

电子商务安全传输系统研究

徐少强, 凌 捷, 李红蕾

(广东工业大学 计算机学院, 广东 广州 510090)

摘要: 从电子商务信息的多样性出发, 采用密码机制和信息隐藏技术以及数字水印相结合的方法来实现商务信息的保密性、完整性、隐蔽性及对商务信息进行认证, 对于图像信息还能保护信息的版权。

关键词: 电子商务; 信息隐藏; 3DES; RSA; 数字水印

中图分类号: TP309.2

文献标识码: A

文章编号: 1007-7162(2005)01-0067-05

引言

一般情况下, 在网络上传输文件时, 通常使用密码技术对传输的文件进行加密, 再在网络上传输。但是, 对于电子商务信息, 若只使用密码机制则会不可避免的存在一些缺陷。因为电子商务信息不但包含文档类信息, 而且还包括图像等多媒体信息, 使用混合密码系统能够很安全的传输电子商务中的文档类信息, 但是, 由于对图像进行认证往往需容忍一定程度的失真, 而密码学中的认证方法(即数字签名)却不容许一个比特的改变, 所以应用密码系统不能满足对图像和多媒体信息的认证要求, 在电子商务的应用中, 还存在一个版权的保护问题, 应用密码系统也很难提供这种服务。但可采用另一种方法来对数字产品进行版权的保护及对图像的认证, 那就是采用数字水印技术。单用混合密码系统还存在其它一些缺陷, 例如, 由于加密后的信息看起来是一堆令人无法理解的乱码, 这会激发非法拦截者破解机密资料的动机。还有, 电子商务信息虽然经过了加密, 但窃听者能对加密信息进行信息量分析, 因为加密后的数据长度跟明文数据长度是一样的, 这样非法窃听者虽得不到任何关于电子商务消息结构的信息, 也不知道谁在跟谁通话, 但他能知道发送的消息多长, 哪天进行的通信等, 这样使得窃听者对信息进行流量分析成为可能。

为了加强电子商务系统的安全性、可靠性, 本文利用现有的密码技术以及信息隐藏等技术来构建一个安全性较高的电子商务信息传输系统。

1 数字水印技术

数字水印就是永久镶嵌在其他数据(载体)中具有可鉴别性的数字信号, 而且并不影响载体数据的可用性^[1]。数字水印是近年来出现的数字产品版权保护技术, 可以标识作者、所有者、发行者、使用者等, 并携带有版权保护信息和认证信息, 目的是鉴别出非法复制和盗用的数字产

收稿日期: 2004-03-01

作者简介: 徐少强(1979)男, 在读硕士研究生, 主要研究方向为网络安全。

品,作为密码学的加密或置乱技术的补充,保护数字产品的合法拷贝和传播。

由于在保护电子产品的版权及对图像进行鉴别所采用的数字水印是不同的,对于版权保护,需要具有很强的鲁棒性和安全性的数字水印;而对于图像的鉴别,即证明图像没被篡改过,需要的是当图像内容发生改变时,数字水印信息会发生相应的改变的特性。为同时满足这两方面的要求,必须在图像中同时嵌入两种水印(当然要保证两种水印的信息在该系统中的嵌入顺序),系统采用了下面两种数字水印技术。

1) 鲁棒水印:利用这种水印技术即可在多媒体内容的数据中嵌入创建者、所有者的标示,或者嵌入购买者的标示信息(即序列号)。这种水印除了要求在一般图像处理(如:滤波、加噪声、替换、压缩等)中生存外,还需能抵抗一些恶意攻击,具有很强的鲁棒性和安全性。其中的一个算法如 DCT 域图像水印技术^[2]。

2) 易损水印:这种水印同样是在内容数据中嵌入不可见的信息。由于当内容发生改变时,这些水印信息会发生相应的改变,因此可以用来鉴定原始数据是否被篡改。其中的一个算法如小波数字水印算法 SVD^[3]。

2 信息隐藏技术

为了进一步提高电子商务文档传输的安全性,可把加密技术和信息隐藏技术结合起来使用。信息隐藏利用人类感觉器官对数字信号的感觉冗余,将一个秘密消息秘密地隐藏在另一个非机密的文件内容(称为载体)之中,而由于隐藏技术并不改变载体消息的基本特征,使人无法看到或听到隐藏的数据,即隐藏了信息的存在,达到令人难以察觉的目的^[1]。为此,先采用加密技术对电子商务信息进行加密,然后再把加密后的密文隐藏于图像中,最后把图像发送出去,这样就能够把信息伪装隐藏于不容易引起怀疑的图像中,免于被拦截者发现而遭到攻击。无论传送多少秘密信息,由于隐藏于图像内,故传送的都是固定大小的图像信号,避免受到窃听者的流量分析。

信息隐藏的载体可以是任何一种数字媒体,如图像、声音、视频或一般的文档等等。本文采用 24 位 BMP 图像文件作为隐藏电子商务信息密文的载体。每一个 24 位 BMP 图像文件含有一个 BMP 文件头、一个点位图信息头以及位图阵列。这里就是把信息储存在位图阵列中,24 位 BMP 图像文件的位图阵列中每 3 个字节表示一个像素,这 3 个字节依次表示这个像素的红(R)、绿(G)、蓝(B)亮度分量。系统使用最不重要比特位(the Least Significant Bits,简称 LSB)方法,即将需要隐藏的信息直接按位替换对图像影响最小的比特位,这样既隐藏了秘密消息,又不会使载体的外部特征发生大的变化。根据亮度公式: $I = 0.30R + 0.59G + 0.11B$ 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,可以用待隐藏消息替换每个像素红绿蓝亮度分量最低不同个数的比特位。即绿色分量改变最低 1 位比特位、红色分量改变最低 2 位比特位、蓝色分量改变最低 3 位比特位都不会使图像发生什么人眼容易察觉的变化。这样对图像位图阵列中的每 3 个字节就可以利用 $2 + 1 + 3 = 6$ 位比特位。示意图如图 1 所示。这样,在一幅大小为 L 字节的图像中,可以隐藏的信息量为 $(L - 54) / 24 \times 6 = (L - 54) / 4$,差不多为图像大小的 1/4,隐藏效率达到 25%。进一步,可以先用 WinZip 或 WinRAR 等压缩软件对秘密信息进行压缩,再进行加密,然后才把加密后的信息隐藏于图像信息中。这样,能更加有效地提高效率,用 WinRAR 软件对大小为 80 KB 的 Word 文档进行压缩,实验得到的压缩文件大小为 36 KB,实验结果表明使用 WinRAR 能把文档信息量压缩到原来的 1/2。于是,把隐藏的效率

从 25% 提高到 50%。所以, 在一张大小为 1 MB 的图像中, 能够隐藏的秘密信息大约为 $1 \text{ MB} \times 1/4 \times 2 = 500 \text{ KB}$, 可见, 用图像作载体和使用压缩技术能够隐藏大量的信息, 用效地利用线路带宽。

为了进一步加强安全性,可使用伪随机数发生器以相当随机的方式来扩展秘密信息,一个流行的方法是随机间隔法。如果通信双方使用同一个伪装密钥 K 作随机数发生器的种子,那么他们能生成一个随机序列 $k_1, k_2, \dots, k_m$, 并且把它们和索引一起按下列方式生成隐藏信息位置来进行信息传送:

$$j_1 = k_1,$$

$$j_i = j_{i-1} + k_i, \quad i \geq 2.$$

从而, 可以伪随机地决定两个嵌入位的距离. 由于接收者能获得种子 k 和随机数发生器的信息, 因此他能重构 k_i 进一步获得整个元素的索引序列 j_i . 从而从这个索引序列中把隐藏信息提取出来^[2].

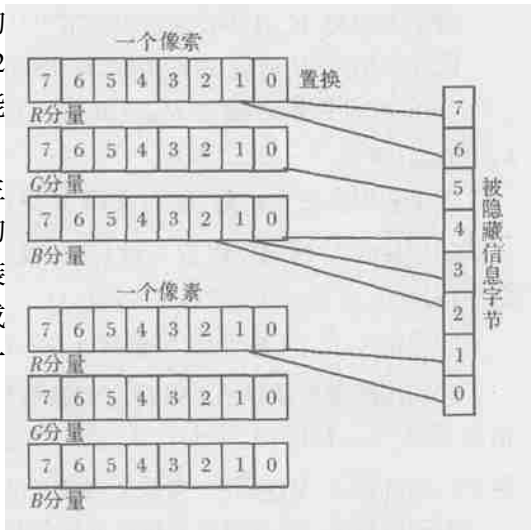


图 1 信息隐藏示意图

3 系统架构

应用密码体制和图像隐藏及数字水印技术保证电子商务安全传输系统架构如图 2。

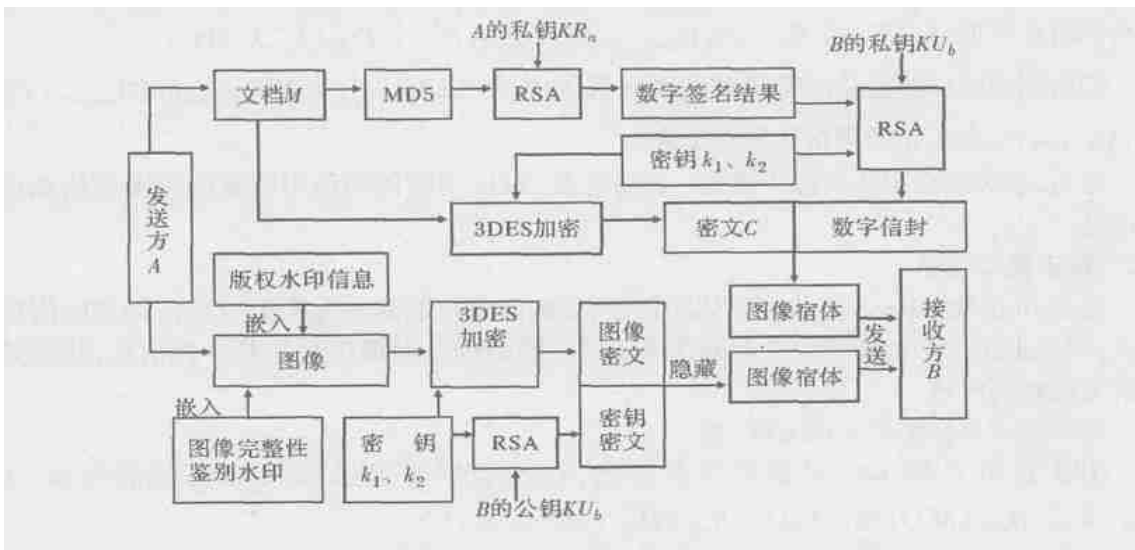


图 2 电子商务安全传输系统

这里, 密码体制中的对称加密系统采用安全度级别较高的 3DES 加密, 而公钥系统则采用 RSA 算法, 对信息产生摘要的是 MD5 散列算法. 数字水印嵌入技术采用鲁棒水印技术和易损水印技术. 隐藏密文的图像载体采用 24 位 BMP 图像附件.

3.1 加密隐藏传输

发送方 A 对要发送的电子商务信息进行分类处理: 可把商务信息分为文档和图像两大类,

对于文档类 M , 具体处理过程如下^[4-5]:

- ①先让明文 M 通过 MD5 函数, 产生信息摘要 $H_{MD5}(M)$;
- ②用 A 的私钥对摘要 $H_{MD5}(M)$ 进行 RSA 加密, 这样便形成 A 对文档 M 的数字签名 $E_{KR_a}(H_{MD5}(M))$;
- ③ A 利用会话密钥 k_1, k_2 对文档 M 进行 3DES 加密, 形成密文 $E_{K_1K_2}(M)$;
- ④用接收方 B 的公钥 K_{Ub} 对 k_1, k_2 及由第 ②步产生的数字签名结果进行 RSA 加密, 形成数字信封 $E_{K_{Ub}}(E_{KR_a}(H_{MD5}(M)) \parallel k_1k_2)$;
- ⑤把密文 $E_{K_1K_2}(M)$ 和数字信封连在一起, 得到 $E_{K_1K_2}(M) \parallel E_{K_{Ub}}(E_{KR_a}(H_{MD5}(M)) \parallel k_1, k_2)$;
- ⑥利用图像隐藏算法 LSB 把它们隐藏到宿体图像中, 用 C 来还表示最终在网络上传送的信息, 即有 $C = \text{LSB}_k(E_{K_1K_2}(M) \parallel (E_{KR_a}(H_{MD5}(M)) \parallel k_1k_2))$ (公式中密钥 k 为随机数发生器的种子). 最终把 C 发送出去, 完成文档信息的加密隐藏传输.

对于图像类, 用 P 表示要传送的图像信息, 用 copyright 表示版权信息, 用 distinguish 表示鉴别信息, 则具体处理过程如下:

- ①先用鲁棒水印技术嵌入版权信息, 得 $\text{DCT}_{\text{copyright}}(P)$;
- ②再使用易损水印技术嵌入图像的完整性鉴别信息, 得 $\text{SVD}_{\text{distinguish}}(\text{DCT}_{\text{copyright}}(P))$;
- ③水印嵌入后, 图像信息还是可见的, 为了保证其保密性, 用 3DES 对其加密, 得 $E_{k_1k_2}(\text{SVD}_{\text{distinguish}}(\text{DCT}_{\text{copyright}}(P)))$;
- ④同样把会话密钥 K_1, K_2 采用 B 的公钥进行 RSA 加密, 加密结果为 $E_{K_{Ub}}(k_1, k_2)$, 加密后的密钥附在图像信息后, 得 $E_{k_1k_2}(\text{SVD}_{\text{distinguish}}(\text{DCT}_{\text{copyright}}(P)) \parallel E_{K_{Ub}}(k_1, k_2))$;
- ⑤再把加密后的密文图像隐藏到图像宿体中, 得 $\text{LSB}_k(E_{k_1k_2}(\text{SVD}_{\text{distinguish}}(\text{DCT}_{\text{copyright}}(P))) \parallel E_{K_{Ub}}(k_1, k_2))$, 最后把图像宿体发送出去.

最后, 还必须在宿体图像中设置一些标志位, 以区别宿体图像中隐藏的是图像信息还是文档信息.

3.2 解密提取信息

接收方 B 从 Internet 上收到宿体图像后, 根据隐藏提取算法先把隐藏在宿体里的信息提取出来, 再根据图像中的标志位来判断宿体图像中隐藏的是图像信息还是文档信息, 从而采用不同的方法对其解密.

如果标志位标明是文档文件, 则:

- ①用 B 的私钥 K_{Rb} 对数字信封解密, 得到数字签名的结果和会话密钥 k_1, k_2 , 即 $D_{K_{Rb}}(E_{K_{Ub}}(H_{MD5}(M)) \parallel k_1, k_2) = E_{KR_a}(H_{MD5}(M)) \parallel k_1, k_2$;
- ②再用 A 的公开密钥 K_{Ua} 对数字签名的结果解密, 即 $D_{K_{Ua}}(E_{KR_a}(H_{MD5}(M))) = H_{MD5}(M)$, 得到文档 M 的数字摘要 $H_{MD5}(M)$;
- ③ B 用会话密钥 k_1, k_2 对密文 $E_{k_1k_2}(M)$ 进行解密, 得到文档 $M' = D_{k_1k_2}(E_{k_1k_2}(M))$;
- ④最后, B 用 MD5 算法对文档 M' 进行散列计算, 得到数字摘要 $H_{MD5}(M')$;
- ⑤比较 $H_{MD5}(M)$ 和 $H_{MD5}(M')$, 若两者值相同则表明文档没被修改过, 即有 $M' = M$, 若不同, 则表明文档受到篡改, 于是该文档无效.

如果标志位标明是图像信息, 则:

- ①先用 B 的私钥 K_{Rb} 解密出会话密钥 k_1, k_2 , 即 $D_{K_{Rb}}(E_{K_{Ub}}(k_1, k_2)) = k_1, k_2$;

②然后再用 k_1 、 k_2 对图像密文进行解密, 得到发送方 A 发的原图像 $D_{k_1 k_2}(E_{k_1 k_2}(\text{SVD}_{\text{distinguish}}(\text{DCT}_{\text{copyright}}(P)))) = \text{SVD}_{\text{distinguish}}(\text{DCT}_{\text{copyright}}(P));$

③最后通过提取水印算法把嵌入的水印提取出来, 从而判定图像的版权及图像的完整性。若版权和完整性都得到验证, 则表明该图像是正确的, 否则需要对方重传信息。

4 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。而使用对称密码体制加密后, 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, 采用对商务文档进行数字签名, 这样处理过后的商务文档既具有保密性、隐蔽性、完整性, 还可以对发送者进行认证以防假冒。同样对图像信息进行的加密操作以及嵌入水印操作能保证图像信息的保密性、隐蔽性和完整性, 对版权水印信息的确认又可以认证对方, 防止电子交易的假冒^[6]。

参考文献:

- [1] 杨义先. 信息安全新技术[M]. 北京: 北京邮电大学出版社, 2001.
- [2] 王丽娜. 信息隐藏技术与应用[M]. 武汉: 武汉大学出版社, 2003.
- [3] Kundur D, Hatzinakos D. Digital Watermarking for Telltale Tamper Proofing and Authentication [J], Proceedings of the IEEE, 1999, 87(7): 1167, 1181.
- [4] William Stallings[美]. 密码编码学与网络安全: 原理与实践(第二版)[M]. 杨明译, 北京: 电子工业出版社, 2002.
- [5] Bruce Schneier[美]. 应用密码学—协议、算法与 C 源程序[M]. 吴世忠译, 北京: 机械工业出版社, 2002.
- [6] 凌捷. 网络敏感信息传输中的图象隐藏技术[J]. 计算机工程. 2001, 27(7): 53-55.

Research on Electronic Commerce Security Transmission System

XU Shao-qiang, LING Jie, LI Hong-lei

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510090, China)

Abstract: Based on the multiplicity of the EC information, this paper introduces a method that combines Cipher mechanism with information hiding and digital watermark to implement the secrecy, integrity and concealment of the commerce information. It can not only authenticate the commerce information. but also protect the copyright of the image information.

Key words: electronic commerce; information hiding; 3DES; RSA; digital watermark