林丕源　肖德琴　刘才兴　(广州 华南农业大学计算机科学系　510642)

Secret Transmission of Business Documents by the PKC and Images the Hiding Technique

利用公开密码体制和图像隐藏技术秘密传输商务文档

摘要：信息隐藏将数据隐藏在某种载体里，信息加密将明文变成密文。为提高商务文档传输的安全性，本文结合加密技术和信息隐藏，提出将商务文档先用公开密码体制的公开密钥加密，再将密文隐藏于24位BMP图像中进行传输，实现了对商务文档传输的双重保护。

关键词：信息安全　公开密码体制　信息隐藏　商务文档

1　引言

为确保商务文档在Internet安全传输，需要采用加密技术，最常见的方法是对商务文档加密后传输密文。为了进一步提高商务文档传输的安全性，可以将加密技术和隐藏结合使用，为此我们提出：将商务文档加密后再对密文进行信息隐藏处理——将商务文档密文的隐藏于不容易引起怀疑的或具有伪装性的其他载体，而在Internet上传输载体。

根据以上思想，我们设计并实现了用公开密钥加密商务文档并用BMP图像作为载体进行密文隐藏和传输的方案。本文先介绍该方案中利用BMP图像进行隐藏和提取密文的原理与方法，然后阐述公开密钥密码体制的加密与解密原理，最后完整给出利用公开密码体制和图像隐藏技术秘密传输商务文档的流程。

2　利用BMP图像进行隐藏和提取密文的原理与方法

信息隐藏实现将一个消息(被隐藏消息或秘密消息)隐藏在另一个消息(载体或遮掩消息)中，在基本不改变载体的外部特征(及使用价值)的情况下，我们的感觉器官察觉不到载体外部的变化，而让被隐藏消息消失得“无影无踪”。

图像文件一般比较大，通常可作为隐藏信息的载体。本案实现的是：让被隐藏消息——商务文档明文经加密得到的密文——隐藏在未压缩的24位BMP图像文件载体中。

2.1 基本原理

BMP图像文件[1]包括每个像素为1位、4位、8位和24位的图像。其中，24位图像是直接彩色，在位图文件头和位图信息头后直接是位图阵列数据。

选用24位BMP图像作为隐藏密文的载体，可以轻易地把密文信息存储到位图阵列信息中，因为从24位BMP图像文件的第55个字节起，每3个字节为一组记录1个像素的红(R)、绿(G)和蓝(B)三种颜色的亮度分量。于是，可以使用每个字节的最不重要位(即最低位)来隐藏密文，这

可以保证对作为载体的BMP图像的外部特征不会发生大的变化，人们在浏览图像时感觉不到有变化。可以计算，使用这种方法隐藏信息的效率近于12.5%（即3个字节的24位隐藏3位）（还需排除位图文件头和位图信息的头部共54字节）。一个长度为L字节的24位BMP图像可以隐藏信息的最大字节数是(L-54)/8字节。

要提高24位BMP图像隐藏信息的效率，不能简单地将每个像素3个字节的RGB亮度分量的每个字节的最低2位替换为要隐藏的密文，这样在浏览图像时人眼能感觉出外部特征的细微变化。但是，考虑到人眼对红绿蓝的感觉是不同的，根据亮度公式[2]

$$Y = 0.3R + 0.59G + 0.11B$$

以及人眼视锥细胞对颜色敏感度的理论，人眼对绿色最敏感，对红色次之，而对蓝色最不敏感。因此，可以用密文替换每个像素RGB亮度分量不同的最低位数。实验[3]证明，红色分量改变最低2位，绿色分量改变最低1位，蓝色分量改变最低3位，都不会让图像产生人眼容易察觉的变化。按照这种方法隐藏信息的效率提高到近于25%（即24位隐藏6位）（还需排除位图文件头和位图信息头部共54字节）。一个长度为L字节的24位BMP图像可以隐藏信息的最大字节数是(L-54)/4字节。

设密文文件的长度为N字节，再考虑存储该数字N要使用3个字节，要选取一个字节数为L的24位BMP图像来隐藏密文，则需要满足下面的关系：

$$L \geqslant 4*(N+3)+54$$

2.2 隐藏密文过程

(1) 根据要隐藏的密文文件的长度N，选择一个长度不小于4*(N+3)+54字节的24位BMP图像；

(2) 将数字N转化为24位二进制数bi：b_i=0或1，i=0, 1, 2, ...23，$N=\sum_{i=0}^{23}2^i b_i$

(3) 对b_i(i=23, 22, 21, ...0)进行隐藏。从BMP图像文件第55字节起连续读出12字节，用bi(i=23, 22, 21, ...0)分别替换这12个字节的低位：第1字节的第1位、第0位、第2字节的第0位、第3字节的第2位、第1位、第0位、第4字节的第1位、第0位、第5字节的第0位、第6字节的第2位、第1位、第0位、第7字节的第1位、第0位、第8字节的第0位、第9字节的第2位、第1位、第0位、第10字节的第1位、第0位、第11字节的第0位、第12字节的第2位、第1位、第0位。

这12个字节低位字节替换后，回写到BMP图像文件中。

(4) 隐藏密文文件具体内容。从第67字节起按12字节一组（最后一组不够时可少于12字节）依次读出BMP图像文件的各字节，同时从头开始按3字节一组（最后一组不够时可少于3字节）依次读出密文文件字节到A、B、C。每读一组BMP图像文件的12字节和一组密文文件的3字节后，进行这样的替换：

BMP图像文件字节组的第1、4、7、10字节的最低2位（第1和0位）分别被A的第7和6位、A的第1和0位、B的第3和2位、C的第5和4位所替换；

BMP图像文件字节组的第2、5、8、11字节的最低1位（第0位）分别被密文文件字节组的A的第5位、B的第7位、B的第1位、C的第3位所替换；

BMP图像文件字节组的第3、6、9、12字节的最低3位（第2、1和0位）分别被密文文件字节组的A的第4和3及2位、B的第6和5及4位、B的第0位和C的7及6位、C的第2和1及0位所替换；

对每一组12个字节按上面方法替换完毕后，要将结果按原来的位置回写到BMP图像文件中。（说明，最后一组要特殊处理。）

2.3 提取密文过程

提取密文是按隐藏密文的逆过程来从隐藏有密文的24位BMP图像文件中抽取信息，并以字节为单位重新生成出密文文件。

(1) 提取密文文件长度。从BMP图像文件第55字节起连续读出12字节，根据第1字节的第1位、第0位、第2字节的第0位、第3字节的第2位、第1位、第0位……等规则计算出隐藏的密文文件的长度$N=\sum_{i=0}^{23}2^i b_i$

(2) 提取密文文件具体内容。根据密文文件的字节数N，从第67字节起按12字节一组（共有Int(N/3+2)个组，最后一组可能不足12个字节）依次读取隐藏有密文的BMP图像的字节，每读一组后按下述方法生成3个字节A、B和C：

A的第7和6位是BMP图像文件字节组的第1字节的第1和0位，A的第5位为第2字节的0位，A的第4、3和2位是第3字节的第2、1和0位，A的第1和0位是第4字节的第1和0位；

B的第7位是BMP图像文件字节组的第5字节的第0位，B的第6、5和4位为第6字节的第2、1和0位，B的第3和2位是第7字节的第1和0位，B的第1位是第8字节的第0位，B的第0位是第9字节的第2位；

C的第7和6位是BMP图像文件字节组的第9字节的第1和0位，C的第5和4位为第10字节的第1和0位，C的第3位是第11字节的第0位，C的第2、1和0位是第12字节的第2、1和0位；

对每一组12个字节按上面方法处理完毕形成字节A、B和C后，依次将A、B和C写入创建的密文文件中。

(说明，最后一组要特殊处理。)

经过以上处理，即得到密文文件。

3 公开密钥密码体制的加密与解密原理

加密技术是保证信息安全的最常用的手段。在传统加密技术中，消息发送者和消息接收者使用同一密钥。而在公开密钥加密技术中，加密密钥与解密密钥是不一样的，加密者可以将加密密

钥公开，成为公开密钥，而仍将解密密钥保密，作为秘密密钥。任何人如果想发送加密消息，都可以找到公开密钥，然而，其加密的消息却必须用加密者自己保留的秘密密钥才能解密，别人只知道公开密钥，因而无法阅读该消息。如果想向另一个人发送加密消息，则可以先去找他的公开密钥（既然是公开的，因而往往不用与他本人事先联系，甚至不必认识他），然后用此密钥加密，显然，除了他本人之外，别人是无法阅读他的加密消息。

公开密钥加密体制（PKC）通常都是基于一定的数学难题，如基于陷门背包加密法、基于离散对数的公钥体制、基于椭圆曲线的公钥体制、基于大素数的RSA公钥体制[4]。本文采用基于RSA的加密体制加密商务文档，然后将密文隐藏在BMP图像里进行传输，这样既达到一定的安全性，又具有相应的隐蔽性，很好地实现了商务文档的安全传输。以下是RSA加密算法的大致流程：

(1) 找出三个数：p、q、r，其中p和q是两个相异的质数，r是与(p-1)(q-1)互质的数。

(2) 找出e，使得 re ≡ 1 mod (p-1)(q-1)。这个e一定存在，因为r与(p-1)(q-1)互质，用辗转相除法就可以得到。

(3) 计算 n = pq。(n, e)作为公开密钥，(n, r)为私有密钥。

加密的过程是，若待加密信息为a，将其看成是一个大整数，假设a < n。如果a >= n，就将a表成s进位（s <= n，通常取 s = 2^t），则每一位数均小于n，然后分段编码。

(4) 计算c ≡ (a^e mod n, (0 <= c < n)。c就是编码后的信息。

解密的过程是，计算 m ≡ (c^r mod n, (0 <= c < pq)。可以证明m和a其实是相等的。

一般说来，许多数学中的函数都有“单向性”，这就是说，有许多运算本身并不难，但如果想把它作逆运算就很难。从原理上讲，RSA算法是利用了这样单向性。对于RSA来说，用公开密钥加密后，如果想再通过公开密钥解密是很困难的，因为数学上认为对足够大的n的因式分解是很困难的。

RSA的应用非常广泛，RSA方法既可用于保密，也能用于签名和认证，目前已经广泛应用于各种产品、平台等软件上。许多流行的操作系统上如微软、Apple、Sun和Novell都在其产品上融入了RSA。在硬件上，如安全电话、以太网卡和智能卡都使用了RSA技术。而且几乎所有Internet安全协议如S/MIME，SSL和S/WAN都引入了RSA加密方法。

4 利用公开密码体制和图像隐藏技术秘密传输商务文档的流程

我们提出的利用公开密码体制和图像隐藏技术秘密传输商务文档的流程，如图1所示。这里，我们选择的公开密码体制为RSA，隐藏密文的载体为24位BMP图像文件。

(1) 发送方：先利用RSA算法以公钥对商务文档加密生成密文文件，再利用隐藏技术将密文文件隐藏到BMP图像文件，发送到Internet上的是隐藏有密文文件的BMP图像文件。

(2) 接收方：从Internet上接收到的是隐藏有密文文件的BMP图像文件，接收后先从BMP图像文件中提取出密文文件，再利用RSA算法以私钥将密文文件解密，还原为商务文档的原文。在正常情况下，如果不对商务文档原文加密，网络黑客在截获文档后就可能得知文档的内容。因此，需要通过加密的方法来保护商务文档。为了迷惑网络黑客，我们又将加密得到的密文进行隐藏处理，以使他们失去截获图像文件的兴趣。因为从图像外观上，他们不容易注意到其中包含有意义的信息。以上两点相结合，就实现了对商务文档的双重保护。

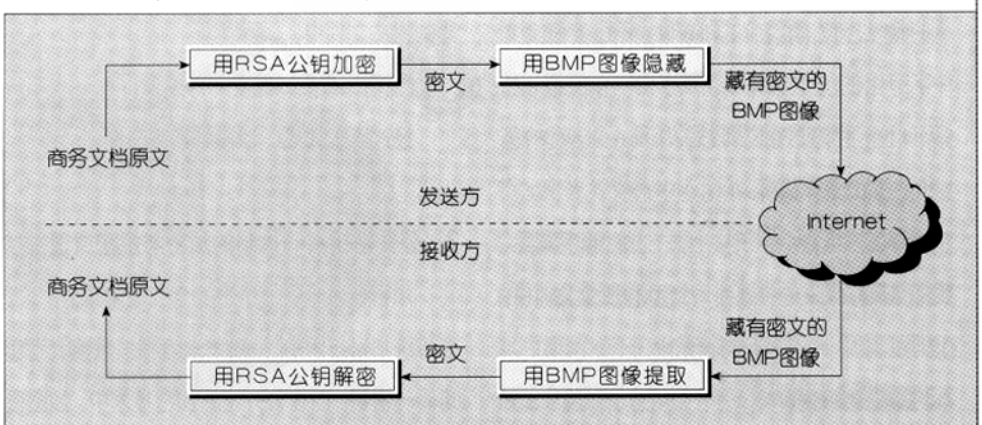

图1

5 结束语

本文的方案具有良好的应用前景，这是因为BMP图像文件获取容易，作为隐藏载体不容易引起怀疑。而使用公开密码体制加密后，用密文文件取代原商务文档，进一步提高了信息传输的安全性，实现了对被传输文档的双重保护。

在实现上，本文中仅应用了RSA的保密功能。再进一步，也可以对要传输的商务进行先签名再加密，然后隐藏发送出去，这样处理过后的商务文档既具有隐蔽性、难破解，还可以对发送者进行认证以防假冒。

参考文献

1 候阳，微机图形文件格式集粹，北京 学苑出版社，1993。

2 钟玉琢、冼伟铨、沈红，多媒体技术基础及应用，北京清华大学出版社，2000。

3 周瑞辉、荆继武，利用BMP图像文件进行秘密存储，计算机应用，2001, 21(5)。

4 冯登国、裴定一，《密码学导引》，科学出版社，2000年。