文章编号:1001 - 9081(2005)02 - 0403 - 04

基于数字水印和数字签名的电子支票支付系统

戴 华,张林聪 ,李炳法
(四川大学 计算机学院,四川 成都 610065)
(huazisc@126.com)

摘 要:探讨了当前电子商务支付中电子支票的安全问题,分析了其发展的形势及存在的安全缺陷,提出了一种结合数字水印和数字签名的安全保障机制。该机制采用了双重身份认证方案和水印内容认证方案,使得非法接触以及修改电子支票,伪造其内容都是不可能的。分析表明,该方案使得电子支票具有认证精度高、可信度高、安全性强等特点。

关键词:电子支票;数字水印;数字签名;半易碎水印
中图分类号: TP309.2 **文献标识码**:A

E-cheque payment system based on digital watermarking and digital signature

DAI Hua, ZHANG Lin-cong, LI Bing-fa
(School of Computer Science and Engineering, Sichuan University, Chengdu Sichuan 610065, China)

Abstract: The secure problems of E-cheque used in electronic commerce payment were studied. Based on the analysis of the developing circumstance and the security gap of it, a security guarantee system combining watermarking and digital signature were proposed. The double entity authentication and watermarking content authentication made it impossible to gain illegal access to E-cheque, to edit or to forge it. According to the analysis, the security, creditability and authenticity of the E-cheque can be achieved by the system.

Key words: E-cheque; digital watermarking; digital signature; semi-fragile watermarking

0 引言

随着电子商务的迅猛发展,全球电子商务交易额出现了逐年递增的趋势[1]。网上支付作为实现电子商务资金流转移的关键,正日益引起人们的注意,而电子支票作为网上支付的重要方式,也成了人们研究的热点。电子支票是一种借鉴纸张支票转移支付的优点,利用数字传递实现钱款在账户之间转移的电子付款形式,它可以通过因特网或无线接入设备来完成传统支票的所有功能。它具有处理方便、费用低、速度快的优点;而且银行也能为参与交易的商户提供标准化的资金信息,故而可能是最有效率的支付手段。目前电子支票采用公开密钥体系结构(PKI),可以基本上实现支付的保密性、真实性、完整性和不可否认性,从而在一定程度上解决了传统支票中大量存在的伪造问题。

电子支票在实现上的安全要求有:

1) 信息保密性:同传统支付方式一样,电子支票支付中的商务信息同样有很高的保密要求。

2) 交易者身份的确定性:通过网络相连,因为不能谋面,很难直接确定对方的真实身份,这就需要网络系统提供能够方便而安全地确认对方身份的保障措施。

3) 不可否认性:无论在网上还是在传统市场中,商情都是瞬息万变的。交易一旦达成则不可否认,否则必然导致市场的紊乱与交易一方利益的受损。

4) 不可修改性:如果支付细节是可以被修改的,那结果一定比可以否认还要坏,故支付细节应是不可被修改的。

1 基于数字签名的电子支票支付系统

1.1 现有电子支票系统

基于公钥体制的数字签名是当前在电子支票中普遍采用的技术。由于该技术采用的是基于非对称的密码机制,故该系统中应该包括电子支票的支付方、接受方、银行系统以及一个第三方的权威机构 CA(Certification Authority)。系统中用户的身份凭证是数字证书,数字证书对于用户是惟一的,且由用户预先申请。CA 负责发放和管理数字证书,用户在建立会话之前,首先通过数字证书经由 CA 建立彼此信任的关系,在此基础上,数字签名和密文形式的会话过程确保了合法接收和内容的真实性。

该系统的实现过程如下:

1) 双方决定用电子支票作为支付方式,并通过 CA 确定交易双方身份;

2) 买方用自己的私有密钥在电子支票上进行数字签名;

3) 买方使用卖方的公钥加密电子支票;卖方为唯一合法

收稿日期:2004 - 07 - 13;**修订日期**:2004 - 11 - 01

作者简介:戴华 (1981 -),男,四川宜宾人,硕士研究生,主要研究方向:电子商务、数字水印; 张林聪 (1982 -),男,四川眉山人,硕士研究生,主要研究方向:并行与分布式处理; 李炳法(1947 -),男,浙江宁波人,教授,主要研究方向:并行与分布式处理、数字水印.

接收者;

4) 通过网络将支票传送给卖方;

5) 卖方用自己的私有密钥解密电子支票;

6) 卖方用买方的公钥确认买方的数字签名;

7) 卖方向银行进一步确认电子支票;

8) 卖方发货给买方或提供相应的服务。

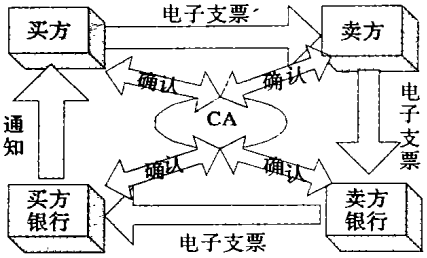

图1 基于数字签名的电子支票支付系统

1.2 数字签名的具体过程

1) 买方准备好要传送的电子支票。

2) 买方对电子支票进行 Hash 运算,得到信息摘要。

3) 买方用自己的私钥对信息摘要进行加密得到买方的数字签名,并将其附在数字信息上。

4) 买方随机产生一个 DES 密钥,并用此密钥对要发送的电子支票进行加密,形成密文。

5) 买方用卖方的公钥对刚才随机产生的加密密钥进行加密,将加密后的 DES 密钥连同密文一起传送给乙。

6) 卖方收到买方传送过来的密文和加过密的 DES 密钥,先用自己的私钥对加密的 DES 密钥进行解密,得到 DES 密钥。

7) 然后卖方用 DES 密钥对收到的密文进行解密,得到电子支票的数字信息,将 DES 密钥抛弃。

8) 卖方用买方的公钥对买方的数字签名进行解密,得到信息摘要。卖方用相同的 Hash 算法对收到的电子支票再进行一次 Hash 运算,得到一个新的信息摘要。

9) 卖方将收到的信息摘要和新产生的信息摘要进行比较,如果一致,说明收到的电子支票没有被修改[2]。

1.3 系统的安全性分析

以数字签名为保障的支付系统基本满足以下要求:1) 发送的不可抵赖性;2) 接收的不可否认性;3) 接收信息内容完整性。

但由于数字签名本身需要附着在电子支票上进行发送,因此其有被非法用户删除的危险;同时,若电子支票以明文方式发送,则有可能被黑客截取,从而泄露商业秘密。对于后者,一般的解决方案是采用传统加密技术加密后进行发送,但随着计算机软硬件技术的发展,密码被破译的可能性越来越大,即使非法拦截者在截获密文后无法破译,但可以将其破坏后再发送,使得接收的消息无法译成明文。

基于以上分析,一个更可靠的支付系统应该满足以下要求:1) 身份确认,合法用户数字证书申请和使用过程的安全性;2) 内容认证,信息内容的完整性和真实性验证;3) 传输过程中敏感信息的保密性。为此,我们构建了一个结合数字水印和数字签名技术的电子支票支付系统,满足了以上要求。

2 电子支票支付系统

2.1 数字证书的安全性

在该系统中,用户身份认证的凭证和基于数字签名的系统一样,也是由 CA 发放的数字证书。数字证书标识和证明了网上交易的主体的身份,是交易中个人或单位在 Internet 上的身份证。所以证书的发放和管理必须有一套严格的保障机制。关于这方面的讨论已经很多[3,4],不再论述。

2.2 数字水印

数字水印技术是通过一定的算法将一些信息直接嵌到不敏感载体数据(例如图片)当中,但不影响原内容的价值和使用,并且不能被人的知觉系统觉察或注意到,只有专用的检测器或计算机软件才可以检测出隐藏的数字水印。基于此,就可以在很大程度上避免恶意攻击。水印信息可以是作者的序列号、公司标志、有特殊意义的文本等,可用于版权保护,产品认证以及信息的秘密传送。目前大多数水印制作方案都采用密码学中的加密(包括公开密钥、私有密钥)体系来加强,在水印的嵌入、提取时采用一种密钥,甚至几种密钥联合使用。

由于要求满足信息隐蔽性、信息完整性等要求,我们在该系统中采用认证水印(Authenticati-on Watermarking)技术。认证水印除了具有数字水印的一般特征,如不可见、稳健性、安全性外,水印本身必须对篡改具有一定的敏感性和脆弱性。根据识别篡改的能力,认证水印分为脆弱水印(Fragile Watermarking)和半脆弱水印(Semi-fragile Watermarking)两种。半脆弱水印是当前数字水印研究的一个热点,它是指能够承受合理失真(如 JPEG 图像压缩),但会被不合理失真损坏的水印[5]。它在水印不可感知性的基础上又引入了内容真实性、完整性认证。这样就可以保证即使在水印被恶意攻击时不会被篡改。可以用来鉴定图像有无被编辑、毁坏或者替换,从而确认该图像内容的真实性。而且保证了嵌入信息可以被完整的提取出来。由于这几方面的特点,半脆弱数字水印可以和数字签名结合起来,弥补电子支票在使用上出现的安全缺陷,从而构建起更安全的电子支票支付系统。

2.2.1 一种可能的算法

对半脆弱水印来说,不但要保证其在临界点以下能继续存在,而且要在超过临界点的情况下失效,可以通过仔细地调整鲁棒性水印使其在失真达到一定程度时失效来获得半脆弱水印[6,7]。这里介绍一个例子:根据量化的特性来设计水印,令 $x \diamond q$ 表示将 X 量化成量化步长 q 的整数倍:

$$x \diamond q = q[x/q + .5]$$

如果 a 是实数标量,$q1$ 和 $q2$ 是量化步长,且 $q1 \leqslant q2$,那么:

$$((a \diamond q1) \diamond q2) \diamond q1 = a \diamond q1$$

就是说,将量化 a 到 $q1$ 的偶数倍,接着用 $q2$ 量化,只要 $q1 \leqslant q2$,就可以再对结果用 $q1$ 进行量化从而抵消 $q2$ 量化的效果[8]。

2.2.2 水印的嵌入

在客户端,当需要进行网上电子支票交易的时候,在本地计算机上或者 POP 上,通过银行获得一张电子支票,其中包

含了一般支票应包含的内容(如出票人、收款人、到期日等)和客户自己的签名、证书等。系统采用非对称密钥作为水印嵌入密钥[9,10],其生成是在客户与商家建立安全连接的时候进行的,客户用对方的密钥将电子支票嵌入到载体图片中,实现保密、安全、不可见及完整性通信。其一般过程如图 2 所示。

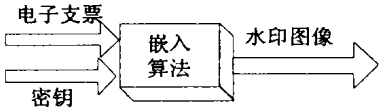

图 2　水印嵌入过程

2.2.3　水印的提取与验证

在水印提取端,用自己密钥和水印图像,作为提取算法的输入,提取出相关的特征值,与阈值进行比较,如果这个百分比大于阈值,则确认没有被篡改,然后再提取出电子支票,进行处理。

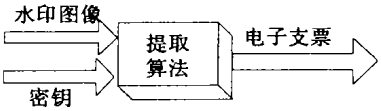

图 3　水印提取过程

2.3　改进后的支付系统

为了方便描述,我们设定交易双方为 A,B;支付方为 A,接收方为 B。支付方银行为 BkA,接收方银行为 BkB;私钥用 Key 表示,公钥用 Key' 来表示。

1) A,B,CA 之间的认证过程,以确认交易双方的身份

a) 交易双方决定交易,并确定用电子支票作为支付方式。

b) 交易双方与 CA 建立对话,表示双方将要交易,并请求 CA 确认各自身份;

c) 交易双方用各自的私钥对各自的数字证书进行加密,形成数字信封,然后发送给 CA;CA 用双方各自的公钥解密数字信封,确认双方各自的身份。若无误,交易继续。

2) A 与 BkA 交互,生成一张电子支票

a) A 与 BkA 建立对话,表示要求生成电子支票。然后 A 将支票信息进行数字签名后用 BkA_Key 加密,确定 BkA 是该支票信息的唯一合法接收者。接着 A 将加密后的支票信息和 A 的数字信封一起作为水印,用银行的公钥作为密码加入到图片中,传送给 BkA。

b) BkA 收到图片后,用专用的水印提取软件和 BkA_Key 进行提取,在验证水印完整性后,用 A_Key' 解密数字信封,确认 A 的身份的真实性。在无误的情况下,再用 BkA_Key 解密支票信息,在核对签名无误后,查看 A 是否具备支付能力,若是,按 A 的要求生成一张电子支票。

c) BkA 将电子支票进行签名,然后用 A_Key' 加密,再将加密后的电子支票作为水印,用 BkA_Key 作为密码加入到图片中,传送给 A。

3) A,B,CA 之间完成电子支票从 A 到 B 的安全传递过程:

a) A 用 BkA_Key' 提取水印,在确定水印完整性后,用 A_Key 解密电子支票,在核对内容无误后,将支票进行数字签名用 B_Key' 加密,并连同数字信封一起作为水印,用 CA_Key' 作为密码加入载体图片,发送给 CA。

b) CA 用 CA_Key 提取水印,验证完整性后,根据数字信封确认 A 的身份。

c) CA 将电子支票作为水印,用 B_Key' 为密码,加入到载体图片中,发送给 B。

d) B 用 B_Key 提取水印,验证完整性后,用 B_Key 解密电子支票,核对签名无误后,向 CA 发送收到的确认信息。

CA 的参与,监督了双方的交易过程,使得双方对交易过程不可抵赖,从而增加了系统的安全性。

4) B 与 BkB 之间的交互,确认支票的真实性:

a) B 与 BkB 建立对话,请求 BkB 验证支票。然后 B 对电子支票进行签名,然后用 BkB_Key' 加密,并连同数字信封一起作为水印信息,用 BkB_K - ey' 作为密码加入到载体中,发送给 BkB。

b) BkB 用 BkB_Key 提取水印,验证完整性后,根据数字信封确认 B 的身份。

c) BkB 解密支票,并通过银行内部网络向 BkA 查询支票的真实性和此时 A 的支付能力,若无误,就向 BkA 发送相关信息,要求转帐或在一段时间后进行行间批量转帐。

d) BkB 向 B 发送支票付款成功的消息;B 向 CA 发送该消息,并按交易协定向 A 提供货物或服务;CA 对此次交易备案,并向 A 发送成功的消息。至此,交易完成。

综上所述,结合数字水印和数字签名的电子支票支付系统涵盖了信息隐蔽性和数据完整性认证两大功能块。整个系统具有高安全性、运作的科学性以及高效性,其部分运行流程如图 4 所示。

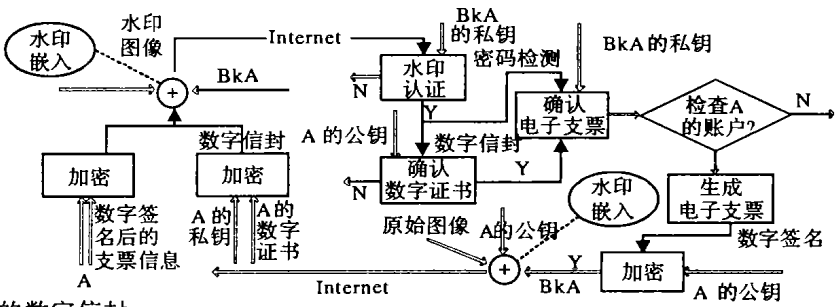

图 4　基于数字水印和数字签名的电子支票支付系统

2.4　系统安全性分析

该系统在原有的基于数字签名的支付系统的基础上,加入了水印技术。半易碎水印的完整性保护的特性,使得不可能对电子支票进行篡改和替换;水印的透明性,使得攻击者不易发现电子支票的存在,从而使电子支票的支付过程具有更高的安全性。虽然水印的加入和提取需要牺牲一定的时间,但由于电子支票本身的信息量不大,它的加入和提取的时间消耗是很微小的,但带来的却是很大的安全性的提升。

3　结语

电子支票相对于其他的在线支付方式有着明显的优势,是当前电子商务研究的一个重点。但由于涉及的金额比较大等原因,其安全性更受关注,还没有能在 Internet 普及,实现

Web 方式操作。本文通过半脆弱水印机制,利用了其信息隐蔽性和脆弱性来设计了一个结合数字水印和数字签名的安全的电子支票支付系统,使得电子支票在网上进行传播时,不会轻易的被察觉进而被攻击,同时,即使被攻击,想要破译几乎是不可能的,而由于其脆弱性,想要进行篡改,也会变得不可能。最后,信道传输误码以及有损压缩格式的传输方式都会给载体信息带来降质,这些改动主观上不可感知,对于只利用数字签名技术的系统来说,极易造成误判,但是对于半易碎水印来说,误判却是可以避免的。将水印技术用于电子支付的安全保障的研究还处于初级阶段,因此,系统的安全漏洞以及一些未知的攻击都有待发现、分析和加强。

参考文献:

[1] CHOIST, WHINSTON AB. The future of E - Commerce: integrate and customize[J]. IEEE computer. 1999, 32(1): 133 - 138.

[2] SCHNEIDER M, CHANG SF. A robust content based digital signature for image authentication[A]. In: Proceedings of the IEEE International Conference on Image Processing, Vol 3. Lausanne: IEEE Computer Society Press[C], 1996. 227 - 230.

[3] HOUSLEY R, POLK W, SOLO D. Internet X.509 Public Key Infrastructure Certificate and CRL Profile[S]. RFC 2459, IFTF, January 1999.

[4] ITU-T. Rec X.509, Information Technology-Open Systems Interconnection-The Directoty: Public-key and Attribute Certificate Frameworks [S]. ITU-T, 1988.

[5] IIN ET, POKDICHUK CI, DELP EJ. Detection of Image Alterations Using Semi-fragile Watermarks[C]. 2000. 152 - 163.

[6] REY C, DUGELAY J-L. Blind Detection of Malicious Alterations on Still Images Using Robust Watermarks[S]. IEE Seminar: Secure Images and Image Authentication, 7/1 - 7/6, 2000.

[7] YU G-J, LU C-S, LIAO H-Y, *et al.* Mean Quantization Blind Watermarking for Image Authentication[J]. in IEEE International conference on Image Processing, 2000, 3: 706 - 709.

[8] LIN C-Y, CHANG S-F. Semi-fragile Watermarking for Authenticating JPEG Visual Content[A]. in Security and Watermarking in Multimedia Contents II[C], 2000. 140 - 151.

[9] RIVEST RL, SHAMIR A, ADLEMAN LM. A Method for Obtaining Digital Signatures and Public-key Cryptsystems[J]. Communications of the ACM, 1978, 219(2): 120 - 126.

[10] EGGERS JJ, SU JK, BernGirod. Asymmetric watermarking schemes, Sicherheit in Mediendaten[A]. GMD Jahrestagung, Proceedings[C]. Springer Verlag, 2000.

(上接第 395 页)

我们这里选用的两种视频序列具有截然不同的运动特征:Foreman 更加动态,而 News 偏向于静态。之所以这样选择,目的是试图分析这种加密方法对于不同的加密对象的加密效率如何。测试加密效率的方法之一就是用视频压缩所用的时间与加密时间作对比,如果加密时间只占压缩时间很小的比例,那么就可以说明我们的加密算法不会引起视频传输的较大时延,具有可以信赖的加密效率。

我们分别选用 100 帧和 300 帧的原始序列进行测试,而且测试序列采用的格式分别为 Cif 和 Qicf,结果如表 1 所示。

表 1 测试结果(单位:s)

视频序列	视频格式	视频帧数	T_{ec}	T_{dc}	T_{ecc}	T_{dcc}	*Incr*%
Foreman	Qcif	100	13.87	1.97	13.98	2.05	1.19
Foreman	Qcif	300	43.25	5.56	43.44	5.70	0.67
Foreman	Cif	100	46.81	5.84	46.97	6.01	0.62
Foreman	Cif	300	145.37	16.4	146.02	16.97	0.75
News	Qcif	100	12.23	1.64	12.30	1.73	1.15
News	Qcif	300	36.35	4.49	36.54	4.58	0.68
News	Cif	100	40.02	5.06	40.14	5.18	0.53
News	Cif	300	112.5	14.35	112.81	14.84	0.63

注:T_{ec}、T_{dc} 分别为原始视频序列用 H.263 编码和解码所用的时间。

T_{ecc}、T_{dcc} 分别为原始视频序列用 H.263 编码、加密以及解码、解密所用的总时间。

$$Incr\% = \frac{(T_{ecc} + T_{dcc}) - (T_{ec} + T_{dc})}{T_{ec} + T_{dc}}$$

由表 1 可知,加解密时间与编解码时间相比,只占很小的比例,完全可以满足实时视频交互的要求。

2)保密性能分析

在我们提出的加密框图中,如果没有 CM_1、CM_2,那么通过一些密码分析方法来重新构造 CM_3、CM_4,从而到达解密的目的是可能的。

但是,由于这里使用了多层次的加密方法,使得 CM_3、CM_4 的状态实时改变,这样,即使通过一些知道部分明文(known-plaintext)的攻击方法得到 CM_3、CM_4 的输入 I,也很难推算出最初始的输入 $X_0^{(1)}$、$X_0^{(2)}$、a、λ。因为 I 是 CM_1、CM_2 的输出相加的结果,要想得到这两个加数各自的值非常困难。

那么,唯一的破解办法就是通过不断尝试的强力破解方法,这样一来,破解所需的时间会非常长。

4 结语

本文提出了一种较新颖的混沌视频加密方法,通过仿真分析实验结果,进一步证明此方法的有效性与安全性。

参考文献:

[1] SOBHY MI, SHEHATA AR. Methods of attacking chaotic encryption and countermeasures[A]. Proceedings 2001 IEEE Acoustic, Speech and Signal Processing[C], 2001. 1001 - 1004.

[2] BERITELLI F, COLA ED, FORTUNA L, *et al.* Multilayer chaotic encryption for secure communications in packer switching networks [J]. Proceedings International Conference on Communication Technology, WCC - ICCT, 2000, 2: 1575 - 1582.

[3] YI X, TAN CH, SIEW CK, *et al.* Fast encryption for multimedia[J]. IEEE Transactions on Consumer Electronics, 2001, 47: 101 - 107.

[4] ALATTAR AM, Al - Regib GI. Evaluation of selective encryption techniques for secure tuansmission of MPEG-compressed bit-streams [J]. Proceedings 1999 IEEE International Symposium on Circuits and Systems, ISCAS '99, 1999, 4: 340 - 343.