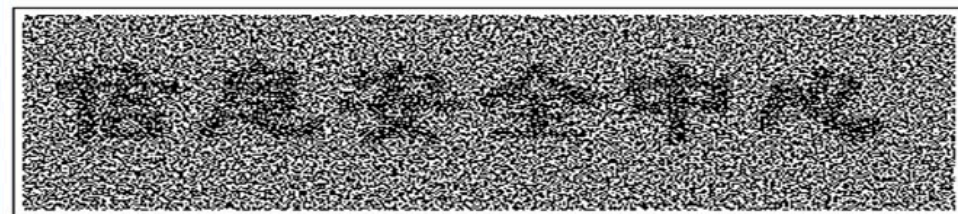




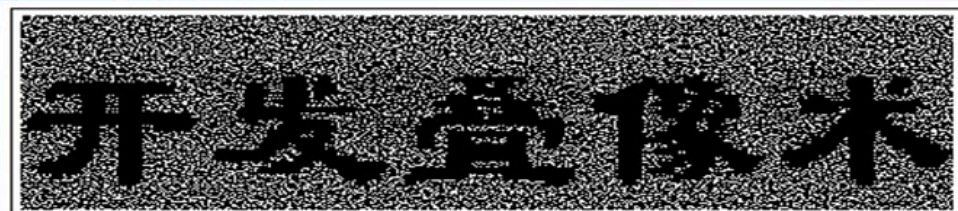
- ✓ 产生的每一张图像不再是随机噪声图像，而是正常人能看懂的图像：图像上有不同的文字或图画。
- ✓ 只要将一定数量的图像叠加在一起，则原来每一张图像上的内容都将消失，而被隐藏的秘密内容出现。
- ✓ 单个图像无论是失窃还是被泄露，都不会给信息的安全带来灾难性的破坏。
- ✓ 由于每一张图像的“可读性”，使其达到了更好的伪装效果。
- ✓ 从理论上可以证明该技术是不可破译的。



p1 “北京邮电大学”



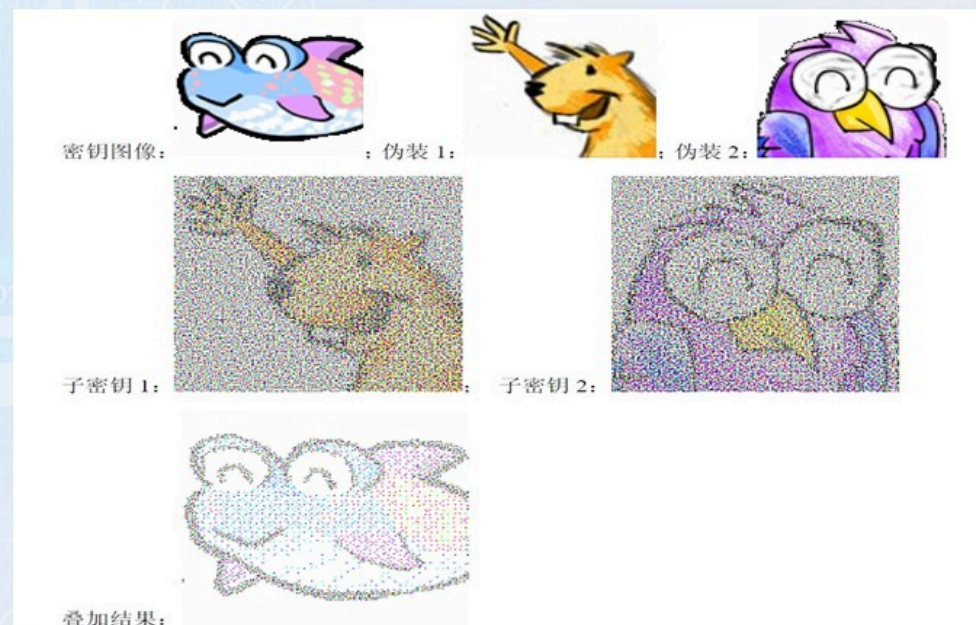
p2 “信息安全中心”



$p3=p1+p2$ “开发叠像术”

图2 改进后的叠像术

彩色叠像术





一级标题:



信息安全斗争的**技术**和**艺术**

思源黑体 CN Heavy

二级标题:

5

信息隐藏技术和密码技术的区别

思源黑体 CN Heavy

数字 英文

Times New Roman (正文)



MFLIHEI_NONCOMMERCIAL-REGULAR.OTF



SOURCEHANSANSNCN-HEAVY.OTF



SOURCEHANSANSNCN-NORMAL.OTF



times.ttf

PS:内容可编辑范围
在异形框内