结合数字签名和数字水印的多媒体认证系统*

胡军全, 黄继武+, 张龙军, 黄达人

(中山大学 信息科学与技术学院,广东 广州 510275)

A Multimedia Authentication System Combining Digital Signature and Digital Watermarking

HU Jun-Quan, HUANG Ji-Wu+, ZHANG Long-Jun, HUANG Da-Ren

(School of Information Science and Technology, Zhongshan University, Guangzhou 510275, China)

+ Corresponding author: Phn: 86-20-84114993, E-mail: isshjw@zsu.edu.cn

http://www.zsu.edu.cn

Received 2002-05-27; Accepted 2002-08-14

Hu JQ, Huang JW, Zhang LJ, Huang DR. A multimedia authentication system combining digital signature and digital watermarking. *Journal of Software*, 2003,14(6):1157~1163.

http://www.jos.org.cn/1000-9825/14/1157.htm

Abstract: In this paper, the issues of entity authentication and content authentication mechanism of the digital signature based on multimedia system are addressed. Based on the analysis of the security gap in the authentication mechanism using digital signature, a novel authentication protocol combining digital signature and fragile watermarking are proposed. Double entity authentication based on digital signature and content authentication base on fragile watermarking is achieved. Illegal access to system, edition, and forgery of multimedia document is proven to be impossible. According to the analysis, the security, creditability, and authenticity are achieved.

Key words: multimedia authentication; fragile watermarking; digital watermarking; digital signature

摘 要: 探讨了基于数字签名的多媒体信息认证系统的身份认证机制和内容认证机制,分析了其基本构成以及安全性和存在的安全缺陷,提出了一种结合数字签名和数字水印的多媒体信息认证方案.系统采用双重身份认证机制和易碎水印内容认证机制,使得非法接触以及修改、伪造多媒体信息的内容都是不可能的.分析表明,该多媒体信息认证方案具有安全性强、可信度高、认证精度高等特点.

关键词: 多媒体认证;易碎水印;数字水印;数字签名

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant Nos.60133020, 69975011, 60172067 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2002AA144060 (国家高技术研究发展计划(863)); the Cross-Century Talent Raising Program of Ministry of Education of China (国家教育部跨世纪优秀人才培养计划); the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No.20020558038 (国家教育部博士点基金); the National Natural Science Foundation of Guangdong Province of China under Grant No.013164 (广东省自然科学基金)

第一作者简介: 胡军全(1977－),男,浙江东阳人,博士生,主要研究领域为多媒体信息安全.

随着多媒体技术和网络技术的飞速发展,通过网络获取信息已经变得日益普遍,信息交换也从简单的文本信息发展到多姿多彩的多媒体信息.在这种情况下,网络信息接受者希望得到预定发送者发送的真实的数据版本,发送者也希望获得接收者的回执以证明正确接收.但是,网络本身并没有提供这种保证.多媒体信息在传输过程中会遭受各类有意或无意的篡改攻击.这意味着信息的安全性极大地降低了,用户对经由网络获得的信息的真实性产生怀疑.

认证是多媒体信息安全技术的一个重要方面[1].由于认证技术提供了通信双方身份和通信内容、过程的可信度保证,从而被广泛应用于以多媒体信息为主要交流方式的网络业务系统中,如电子商务、电子政务等.而在上述系统中,由于多媒体信息往来比较频繁,而且信息权限分级比较细,因此,如何保证信息不被越权接收和发布使用,如何保证信息往来双方彼此信任,如何保证信息内容的真实可靠性,这些都是认证系统必须要解决的问题.

基于公钥体制的数字签名提供了一种身份认证模式,并且当用户用私钥签名时,签名与用户本身联系在一起,且具有法律效力.另外,通过 Hash 技术求取的依赖于原始信息的信息摘要可以反映出原始信息的轻微变化[2,3].因此,数字签名被广泛用于多媒体信息传输过程中,使得传输双方建立互相信任的关系以及确保传输信息的内容完整性.由于图像信息在多媒体信息中具有代表性,因此本文仅以图像为例,探讨认证技术.其他诸如视频、音频等信息具有类比性.

本文第 1 节分析了基于数字签名的认证系统的构成以及安全性,提出了新的认证系统的要求.第 2 节在分析易碎水印机制的基础上,构造了一个结合数字签名和数字水印的新的认证系统,并分析了系统安全性.第 3 节给出了系统的几点附加要求以及结论.

1 基于数字签名的认证系统

一个通用的数字签名认证系统[4]包括两个功能块:身份认证功能和内容认证功能.前者用来限制非法登陆,后者用来保证合法通信过程的内容认证.为此,系统将包括业务双方以及一个大家都信任的权威第三方作为认证中心 CA(certification authority)[5].系统中用户的身份凭证是数字证书.数字证书对于特定用户是惟一的,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.

基于数字签名的认证系统的优点是:(1) 发送的不可抵赖性;(2) 接收的不可否认性;(3) 非法用户的不可接收性;(4) 接收信息内容完整性的保护;(5) 接发过程通过一个中间者完成,并可见证接发全过程,过程具有不可抵赖性.因此,系统集成了身份认证和内容认证两大功能.

一般来说,非法用户常采用以下主要手段对数字签名认证系统进行攻击:(1) 个人攻击,窃取合法数字证书用于非法途径;(2) 内容攻击,篡改或伪造传送公文、删除签名、伪造假签名等,从而对于正常的信息往来程序造成破坏.虽然结合指纹和数字签名认证等技术可以用来加强密钥管理,增加个人攻击难度.但是对于多媒体信息来说,由于其签名的生成主要依靠特征提取算法(以图像为例,首先提取图像特征,然后私钥加密成为签名),因此根据图像特征的特性,在某些保持内容的格式转换或者有损压缩处理后,多媒体内容在主观感觉上没有变化.但是图像特征即便发生微小变化也会由于 Hash 函数的特性而导致签名发生变化.因此,保证图像内容压缩传输前后签名证实算法的一致性,就成为一个至关重要的问题.

综上可知,一个更可靠的认证系统应该满足以下要求:(1) 个人认证,合法用户的分权限级别的访问方式,合法用户数字证书申请过程的保密性;(2) 内容认证,信息内容的完整性和真实性验证;(3) 认证机制的安全性.数字签名信息与原信息内容紧密结合,且签名本身捆绑于原信息后发送,这使得签名的删除变得非常容易.因此,一个新的要求就是签名直接嵌于信息内部.

2 结合数字签名和数字水印技术的认证系统

2.1 易碎水印

数字水印兼有版权保护和内容真实性、完整性认证的功能.鲁棒水印和易碎水印分别完成了这两个功能[6~8].20 世纪 90 年代初期,易碎水印第一次用于认证目的[8].通过研究人们发现,一个具有微弱鲁棒性的水印,由于其对众多图像操作的鲁棒性较低,因此,操作结果或多或少地会在提取水印上有所反映.根据这一特性,用户可以确定原始图像有没有被非法用户进行图像“操作”.这一类水印被称为易碎水印.易碎水印的研究热点目前已经转向在对特定操作鲁棒的同时保持对其他操作易碎的半易碎水印的研究.一般地,一个易碎水印应该满足 3 个基本要求[9,10]:(1) 对篡改高度敏感;(2) 不可见性;(3) 不容易被替换.

易碎水印由于其安全的嵌入策略以及对篡改的高敏感性,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.根据水印嵌入机制,水印直接嵌入宿主内部,且嵌入导致的信息轻微改动主观上不可感知.这使得嵌入信息的删除非常困难,而且保证了嵌入信息可以与原信息脱离,同时保证完整性认证能力.而在这一点上,数字签名用以完成完整性验证的信息摘要却必须与原信息结合.因此,在嵌入水印的设计上,用户可以采用另外一些有意义或直观的信息,使得认证过程更加具体化.另外,易碎水印的内容真实性和完整性验证能力同样可以保证在认证系统中完成内容认证.因此,作为数字签名的互补技术,易碎水印完全满足了多媒体信息认证系统的新要求.通过易碎水印来设计、构建高安全性和高效性的认证系统是完全可行的.

2.2 基于水印的认证策略

类似于数字签名认证系统,基于水印的认证系统由认证中心 CA 以及用户端构成.CA 承担数字证书的生成与管理、身份认证等业务,由能签发数字证书并能确认用户身份的具有权威性、公正性的第三方机构担任.用户端则具备水印嵌入、水印证实和内容完整性检验等能力.下面细述基于水印的认证系统的关键技术.

为了方便叙述,本文采用以下记号:A 代表信息发出者,A_key,A_key'分别代表 A 的私钥和公钥.B 代表信息接收者,B_key,B_key'分别代表 B 的私钥和公钥.M,M',M''代表待发信息.CA 代表认证中心,CA_key,CA_key'分别代表 CA 的私钥和公钥.$Sig_k(\cdot)$代表签名算法,$Ver_k(\cdot)$代表签名证实算法,$Enc_k(\cdot)$代表加密算法,$Dec_k(\cdot)$代表解密算法,其中 k 是密钥.C_A,C_B 代表用户 A,B 的数字证书.

(1) 数字证书的生成与管理

数字证书的要素包括用户名、签发者名称、有效期、用户公钥信息、签发者对证书的数字签名等[5].为了与水印机制相适应,数字证书还必须有原始水印.水印为二值图像,由用户自己设定,可以是用户的手写签名图案或者公司商标等等.数字证书对于用户是惟一的,且由用户预先向 CA 申请.申请时,用户提供上述信息,并设定自己的私钥.CA 负责对信息生成数字签名并最终形成数字证书.为了保证申请过程中用户私人信息的保密性,采用以下机制来保证数字证书颁发过程的合法性.记用户的私人信息为 M.申请与颁发过程有如下 4 步:

① 申请时,A 首先填写真实的个人相关信息,并输入原始水印.再输入事先生成的公钥,A 保留惟一的私钥.然后用私钥对信息生成签名,再用 CA 的公钥加密后发送给 CA,即

$$\mathrm{A}\longrightarrow\mathrm{CA}:\ Enc_{CA\_key'}(M, Sig_{A\_key}(M)).$$

② CA 接收来自 A 的信息 M'后,首先用私钥解密,获得 A 的公钥信息,然后验证 A 的信息完整性.若验证无误,则进入下一步操作,即

$$Ver_{A\_key'}(Dec_{CA\_key}(M'), Sig_{A\_key}(M)).$$

③ CA 颁布数字证书.首先用私钥对 A 的信息进行签名,A 的信息以及该签名即构成数字证书.再用 A 的公钥对证书加密后发送给 A,完成数字证书颁布过程,即

$$\mathrm{CA}\longrightarrow\mathrm{A}:\ Enc_{A\_key}(C\_A, Sig_{CA\_key'}(C\_A)).$$

④ 记 A 接收到信息 M'',则 A 用自己的私钥解密即可得到数字证书,并验证其正确性,即

$$Ver_{CA\_key}(Dec_{A\_key'}(M''), Sig_{CA\_key'}(C\_A)).$$

(2) 水印嵌入机制

CA 提供了用户信用保证,确保了信息往来双方的可信度.但对于往来信息内容的可信度却没有提供保证.因此,系统需要特殊的机制来保证传送信息的完整性和真实性.本文提出的认证系统采用易碎水印技术来实现数据内容的认证.为了防止窃听、重传、非法用户非法接收等情况的发生,系统采用基于双钥体制的水印机制来加强用户的身份认证能力.以用户私钥作为水印嵌入密钥,以公钥作为水印证实密钥,实现单个用户嵌入水印的消息可由多个用户解读[11,12].这满足了多媒体信息认证系统对于用户发送不可抵赖性和不可否认性的内在要求.而且易碎水印保证了会话过程中信息的完整性和真实性,从而满足了内容认证的要求.整个嵌入流程如图1所示.可以用一个函数来表示水印的嵌入过程:

$$I' = Embedding(I, W, Key_{\text{private}}),$$

其中 I 和 I' 分别代表原始图像和水印图像,Key_{private} 是私钥,W 是原始水印.

(3) 水印的证实

在基于双钥密码体制的水印方案中,水印的证实需要用户的公钥.图 2 揭示了水印证实的一般过程.水印的检测一般依赖提取水印与原始水印的差图 $W_{\text{difference}}$ 或者互相关系数 ρ.但在采用第 2 种机制时,篡改的定位主要依靠分块嵌入机制,因此,篡改定位精度很大程度上由分块精度决定,且分块大小会影响潜入水印的信息量,从而对水印算法的安全性产生影响.因此,本文通过水印差图来判断和定位篡改.具体的检测过程如下,首先提取水印:

$$\tilde{W} = Extraction(\tilde{I}, W, Key_{\text{public}}),$$

其中 $\tilde{I}$ 是待检图像和原始图像,W 是原始水印,Key_{public} 是公钥.水印提取完毕之后,计算水印差图:

$$W_{\text{difference}}(i,j) = \begin{cases} 0, & \text{if } W(i,j) = \tilde{W}(i,j) \\ 1, & \text{else} \end{cases}.$$

最后判断有无篡改:

$$Ver(\tilde{I}) = \begin{cases} \text{无篡改}, & \text{if } card(W_{\text{difference}}) = 0 \\ \text{有篡改}, & \text{else} \end{cases},$$

其中 $card(\cdot)$ 是对应集合的势函数,在式中相当于逐点像素值求和.水印差图中值为 1 的点都是篡改发生点,视觉上就是白色背景上的黑色区域.根据差图或仅仅根据视觉可以判断和定位篡改.

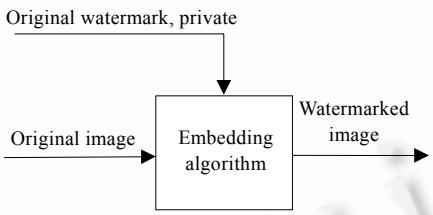


Fig.1 Watermark embedding
图 1 水印嵌入流程

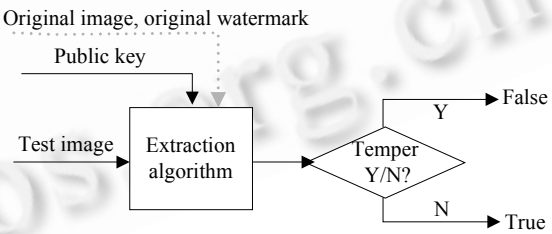


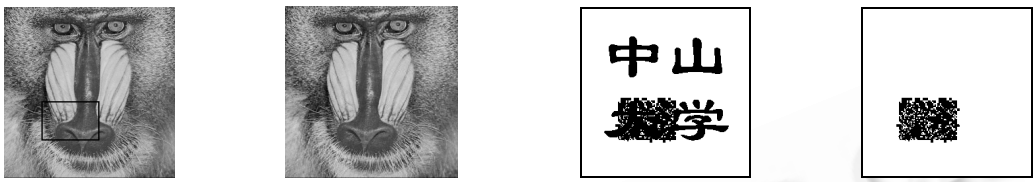
Fig.2 Watermark verification
图 2 水印证实流程

(4) 用户身份认证

在系统中,用户的身份认证通过两步来实现.第 1 步,由认证中心 CA 对双方的数字证书进行认证,经认证合法,则继续通信.首先,用户 A 给 CA 一个会话信息,要求同 B 建立会话.然后,CA 要求 A,B 各自验证身份,A 和 B 用各自的私钥加密数字证书发给 CA,CA 用各自的公钥验证用户签名信息的正确性,再给双方发送信息,确认会话双方正是预期的会话者.第 2 步,通过双钥体制来保证合法接收.首先,发送者通过自己的私钥嵌入水印,再用私钥加密自己的证书成数字信封,然后用 CA 公钥加密两者.CA 是惟一的合法接收者,接收后用自己的私钥解密.CA 先用 A 的公钥解密数字证书验证其真实身份,然后可根据请求对公文的内容真实性进行证实,只需利用 A 的公钥进行水印证实过程,即可判断有无篡改.若无篡改,CA 再用自己的私钥加密 B 的数字证书成数字信封,把数字信封和信息一起用 B 的公钥加密发送给 B.由于 B 是惟一具有私钥的人,因此,只有 B 才能合法接收到实际真实的内容,而且可以通过验证数字证书来确认信息确实来自 CA,从而完成身份认证.

(5) 数据认证

在认证方案中,数据的完整性和真实性认证通过水印差图来完成.接收用户拥有原始水印信息,因而可以通过函数 *Ver*(·)判断是否有篡改.若无,则数据内容属实;反之,有篡改,继续定位篡改.图 3 表示一个用易碎水印来完成图像内容完整性检测的例子.图 3(a)表示水印图像,图中黑框中的内容将被替换.图 3(b)是黑框中的内容被原始图像的相应内容替换后的图像.图 3(c)是水印探测图.图 3(d)是水印差图,黑色区域准确定位了篡改.



(a) Watermarked image (b) Tempered image (c) Extracted watermark (d) Difference image of watermark

(a) 水印图像 (b) 替换后结果 (c) 水印提取图 (d) 水印差图

Fig.3 Tamper detection by using fragile watermarking

图 3 利用易碎水印进行篡改检测

综上所述,结合数字签名和数字水印的认证系统涵盖了身份认证和数据认证两大功能块.整个系统具有高安全性、运作的科学性以及高效性,其运行流程可用图 4 来综合表示(图中 ⊕ 表示联合).

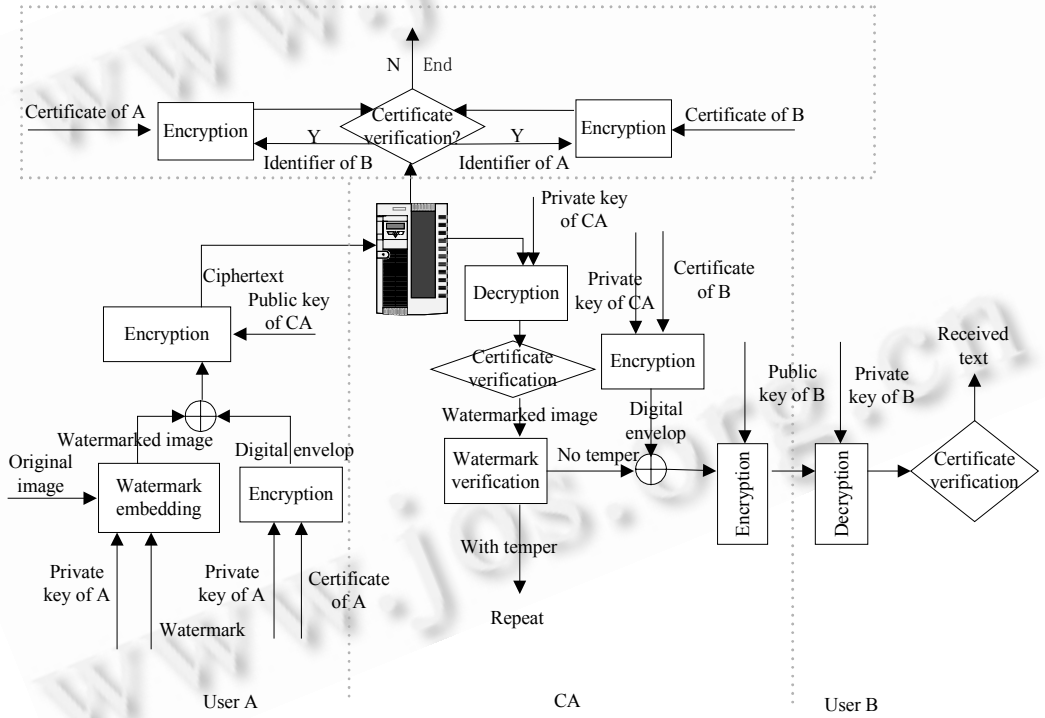


Fig.4 Authentication system based on fragile watermarking and digital signature

图 4 结合易碎水印和数字签名的认证系统

如图 4 所示,用户 A 希望把真实的信息 *M* 发送给合法用户 B.要经过以下几个步骤:

(1) A 先将数字证书发给 CA,验证合法性.然后用私钥嵌入水印,再用私钥加密数字证书成数字信封,并将水印图像与数字证书用 CA 的公钥加密后发送给 CA,且说明与 B 的会话请求,即

$$\text{A}\longrightarrow\text{CA}: Enc_{CA\_key'}(Embedding(M,W,A\_Key)\oplus Enc_{A\_key}(C\_A)).$$

(2) 记 CA 收到的信息为 *M*′,CA 通知 B 有公文,若要接受,则需 B 的数字证书证明身份合法.

(3) B 将数字证书提交给 CA 并请求验证水印.CA 验证其合法性,继而通过私钥解密 *M*′,并验证数字信封确

认是 A 发送的信息,再用 A 的公钥提取水印,验证内容完整性,若无篡改,则给 A,B 信息完整性回复,否则通知 A 重发.

(4) 若 B 接收到内容无误,则向 CA 请求阅览信息.CA 先用私钥加密 B 数字证书成数字信封,并与解密的 M'一起用 B 的公钥加密后发给 B,最后发给 A 一个收报认证,说明 B 已经收到真实的文件,即

$$\text{CA}\longrightarrow\text{B: } Enc_{B\_key'}(Dec_{CA\_key}(M')\oplus Enc_{CA\_key}(C\_B)).$$

(5) 记 B 收到的信息为 M'',则 B 首先用自己的私钥解密,再用 CA 公钥验证数字证书确认信息确实来自 CA 无误,然后接收信息内容.

(6) CA 纪录此次信息往来,以备以后查证.

2.3 系统安全性分析

从多媒体系统业务能力上来看,主要目的有两个:(1) 用户的身份认证;(2) 传递信息的完整性和真实性认证.从系统抗攻击能力来看,主要目的也有两个:(1) 防止非法用户盗用合法证书;(2) 防止合法用户传递非法信息.意指合法用户对重要的接收信息经修改、伪造后进行非法发布.由第 1 节分析可知,数字签名认证系统不能完全保证这一点.基于易碎水印的认证方案弥补了这一不足,水印直接嵌入信息内部.这样做的好处是:(1) 签名的生成可以不依赖于原信息;(2) 签名的删除极其困难;(3) 嵌入引起的微弱信息改动不影响用户对信息的真实性判断;(4) 签名随信息一起发布,避免了数字签名机制中签名对信息的保护有随时失去的危险性,且由于签名嵌入信息一起发布,因此在信息的整个有效期内都提供保护.在系统中,数字证书以及基于双钥体制的数字信封机制完成了两级身份认证.而且用户与 CA 之间传递的信息内容,使用了基于易碎水印的数据完整性和真实性保护.这使得用户的身份和信息内容都得到认证,从而保证了一个会话过程的可信度,防止了黑客的假冒和对信息的篡改,保证了系统的高安全性.

3 结 论

本文通过易碎水印机制,设计了一个结合数字签名和易碎水印的安全的多媒体信息认证系统.在具体水印方案以及签名方案的选择上,还需注意以下几点.首先,为了保证传输过程的安全性,所有信息都是以密文的形式传输的.因而,多媒体信息的加密传输必须保证信息在解码后没有变化.因为这有可能导致敏感性较高的易碎水印产生误判.其次,在完成第一重身份认证时,系统采用了基于数字签名的数字证书的验证方案.而由于复杂性较低的签名方案易受攻击,因此,对于签名方案,系统的要求是必须具备不可否认性,而且破译代价很高.最后,信道传输误码以及有损压缩格式的传输方式都会给多媒体信息带来降质,即便这些改动主观上不可感知,但是对于易碎水印来说,误判还是不可避免的.因此,水印方案要求是半易碎的.基于以上选择,易碎水印和数字签名结合的机制使得系统保证了高安全性,同时具有以下特点:(1) 由于水印嵌入信息内部,从而对整个信息生存期都提供了保护,而不仅仅在通信会话过程中提供保护;(2) 易碎水印的高度敏感性,使得任何对信息的轻微修改都可以检测到,并且具有篡改的定位功能;(3) 两级身份认证机制,保证了非法盗用数字证书是不可能的,同时保证了接发过程的合法性;(4) 数字证书由 CA 中心统一发放和管理,使得管理非常方便且易于扩充.由于易碎水印技术的研究发展远未成熟,基于水印技术的安全认证系统的研究也才处于探索阶段,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.下一步的研究目标是探讨如何利用易碎水印机制以及双钥体制来对多媒体信息提供更完善的认证保护.

References:

[1] Nahrstedt K, Dittmann J, Wohlmacher P. Approaches to multimedia and security. In: Proceedings of the IEEE International Conference on Multimedia and Expo. New York: IEEE Computer Society Press, 2000. 1275~1278.

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

[3] Lou DC, Liu JL. Fault resilient and compression tolerant digital signature for image authentication. IEEE Transactions on Consumer Electronics, 2000,46(1):31~39.

[4] Deng H, Gong L, Lazer A, *et al*. Practical protocols for certified electronic mail. Journal of Network and System Management, 1996,4(3):279~297.

[5] Gray JW, Epsilon KF. Protocols for issuing public-key certificates over the Internet. In: Han YF, ed. Proceedings of the International Conference on Information and Communications Security. Beijing: Springer-Verlag, 1997. 424~434.

[6] Huang JW, Shi YQ, Shi Y. Embedding image watermarks in DC components. IEEE Transactions on Circuits and Systems for Video Technology, 2000,10(6):974~979.

[7] Cox I, Kilian J, Thomson F, *et al*. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997,6(12):1673~1687.

[8] Friedman G. The trustworthy digital camera: Restoring credibility to the photographic image. IEEE Transactions on Consumer Electronics, 1993,39:905~910.

[9] Lin ET, Delp EJ. A review of fragile image watermarks. In: Proceedings of the Multimedia and Security Workshop at ACM Multimedia'99. Orlando: ACM Press, 1999. 35~39.

[10] Fridrich J. Methods for tamper detection in digital images. In: Proceedings of the Multimedia and Security Workshop at ACM Multimedia'99. Orlando: ACM Press, 1999. 29~33.

[11] Wong PW. A public key watermark for image verification and authentication. In: Proceedings of the International Conference on Image Processing, Vol 1. Chicago: IEEE Computer Society Press, 1998. 425~ 429.

[12] Katzenbeisser S. On the design of copyright protection protocols for multimedia distribution using symmetric and public-key watermarking. In: Proceedings of the 5th International Query Processing and Multimedia Issues in Distributed Systems Workshop. Munich: IEEE Computer Society Press, 2001. 815~819.

全国第 13 届网络与数据通信学术会议(NDCS13)

征 文 通 知

本届会议旨在推动开放系统及其互联技术、开放式网络技术和数据通信技术的发展。会议由中国计算机学会开放系统专委会和网络与数据通信专委会联合主办、大连理工大学电子与信息工程学院承办、大连市计算机学会协办，定于 2003 年 10 月在大连市同 2003 年全国开放式分布与并行计算学术会议联合举行。有关信息如下：

一、征文范围

开放系统及其互联技术，新一代网络体系结构与协议，网络智能化，网络管理，网络信息系统模型，网络计算与应用，网络环境下的信息安全，无线通信网络，电子商务系统以及光纤通信等技术。

二、征文要求

(1) 论文应是未正式发表的，或者未正式等待刊发的研究成果；

(2) 论文格式仿照《计算机研究与发展》刊物的格式，应包含题目、摘要、关键词、正文和参考文献；

(3) 论文中、英文均可，一般不超过 5000 字，一律用 Word2000 格式排版，提供 A4 激光打印稿一式两份，并随寄软盘；

(4) 邮寄论文时，须在信封左下角或 Email 主题中注明"NDCS13"；

(5) 经程序委员会审查合格的论文，将收入论文集，在自然科学核心刊物集中发表或者推荐到适当刊物发表；

(6) 论文一律寄给大连地区联系人。论文自留底稿，恕不退稿。

三、重要日期与联系方式

(1) 论文须在 2003 年 6 月 30 日之前寄达，录用通知将在 2003 年 7 月 15 日发出。

(2) 联系方式:

- 大连地区联系人:郭禾、单慧英

地址: 大连理工大学计算机系系统结构教研室 邮编: 116023 电话: 0411–4708497

E-mail: dpcs2003@dlut.edu.cn

- 北京地区联系人:陈炳从(中国计算机学会开放系统专委会主任)

通信地址: 北京 619 信箱 63 号 邮编: 100083 联系电话: 010–62311951

- 石云(网络与数据通信专委会秘书长)

通信地址: 北京宣武门西大街 131 号国家邮政局信息技术局 邮编: 100808 联系电话: 010–66419786

(3) 会议主页: http://hefeng.dlut.edu.cn/DPCS2003