# 信息隐藏实验

**【实验目的】**

(1)了解数字水印和信息隐藏技术；

(2)利用相关软件给图片添加数字水印。

**【实验仪器】**

一台安装Photoshop3.0版本的安装Windows 2000系统计算机。

**【实验原理】**

**3.1**信息隐藏技术概述

　　信息隐藏技术与传统密码学不同的是，它利用多媒体信息普遍存在的冗余性，将秘密信息隐藏在多媒体信息中而不引起多媒体信息物理外观的显著变化，使得人们觉察不到它的存在，即使截获者知道秘密信息的存在，未经授权也难以将其提取出来，从而保证了秘密信息的机密性和安全性。

(1)信息隐藏技术的一些典型算法

　　信息隐藏技术的基本应用领域是版权保护（Copyright Protection），隐藏标识（Hidden Annotation）、认证（Authentication）和安全不可见通信（Secure and Invisible Communication）。当采用信息隐藏技术作为鲁棒的隐蔽通信时，在国防和情报部门得到广泛的应用，在这些部门中传统的数据隐藏技术或密写术（Steganography）已得到了数个世纪的应用，信息隐藏技术在此领域的应用也将占有一席之地。

关于信息隐藏技术的算法有很多，但按照隐秘空间来划分，主要有空间域信

息隐藏和变换域信息隐藏。

●空间域信息隐藏技术

●变换域信息隐藏技术

(2)信息隐藏系统分类

　　信息隐藏技术与传统的密码学相结合，不仅可以保持信息隐藏技术原有的优势，还可以进一步提高信息隐藏系统的机密性与安全性。在学术界，信息隐藏系统从与密码学结合的角度上看可以分为三种：无密钥信息隐藏系统、私钥信息隐藏系统和公钥信息隐藏系统。

● 无密钥信息隐藏系统

● 私钥信息隐藏系统

● 公钥信息隐藏系统

**3.2图像信息隐藏技术**

（1）伪随机序列与信息嵌入位的选择

　　前面我们讨论了对伪随机序列进行了概述，接着我们讨论伪随机系列在信息隐藏技术中的一个应用方面——信息嵌入位的选择。之所以要讨论这个问题，是因为我们发现随机序列的知识与具体的隐藏算法有着密切的联系，甚至决定着隐藏效果的好坏。如对于盲嵌入水印，其水印本身就是一个随机序列构成的信号，水印的区别完全由序列种子（Seed）决定。在不知道真实Seed的情况下检测秘密信息就好比在不知道密钥的情况下试探性地解密文件一样，成功的几率是可以忽略的。

一个品质良好的随机序列可以在信息安全的诸多领域发挥不可估量的作用。在信息隐藏中，最直接的一个例子就是利用随机序列控制秘密信息的嵌入规则。一个没有随机序列控制的隐藏算法是没有安全性可言的。图13-1是在顺序选取像素点的情况下利用LSB空间域算法得到的效果（为了效果明显，将原始图像的第6比特位置为0），仔细观察不难发现在图像中隐藏有信息。图13-1所示是由于秘密信息很多短，只占用了载体图像的一部分像素位而造成的。出现这样的效果基本上可以认为实验是失败的。解决这一问题的方法就是使用为随机序列将秘密信息打乱嵌入到图像中，使其不至于在一个局部形成明显的分界线，如图13-2所示。  


a 原图像 b 嵌入秘密信息后有明显分界线的图像

图13-1 顺序选择嵌入位



a.原图像 b.嵌入秘密信息后无分界线的图像

图13-2 伪随机序列选择嵌入位

　　Krckhoffs原则是信息安全领域里的一个基本原则，即系统的安全仅仅依赖于密钥而不是安全算法。同样还是举LSB算法的例子，如果将信息顺序地隐藏到图像中，那么将不存在密钥的应用空间。在算法公开的要求下，任何一个人都可以逐一将秘密信息提取，信息隐藏将毫无意义。

　　所以我们使用随机序列控制信息嵌入位。在整幅图像中随机选择嵌入位将秘密信息嵌入，而随机序列的种子就可以视为密钥。

（2）对称密钥系统

　　对称密钥系统是密码学中常见的一种加密系统，有时又叫传统密钥系统，就是加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加密和解密的密钥是相同的。这些算法也叫秘密密钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄漏密钥就意味着任何人都能对消息进行加密解密。只要通信需要保密，密钥就必须保密。

常用的采用对称密码术的加密方案有5个组成部分：

▲ 明文：原始信息。

▲ 加密算法：以密钥为参数，对明文进行多种置换和转换的规则和步骤，变换结果为密文。

▲ 密钥：加密与解密算法的参数，直接影响对明文进行变换的结果。

▲ 密文：对明文进行变换的结果。

▲ 解密算法：加密算法的逆变换，以密文为输入、密钥为参数，变换结果为明文。

**3.3数字水印技术**

　　数字水印（Digital Watermarking）技术是将一些标识信息(即数字水印)直接嵌入数字载体(包括多媒体、文档、软件等)当中，但不影响原载体的使用价值，也不容易被人的知觉系统(如视觉或听觉系统)觉察或注意到。通过这些隐藏在载体中的信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印是信息隐藏技术的一个重要研究方向。

**【实验内容及步骤】**

 1. 打开Photoshop软件，点击【文件】菜单下的【打开】，打开预选图，如图13-3所示：



图13-3 待加水印样本图片

 2. 点击【文件】菜单下的【新建】，修改数值完成后，点击“确定”，如图13-4所示。



图13-4 所加水印图片的各项值

 3. 使用文字工具，在对话框中打入文字，进行方向调整选择合适的方向，如图13-5所示。

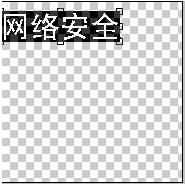


图12-5 水印图片

 4. 单击【选择】菜单下的【全选】，然后选择【编辑】菜单下的【定义图案】，在此使用默认图案，至此水印定义完成，如图13-6所示。

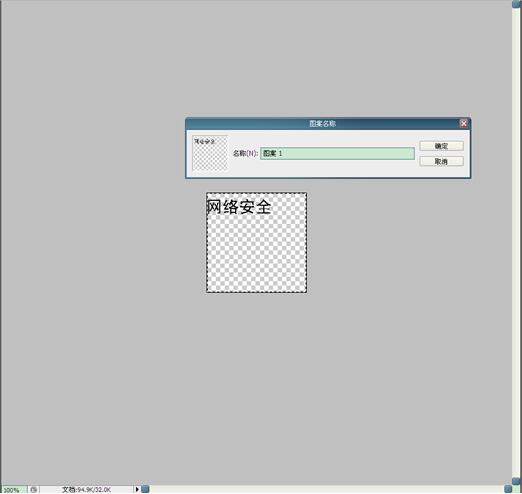


图13-6 定义水印图片

 5. 打开原图，点击【图层】菜单下的【新建】->【图层】，创建一个新的图层，之后，执行【编辑】->【填充】，选择我们刚刚建立的图案，如下图所示：



 6. 点击确定，就添加了水印，如图13-7所示。



图13-8 添加好的水印图片

【实验报告】

利用软件Photoshop CS3对JPG格式（或JPEG格式）的图像添加水印，掌握增加水印的方法。

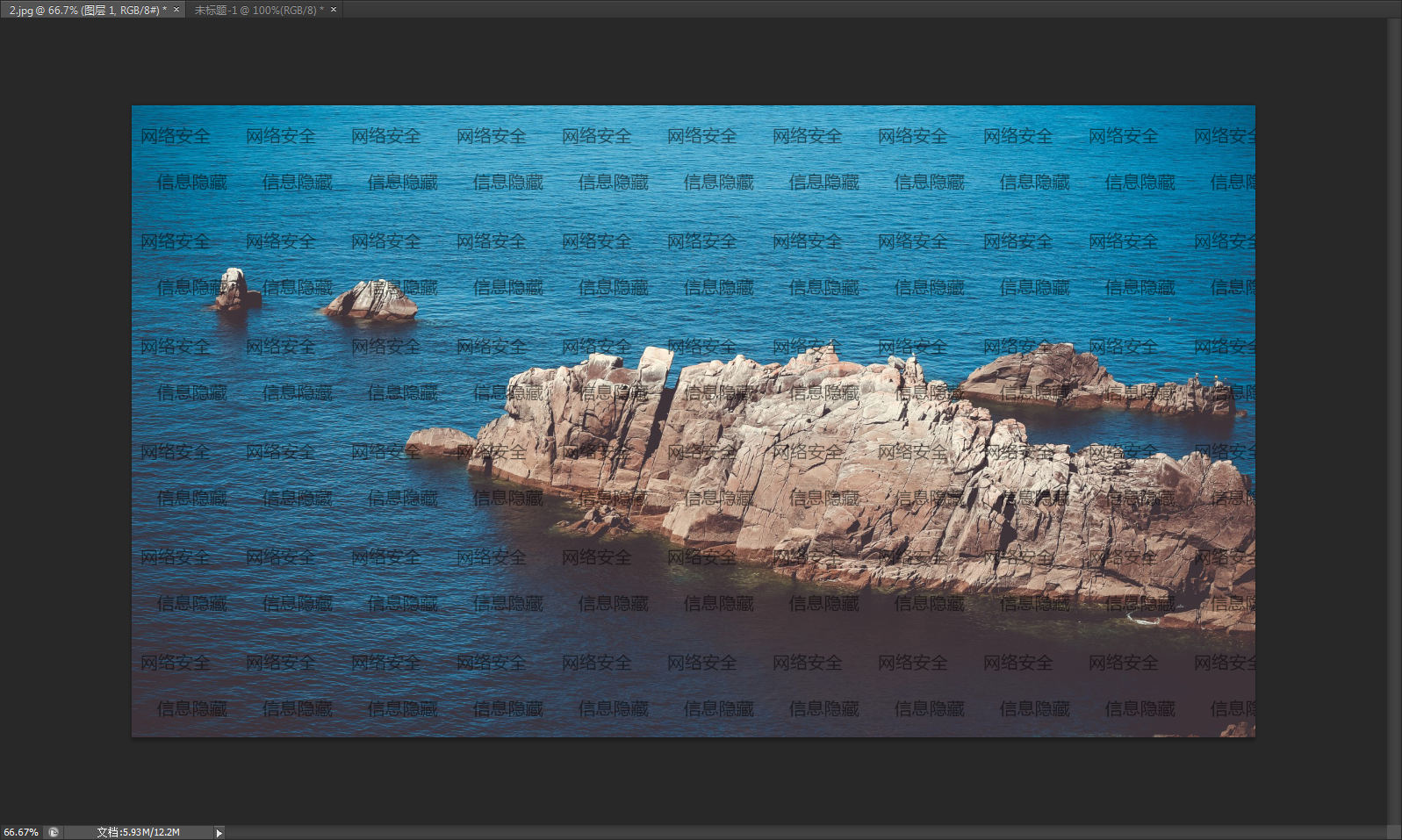


图13-9 实验结果