**《网络空间安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | |  | | **年级** | | **2021级** |
| **学号** | |  | | **专业、班级** | | **计算机科学与技术01班** |
| **实验名称** | **实验二 信息隐藏实验** | | | | | |
| **实验时间** | **2024.4.13** | | **实验地点** | | **DS3304** | |
| **实验成绩** |  | | **实验性质** | | **□验证性 □设计性 □综合性** | |
| 教师评价：  □算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  评语：  评价教师签名（电子签名）： | | | | | | |
| 一、实验目的  1.学习并掌握图像信息隐藏的基本原理和方法  2.实现基于LSB的信息隐藏和提取算法 | | | | | | |
| 二、实验项目内容  1.使用LSB算法在图片中隐藏如下信息：CQUWATERMASKEXP  2.从被隐藏数据的图片中解析出如上信息，建议使用Matlab  3.在实际应用中，隐藏信息量通常是不可预知的，同时，攻击者也很容易从最低位像素提取到隐藏信息并对此进行密文分析。另一方面，如何确保信息来源于正确的发送者？针对这些问题，请设计完整的方案。 | | | | | | |
| 三、实验设计  **1.LSB算法原理**  任何多媒体信息在数字化时都会产生物理随机噪声，而人的感官系统对这些随机噪声并不敏感，通过使用秘密信息比特替换随机噪声，从而实现信息隐藏。在图像中，高位平面对图像感官质量起主要作用，去除图像最低几个位平面并不会造成画面质量的下降。利用这个原理可用秘密信息（或称水印信息）替代载体图像低位平面以实现信息嵌入。  LSB算法选用最低位平面来嵌入信息，最低位平面对图像的视觉效果影响最轻微，因此在视觉上很难察觉。作为大数据量的信息隐藏方法，LSB在保密通信中仍占据相当重要的地位。  PNG图片中的图像像素一般是由RGB三原色组成，每一种颜色占用8位，取值范围为0x00~0xFF，如图所示。    当仅仅更改颜色分量的最低位时，人类的眼睛不能区分这前后的变化，LSB就是在该位置存放隐藏信息，如图所示。  LSB  **2.LSB算法加解密主要步骤**  **加密：**1.读入图片  2.准备待隐藏的信息，将其转换为二进制  3.遍历图像，对像素的最低位置0，同时在该比特位写入1位二进制表示隐藏的信息  **解密：**1.预知隐藏信息量（等同于key）  2.提取出像素的最低1bit，组合成连续bit数据，转换为ASCII码对比是否与隐藏信息一致  **3.基于信息加密和身份验证的信息隐藏**  将隐藏信息量即隐藏信息的长度同隐藏信息一并隐藏到图片中，在进行信息提取时，先提取出前32位的二进制信息，即可实现隐藏信息量的传递。  通过RSA算法可以使用公钥加密技术来确保只有私钥持有者可以解密消息，同时使用数字签名来验证消息的完整性和来源。  基本流程：  ·密钥生成：  A 和 B 都会生成一对公钥和私钥。A 会将其公钥分享给 B，B 也会将其公钥分享给 A。  ·加密：  A 想要发送消息给 B 时，首先使用 B 的公钥对消息进行加密。这确保只有持有 B 的私钥的人才能解密该消息。  ·数字签名：  A 使用自己的私钥对消息进行签名。这个签名是基于消息内容的哈希值和 A 的私钥生成的。A 将消息和签名一起发送给 B。  ·验证：  B 收到消息后，首先使用 A 的公钥验证签名的有效性。如果验证成功，则表示消息确实是由 A 发送的，并且没有被篡改。然后，B 使用自己的私钥解密消息，以获取原始的明文信息。  通过这种方式，B 能够确信消息的来源是 A，因为只有 A 才能生成有效的签名。同时，由于消息是使用 B 的公钥加密的，其他人无法在传输过程中窃听或篡改消息。 | | | | | | |
| 四、实验过程或算法  **1.LSB加密**  函数hide\_message实现了信息的隐藏，接受图像路径和需要隐藏的信息作为输入，返回隐藏了信息的图像。  首先，打开原始图像，并将要隐藏的消息转化为二进制字符串。  接着，将隐藏信息长度即隐藏信息量转化为32位二进制字符串，并与其隐藏消息本身连接。  最后，遍历图像的每个像素，并将消息的二进制位逐个嵌入到像素的最低位中，直到所有信息都被隐藏完毕。    **2.LSB解密**  函数extract\_message实现了从包含隐藏信息的图像中提取信息，接受加密图像的路径作为输入，并返回提取出的信息。  首先，读取加密后的图像，并提取出32位的二进制信息隐藏量。  接着，根据信息隐藏量提取出隐藏的二进制信息，并将其转换回字符串。    **3.基于RSA算法的LSB加密解密**  **·RSA加密和签名**  使用接收方（B）的公钥对信息进行加密，以确保只有拥有私钥的接收方才能解密。  使用发送方（A）的私钥对加密后的数据进行签名，以确保接收方可以验证发送方的身份和信息的完整性。    **·RSA解密和验证**  使用接收方（B）的私钥对加密后的数据进行解密，获取原始数据。  使用发送方（A）的公钥对签名进行验证，以确认签名的有效性和信息的完整性。    **·LSB算法信息隐藏**  首先将待隐藏的信息（即加密后的数据和签名）转换为二进制字符串。接着将信息长度编码为32位二进制，作为前缀放置在加密后的数据前面，用于提取时确定隐藏信息的长度。然后将加密后的数据和签名按位嵌入到图像的像素中的最低有效位中。最后返回隐藏信息后的图像。    **·LSB算法信息提取**  首先从图像中提取加密后的数据长度和签名长度，以确定待提取的隐藏信息的长度。然后根据长度信息，提取加密后的数据和签名的二进制字符串。最后将二进制字符串转换为字节对象，即加密后的数据和签名。 | | | | | | |
| 五、实验过程中遇到的问题及解决情况  **1.问题：**jpg格式图片无法进行信息隐藏和提取  **解决方案：**jpg图像默认被计算机压缩了，损失了大量隐藏信息，将jpg格式转化为png格式即可实现信息隐藏和提取。  **2.问题：**解密函数无法确定信息隐藏量的大小，导致提取过多无效信息  **解决方案：**将隐藏信息量即隐藏信息的长度同隐藏信息一并隐藏到图片中，在进行信息提取时，先提取出前32位的二进制信息隐藏量，根据信息隐藏量再继续提取后面真正的隐藏信息  **3.问题：**无法对隐藏信息进行加密和签名  解决方案：输入的隐藏信息类型为字符串，但是在RSA加密和签名中要求对字节进行操作，所以在将隐藏信息传入encrypt\_and\_sign\_message函数前需要将隐藏信息转为字节类型再传入  **4.问题：**在RSA算法中，无法向解密函数传输加密数据和签名  **解决方案：**返回的加密数据和签名都是字节类型，将加密数据和签名转化为二进制字符串，然后通过LSB算法隐藏到图片中进行传递数据，解密函数通过读取加密数据和签名的长度，然后提取出对应长度的加密数据和签名二进制串，最后再转化回字节类型 | | | | | | |
| 六、实验结果及分析和（或）源程序调试过程  **1.LSB隐藏和提取信息**    选择需要进行信息隐藏加密的图片CQUlibrary.png，然后输入需要隐藏的信息CQUWATERMASKEXP，接着调用hide\_message函数实现LSB算法对图片进行信息隐藏，最后返回隐藏信息加密图片CQUlibrary\_hidden.png。    信息隐藏前的照片CQUlibrary.png    信息隐藏后的照片CQUlibrary\_hidden.png  根据上面两张LSB算法信息隐藏前后的照片，照片前后的变化在人眼视觉上很难察觉，成功实现了在图像中隐藏信息。    选择需要解密的图片CQUlibrary\_hidden.png，接着调用extract\_message函数实现LSB算法从隐藏信息的图像中提取信息，最后返回提取出“CQUWATERMASKEXP”隐藏信息。  **2. 基于RSA算法的LSB加密解密**    选择需要进行信息隐藏加密的图片CQUlibrary.png，然后输入需要隐藏的信息CQUWATERMASKEXP，并将隐藏信息从字符串类型转化为字节类型，接着调用encrypt\_and\_sign\_message函数对隐藏信息进行加密和签名，接着调用hide\_message函数实现LSB算法对图片进行加密和签名信息的隐藏，最后返回加密图片CQUlibrary\_hidden.png。    信息隐藏前的照片CQUlibrary.png    信息隐藏后的照片CQUlibrary\_hidden.png  根据上面两张基于RSA算法的LSB加密算法信息隐藏前后的照片，照片前后的变化在人眼视觉上很难察觉，成功实现了在图像中隐藏信息。    选择需要解密的图片CQUlibrary\_hidden.png，接着调用extract\_message函数实现LSB算法从隐藏信息的图像中提取加密和签名信息，然后调用verify\_and\_decrypt\_message函数对从图片中提取出来的加密和签名进行验证，验证通过后再进行解密，最后返回提取出“CQUWATERMASKEXP”隐藏信息的字节类型。 | | | | | | |