一种基于虹膜识别技术的数字版权管理系统*)

裴庆祺[1] 范科峰[2] 马建峰[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[1]
(中国电子技术标准化研究所 北京 100007)[2]

摘 要 数字版权管理(DRM)系统是用于数字交易的有效保护方案。基于高安全性的虹膜生物识别方法,本文提出了一种新的DRM模型。该模型能够稳定而准确鉴别用户身份和权限,完成对数字内容使用的权限管理。为了克服现有DRM系统中数字内容分发存在的安全漏洞,在对用户的身份识别过程中,采用自动虹膜识别方法而不是传统的密码口令。为了保证生物数据的安全性,此模式采用基于PKI的安全交互协议。分析和研究表明此模型有较高的安全性、可靠性,适用于数字内容的安全分发。

关键词 数字版权管理,数字内容,生物测定学,自动虹膜识别系统

A Digital Rights Management System Based on Iris Recognition Technology

PEI Qing-Qi[1] FAN Ke-Feng[2] MA Jian-Feng[1]
(Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071)[1]
(China Electronics Standardization Institute, Beijing 100007)[2]

Abstract Digital rights management (DRM) system is the effective schemes for digital transactions. A new DRM model based on highly secure iris recognition is proposed, which is can achieve the rights management of digital content exactly through the illegal user's access control. To overcome the security loopholes in the distribution of digital content in the current DRM, an automatic iris recognition system rather than password is adopted during the process of identifying the users. To ensure the security of the biometric data, a protocol based on PKI is proposed. The analysis and the research show the proposed model is highly reliable, and is applicable to the secure distribution of digital content.

Keywords DRM, Digital content, Biometric, Automatic iris recognition system

1 引言

数字技术的迅速发展,互联网、电信移动网络等新兴传输方式和各种多媒体终端(如手机、数字电视、网络电视、机顶盒、电脑等)的广泛应用,极大拓展了数字内容的传输范围。数字内容易于无损复制和分发,在互联网上,借助数字技术,随意批量复制和发行受知识产权保护的数字媒体产品和内容的现象普遍存在。由此而滋生大量盗版以及数字内容的不规范使用行为,这些不但对数字媒体产业造成巨大的冲击,而且对经济、社会和文化造成了严重伤害。

数字版权管理DRM(Digital Right Management)便是随着数字技术的广泛应用而发展起来的一种保护数字内容版权的新技术。其目的就是从技术上防止对数字内容的非法复制和滥用。DRM系统提供了对数字内容进行安全分发、权限控制和运营管理的功能。数字内容权益方为每个数字内容定义不同的使用权限。支付相应费用并得到授权之后的用户能够按照相应的权限消费数字内容。

目前DRM系统大多依赖于密码技术,但在密码技术的操作过程中存在很大的隐患,其中最突出是密钥管理,盗取密钥的非法用户能够充当合法用户非法访问数字内容。许多客体(个体消费者,系统管理员,经销商和发行人,支付经纪人等)都在使用类似的密钥,加之人们通常设置简单易于记忆的密码,使得密码破译更加容易。使用密码的一个主要问题就是一旦密码被破译,则不能够区分合法用户和破译了密码的非法用户。使用用户生理特征和密码之间的绑定为克服此缺点提供了新的思路。这种密码机制使用生物识别技术来对数字内容进行保护。

本文将虹膜识别技术应用到数字版权管理系统中,结合传统的PKI机制,实现对访问数字内容的用户身份验证。分析和研究表明,提出的模型具有较高的安全性和可靠性,适用于数字内容的安全分发和访问控制。

2 现有DRM系统分析

目前,内容提供商主要采用两种方式来保证内容安全分发,一是在供应商和用户之间建立安全通道,在分发数字内容之前,对用户进行身份验证;二是使用加密的方式分发数字内容,拥有密钥的合法用户可以解密接收到的数字内容,这种方式需要安全的密钥管理机制的支撑。现有的DRM系统的安全结构大都基于以下技术[8,9]。

1)数字水印:在被保护的数字对象(如图像、音视频等)中嵌入能够证明版权归属或跟踪侵权行为的信息,这些信息可能是作者的序列号、公司标志等;

*)基金项目:国家自然科学基金(60672112,60633020),陕西省自然科学基础研究计划资助项目(项目批准号:2005F28);西安电子科技大学研究生创新基金资助课题(课题编号:创5001,创05006)。裴庆祺 博士研究生,CCF高级会员,主要研究领域:信息安全、无线传感器网络及安全。

2)数字指纹:是一种信息隐藏技术,利用数据冗余性和随机性,采用技术手段向数字作品中引入指纹标记,它必须隐含用户信息;

3)抗软/硬件篡改:该技术是终端用户安全传输、解密内容的可靠技术。硬件能够主动监测并对攻击作出响应。抗篡改技术为 DRM 系统提供安全的运行环境;

4)加密:加密可以阻止侵犯者读取信息著作权,能够进行数字内容的安全分发。但是它不能控制副本的非法传播和发布,这些非法副本可能是由合法用户解密得到的。

以上方式存在的主要问题:1)合法用户和欺诈用户对系统而言没有区别;2)系统需要为用户安全地分发、存储和管理密钥。针对现有方式存在的缺点,本文引入生物特征识别技术,建立基于虹膜识别技术的数字版权管理系统。此 DRM 的主要思想为:人体的某些特征是人体固有的且具有不可复制的唯一性,这些特征的应用成为"用户认证"的最佳方式;将这些特征应用于 DRM 系统的用户认证和密钥产生,解决现有 DRM 系统中存在的问题。基于虹膜识别技术的数字版权管理系统在现有系统中增加基于虹膜识别技术的安全层,以此实现对加密密钥的安全控制。

3 基于虹膜识别技术的 DRM 系统

本文提出了一种基于虹膜识别技术的 DRM 系统,此系统能够有效地对用户进行身份验证和密钥分发,解决现有的 DRM 系统中存在的缺陷,达到保护数字版权的目的。此系统具有以下功能和特点:

1)采用实时虹膜识别系统,更有效地保护数字内容不被非法使用;

2)保证数字音视频内容和收费电视节目的安全出售和发布;

3)保证创作者和数字内容提供者在网上分发的所有版权;

4)使用数字内容的用户必须通过 DRM 识别和身份验证;

5)数字内容提供商能够通过改变相关变量和安全策略来保护系统。

3.1 自动虹膜识别方法

生物测定是一种使用身体或者个体特征的自动鉴别方法,本文采用自动实时虹膜识别系统方法来代替传统的密码技术。为了得到所需信息,用户必须向识别服务器发送经仔细检查的虹膜,图 1 给出了人眼的正面图。由于非法用户能够私自截获和存取虹膜数据,因此用户发送的虹膜代码信息必须经过安全转移协议处理后才能被存入数据库[9,10]。

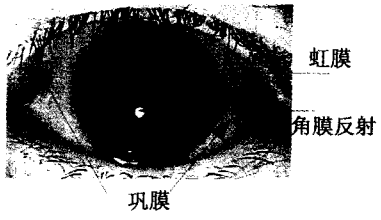

图 1 人眼正视图

当用户输入密码,系统将这个密码转变成了某域内可以实现认证的数字代码。这种方法较为可靠,因为即使那些恶意用户私自进入数据库,也不能截获有严格程序保护的加密信息。在新的 DRM 系统中,自动虹膜识别系统(AIRS)通过识别服务器和应用程序服务器来处理这个认证过程。

目前,虹膜识别技术已经取得了长足的发展,相应系统充分利用了虹膜识别模型的复杂性和稳定性,保证系统拥有很高的正确率。经典的虹膜识别算法是由 Daugman 教授提出的[11],很多虹膜识别系统就是以此算法为基础的。该算法分四个步骤进行:虹膜图像的定位,图像标准化,特征提取和匹配。相应的自动虹膜识别系统(AIRS)如图 2 所示。

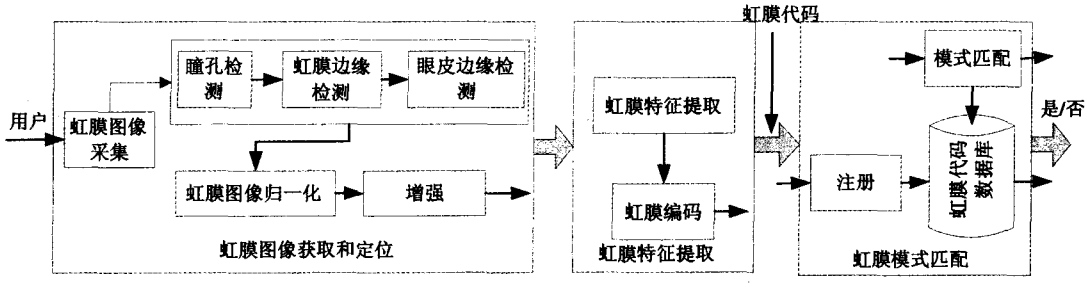

图 2 虹膜识别系统流程图

3.2 基于虹膜识别技术的 DRM 系统

3.2.1 DRM 系统流程

基于虹膜识别技术的 DRM 系统的流程如图 3 所示。此系统由数字内容提供商、消费者、应用程序服务器、AIRS 服务器组成。基于虹膜识别技术的 DRM 系统具体工作流程为:

1)用户通过与应用服务器联系得到数字内容的概要、数据权利和使用规则,并从应用程序服务器获得使用内容的许可;

2)为了实施认证,用户将 ID 和虹膜代码信息传送给服务器,应用程序服务器将信息发送给 AIRS 服务器;

3)AIRS 服务器搜索自身数据库找到相同且已注册的 ID 号。然后,通过把数据库中已存的虹膜和所提供的虹膜作比较,验证用户提供的虹膜代码信息的正确性,以判断此用户是

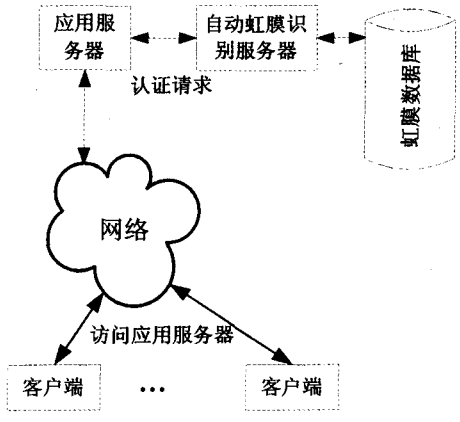

图 3 基于虹膜识别技术的 DRM 系统

否具有访问相应服务的权限，AIRS 服务器将鉴别结果发给应用程序服务器；

4)根据 AIRS 服务器鉴别的结果，应用程序服务器决定是否允许用户访问相关内容；

5)收到许可回复，合法用户就可以使用应用程序服务器中的数字内容；

6)当用户需要对数字权利进行处理时，所有的处理日志就会被记录在应用程序服务器中。

3.2.2 虹膜采集和提取特征

虹膜采集和特征提取是基于虹膜识别技术的 DRM 运作的第一步，具体的流程如图 4 所示。虹膜采集和特征提取程序主要包括与服务器的通信程序界面，自动定时程序，信息处理程序，特征提取程序。

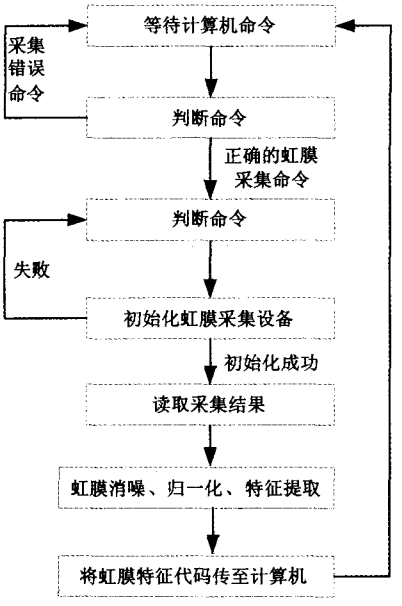

图 4 虹膜采集提取特征

3.2.3 用户终端

通过用户和服务器之间连接装置，用户获得服务器的随机码、证书，并检验服务器的合法性。然后，把已获取的虹膜特征传给服务器，等待服务器认证。如果失败，则再次索取随机码，把虹膜代码信息发送给服务器直到验证成功。用户终端的具体流程图如图 5 所示。

3.2.4 服务器终端

所有的操作都是基于用户终端和服务器之间的准确通信。由于要确保基于虹膜识别技术的 DRM 系统中的虹膜系统的性能，本系统选用经典的 Daugman 虹膜识别的算法[11]。

3.3 认证机理的描述

如何保护虹膜认证数据是一个关键问题，否则个人的隐私将受到破坏。我们提出了一种结合 PKI 的安全协议。在实施中，虹膜生物认证的特征数据和用户的证书一起被存储在一个智能卡中来减少风险。假定用户和服务器都拥有一对有效的公、私钥。

在初始化过程中，用户和服务器之间共享的信息有：大素数 p(包括大素因子 q)和群 G_p 的生成元。安全的单向哈希函数 H_1, H_2, H_3，对称加密的运算法则 $E_k(m)$，$D_k(m)$，签名运算 $Sig(m)$和验证算法，服务器的密钥 $x \in Z_p$ 和公钥 $y = g^x / p$。用户和服务器之间的协议如图 6 所示。

1)用户随机选择 $u \in Z_p$，并计算 $a = g^u \bmod p$

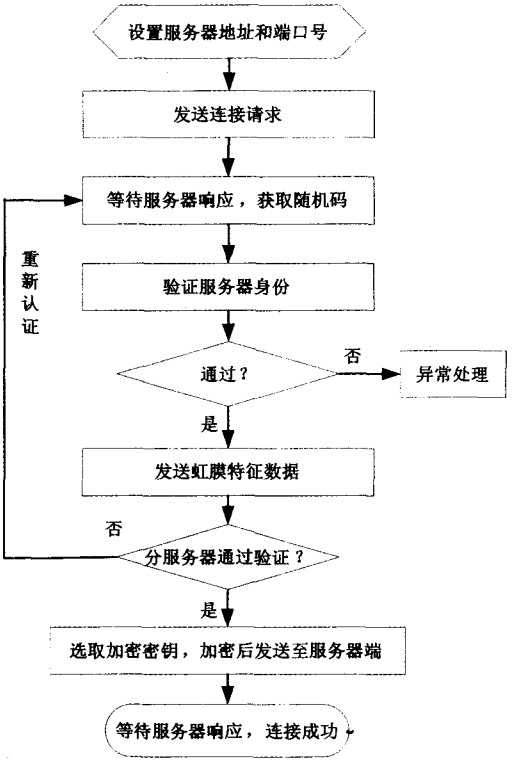

图 5 用户终端流程

2)当服务器接到以上信息，选择一个随机数 $r \in Z_p$，计算会话密钥 $K = H_1(a^x, r)$，然后计算 $b = H_2(K, r, V_{id})$，把$(b, r, CertV)$传输给用户。

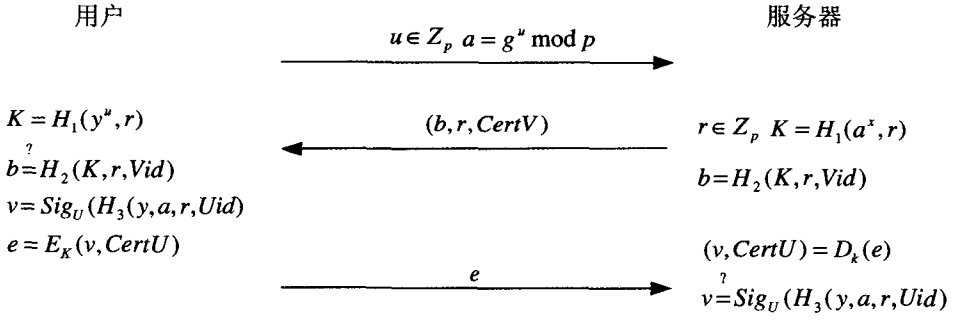

图 6 虹膜认证机理

3)当用户从服务器接收到信息后，从 $CertV$ 中提取得到 y。计算 $K = H_1(y^u, r)$，然后检验 $\overset{?}{b} = H_2(K, r, Vid)$ 是否正

确。如果正确，用户就确定服务器知道 K，从而认证服务器的身份。用户签名 $H_3(y,a,r,Uid)$，也就是 $v=Sig_U(H_3(y,a,r,Uid))$。用会话密钥加密 V 和公钥证书得到 $e=E_K(v,CertU)$，将加密结果 e 发送给服务器。

4)解密服务器通过解密 $(v,CertU)=D_k(e)$，获取 e。当公钥证书 $CertU$ 被检验是合法的，使用公钥 $v\stackrel{?}{=}Sig_U(H_3(y,a,r,Uid)$ 来验证用户的签名。

4 基于虹膜生物识别的 DRM 系统分析

4.1 性能

基于虹膜识别技术的 DRM 系统具有以下性能：

1)系统具备独特的设计和不同的技术分类。能够清楚表示出所执行指令和数字内容保护的详细内容；

2)系统拥有识别和监测非法用户的功能；

3)在线数字权利保护方案与离线的是一致的，并且具有统计分析功能；

4)系统具有钥匙管理功能。虹膜识别技术提供了一种保护合法用户获取访问权限的简单方法。

4.2 安全性分析

本文方案的安全性主要从以下方面考虑：

1)每次认证过程中，用户随机选择 $u\in Z_p$，并计算 $a=g^u \bmod p$，不同的 u 保证了协议认证消息的新鲜性，能够防止攻击者重放攻击；

2)尽管 $a=g^u \bmod p$ 是以明文形式发送给服务器，而任何人要从 a 中计算出 u 是计算上不可行的，这将面临着求解离散对数的困难性，从而能够实现对 u 的保密性；

3)如果攻击者对第 1 条消息进行恶意篡改，或者冒充合法用户发起认证过程，尽管在服务器端无法识别这种攻击，但当用户收到第 2 条消息后，通过验证可以发现这种攻击；

(4)如果攻击者对第 2 条和第 3 条消息进行恶意篡改，那么由于第 2 条和第 3 条消息使用了数字签名保护，因此，攻击者试图篡改消息而不被发现是不现实的。

通过以上分析，可以发现该认证协议充分考虑了消息的保密性、完整性和新鲜性，从而说明该协议是安全可行的。

结论 本文在虹膜识别技术和现有的 DRM 系统基础上，提出了一种安全的 DRM 系统模型，这种方法可安全地进行数字内容的分发。详细介绍了一种 AIRS 系统，这种系统用于对保护的内容建立接入控制。与现有文献中的方法不同的是本文提出的模型也给出了用于虹膜生物识别的认证协议，确保了系统的安全性。AIRS 促进了接入控制与内容之间的相互作用。本文提出使用 AIRS 识别机理来进行数字版权管理，这个思想的目的是要引入数据内容的保护措施，以便于只有经允许的用户能够存取制定的数据和登记他们的虹膜代码。如果未经允许的用户想要进入数字内容环境，AIRS 将起禁止作用。因此，使用这种具有不变性的 AIRS，能够公平地使用数字内容。

参 考 文 献

1 Federrath H. Scientific evaluation of DRM systems. [Online]. Available at: http://www.inf.tu-dresden.de/~hf2

2 Hartung F, Ramme F. Digital rights management and watermarking of multimedia content for m-commerce applications. IEEE Commun. Mag., Nov. 2000,38:78~84

3 Jain A K, Bolle R, Pankanti S. Biometrics-Persona Identification in Networkwed Society. Norwell, MA: Kluwer, 1999

4 Ortega-Garcia J, Gonzalez-Rodriguez J, Simon-Zorita D, et al, From biometrics technology to applications regarding face, voice, signature and fingerprint recognition systems. In: D. D. Zhang, ed. Biometric Solutions for Authentication in an E-World, Norwell, MA: Kluwer, July 2002. 289~337

5 Zhang D D. Biometrics Solutions for Authentication in an E-World. Norwell, MA: Kluwer, July 2002

6 Waller A O, Jones G, Whitley T, et al. Securing the delivery of digital content over the Internet. Electron. Comm. Eng. J., Oct. 2002, 14(5):239~248

7 Federrath H. Scientific evaluation of DRM systems. [Online]. Available at: http://www.inf.tu-dresden.de/~hf2

8 Ortega-Garcia J, Bigun J, Reynolds D, et at. Authentication gets personal with biometric. IEEE signal processing magazine, March 2004. 50~62

9 FAN Kefeng, MO Wei, WANG Meihua, et al. Human identification Technique based on Iris Feature Watermarking. Chinese Journal of Electronics, 2006(2):251~256

10 Wildes R P. Automated Iris Recognition: An Emerging Biometric Technology. Proceedings of the IEEE, 1997,85(9): 1348~1363

11 Daugman J. Recognizing persons by their iris patterns. In: K. Jain, et al., eds. Biometrics-Personal Identification in Networkwed Society, Norwell, MA: Kluwer, 1999. 103~121

(上接第 125 页)

无必然的关系，而是由其活跃时间来决定的。

致谢 本文所用数据由北京大学网络实验室肖明忠老师提供，在此表示非常感谢！

参 考 文 献

1 Adar E, Huberman B A. FreeRiding onGnutella [R]. www.hpl.hp.com/research/idl/papers/gnutella/gnutella.pdf

2 Hughes D, Coulson G. FreeRiding Riding on Gnutella Revisited: The Bell Tolls? [C]. IEEE Distributed Systems Online, 2005, 6(6)

3 Gummadi K P, Dunn R J, Saroiu S, et al. Measurement Modeling, and Analysis of a Peer-to-Peer File-Sharing Workload [C]. In: Proc. SOSP, Bolton Landing, NY, Oct. 2003

4 Saroiu S, Gummadi P, Gribble S. A measurement study of peer-to-peer file sharing systems [C]. In: SPIE Multimedia Computing and Networking, San Jose, CA, 2002. 156~170

5 Sen S, Wang J. Analyzing peer-to-peer traffic across large networks. IEEE/ACM Trans on Networking, 2004, 12(2): 219~232

6 Plissonneau L, Costeux J L, Brown P. Analysis of peer-to-peer traffic on ADSL [C]. In: Proc. of the PAM 2005. LNCS 3431, Heidelberg: Springer-Verlag, 2005

7 Goh S T, Kalnis P, Bakiras S. Real Datasets for File-Sharing Peer-to-Peer Systems [C]. In: 201-213, 10th International Conference, DASFAA 2005, Beijing, China

8 Liang J, Kumar R, Ross K W. The FastTrack overlay: a measurement study [C]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2006, 50(6):842~858

9 Tutschku K. A measurement-based traffic profile of the eDonkey filesharing service [C]. In: Proc. PAM'04, Juan-les-Pins, France, Apr. 2004. 12~21