基于虹膜识别的网络安全认证系统

符艳军[1]， 夏靖波[1]， 孙开锋[2]
(1. 空军工程大学 电讯工程学院，陕西 西安 710077;2. 西安精密机械研究所，陕西 西安 710075)

摘 要:随着信息技术的飞速发展,传统的身份验证已不能完全满足电子信息安全的要求,通过对几种生物特征识别的性能进行比较,结合信息加密技术,提出了一种基于虹膜识别的网络安全认证系统,该系统与现存的很多认证体系(如Kerberos认证系统)相比,多了一层对网络身份的识别功能,本文从理论上证明了该系统的安全性和可行性。

关键词:虹膜;生物特征识别;加密
中图分类号:TN393.08 **文献标识码**:A **文章编号**:1009-3516(2004)06-0060-03

现存的很多认证系统(如Kerberos认证系统)都只是对网络身份进行验证,即通过个人所知或所有的东西对身份进行验证,因此不能防范通过对口令的猜测或对凭证的伪造而进行的身份假冒攻击,而基于个人特征如指纹、笔迹、声纹、手型、脸型、血型、视网膜、虹膜等活体自身固有属性的身份识别却能很好地克服这一缺陷[1]。目前,对虹膜识别系统的研究大多是单机系统的,因此,设计开发具有网络功能的身份识别认证系统具有非常广阔的应用前景。

1 虹膜识别系统

利用生物特征进行身份识别的研究刚刚起步,由于虹膜自身的生物特点,近几年来虹膜识别技术有了很大的发展。与其它生物特征相比,虹膜具有以下特点:①虹膜具有随机的细节特征和纹理图象,且这些特征在人的一生中保持相当高的稳定性;②虹膜具有内在的隔离和保护能力;③在不冒影响视力危险的情况下,难以通过手术修改虹膜的结构;④虹膜图象可以通过相隔一定距离的摄象机捕获而不须对人体进行侵犯。

虹膜识别技术在各个性能指标上都有明显的优势,其普适性[2-3]、独特性、稳定性、非入侵性和防欺骗性等性能都很好,由于受到眼睑或眼白等的遮挡,其可采集性指标不是很高,但总的性能仍然很高。据统计,虹膜识别的错误率是各种生物特征识别中最低的,根据仿真实验结果[4],在160个虹膜样本的实验中,总识别率可达93.8%以上。

虹膜识别一般包括图象采集、预处理、虹膜纹理编码、模式匹配等步骤。

眼部图象采集可通过CCD摄象头及图象采集卡输入计算机。为了提高图象对比度,有时也采用LED辅助光源;在对原始图象进行预处理时,首先要对虹膜进行定位,即精确确定虹膜的内外边界,准确地隔离出虹膜,并对虹膜图象进行校准,消除图象采集过程中出现的漂移、旋转及放缩等造成的偏差;在提取出虹膜图象后,用同态滤波增晰的方法对虹膜图象进行增强处理,使虹膜具有明显的、可区别的各种模式特征,并利用一系列Gabor滤波器对虹膜图象进行分解,从中提取编码信息。模式匹配是虹膜识别的关键,是把当前要识别身份的虹膜特征信息与已有的样本库中的虹膜特征信息作比较进行模式识别,最后作出相应的决策。

收稿日期:2004-07-01
基金项目:国家"863"计划基金资助项目(2002AA143020)
作者简介:符艳军(1972-),女,陕西兴平人,讲师,硕士,主要从事网络安全技术研究;
夏靖波(1963-),男,河北秦皇岛人,教授,博士生导师,主要从事网络管理及网络安全技术研究.

2　结合虹膜识别和加密技术的网络认证系统

2.1　生物特征系统及其子系统

在 ANSI X9.84 生物特征信息管理与安全标准中,将一个生物特征系统分成数据采集、信号处理、存储、匹配及传输等 5 个子系统。这 5 个子系统独立工作,相互之间不受影响,整个系统的安全性是通过保证各个子系统的安全来实现的。

数据采集子系统主要完成生物特征信息的采集。在该子系统中,应保证生物特征获取装置检测的是真正的用户特征,而不是照片或者记录,防止生物特征信息被篡改或替换;信号处理子系统主要完成图像预处理和特征提取等数字信号处理工作;存储子系统的任务是保存注册的用户模板,其安全性主要是防止恶意者对数据的破坏、盗用、篡改等;匹配子系统利用信号处理子系统输出的生物特征进行匹配判决;而传输子系统将其他 4 个子系统连接在一起,实现系统的信息流通,其安全方面的任务是防止传输过程中遭受未被授权者的恶意攻击,包括对传输数据的干扰、截取等。

因此,在开放的网络上,要设计一个基于生物特征的安全的网络身份认证系统,应该把加密技术和认证系统结合起来,对于存储和传输的数据,应使用高级加密工具来保障数据信息的安全。

2.2　基于三方认证的虹膜识别系统

为了有效地把加密技术和认证技术相结合,目前,在认证安全机制方面,比较流行的方法是引入可信第三方[5-6],把整个认证过程分成虹膜识别系统和三方认证系统两个逻辑系统,这两个系统相互渗透、同时工作,其中虹膜识别系统的安全由三方认证系统来保证。三方认证系统的结构如图 1 所示。

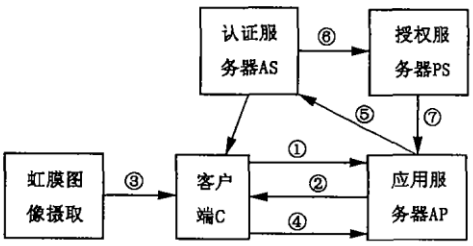

图 1　基于三方认证的虹膜识别系统结构图

假设在三方认证系统中,认证服务器 AS 为可信第三方,即客户端 C、授权服务器 PS 和应用服务器 AP 都信任 AS,并且都和 AS 有共享密钥,分别为 K_{C-AS}、K_{P-AS}、和 K_{A-AS}。AS 利用虹膜特征信息和加密技术提供安全认证,确保客户端 C 用户请求的有效性。如果认证被通过,授权服务器 PS 负责向应用服务器 AP 证明用户所拥有的权限,最后由应用服务器 AP 向用户提供应用服务。其中 PS 和 AP 都有自己的公私钥对,分别记为(K_{PSU}, K_{PSR})、(K_{APU}, K_{APR}),客户端 C 实现虹膜图像的特征提取功能。下面详细叙述该认证系统的认证过程。

设 EK 表示用密钥 K 进行加密, DK 表示用密钥 K 进行解密,其过程如下:

1)客户端 C 向应用服务器 AP 发出请求,希望得到某种服务;

2)应用服务器 AP 回应 C,要求客户端 C 提交虹膜特征信息;

3)客户端 C 从摄取的虹膜图象中提取特征信息;

4)客户端 C 向应用服务器 AP 发送包含虹膜特征信息 ID_{IRIS}、身份 ID_C 和所请求的服务类型信息 S。为了保证自己的 ID_{IRIS} 不泄露给 AP,C 首先用其与 AS 的共享密钥 K_{C-AS} 对 ID_{IRIS} 及 S 进行 DES 加密,即: $C_1 = EK_{C-AS}(ID_{IRIS}, S)$。为了保证所有信息在传输过程中的安全,客户端 C 用 AP 的公钥 K_{APU} 对信息 C_1、ID_C 及服务类型信息 S^*(为了与 C_1 中的 S 相区分) 进行 RSA 加密。即 C 最终传给 AP 的加密信息 C_2 为

$$C_2 = EK_{APU}(C_1, ID_C, S^*) = EK_{APU}(EK_{C-AS}(ID_{IRIS}, S), ID_C, S^*)$$

5)应用服务器 AP 把从客户端 C 传来的加密信息用自己的私钥 K_{APR} 进行解密,即:

$$DK_{APR}(C_2) = DK_{APR}(EK_{APU}(EK_{C-AS}(ID_{IRIS}, S), ID_C, S^*)$$

得到 $C_1 = EK_{C-AS}(ID_{IRIS}, S)$、$ID_C$ 和 S^* 3 个信息,并通过获得的明文 S^* 验证客户端 C 所请求服务类型的有效性,若有效,AP 向认证服务器 AS 提交信息 C_1、ID_C 及服务类型信息 S^*,并且要向 AS 证明自己参与了这次通信。为此,AP 首先对信息 C_1 用自己的私钥 K_{APR} 进行 RSA 数字签名,得:

$$C_3 = EK_{APR}(EK_{C-AS}(ID_{IRIS}, S))$$

最后再用其与 AS 的共享密钥 K_{A-AS} 对 C_3、ID_C、信息 S^* 及 AP 本身的识别号 ID_{AP} 进行 DES 加密。AP 最终传给 AS 的加密消息 C_4 为

2　结合虹膜识别和加密技术的网络认证系统

2.1　生物特征系统及其子系统

在 ANSI X9.84 生物特征信息管理与安全标准中,将一个生物特征系统分成数据采集、信号处理、存储、匹配及传输等 5 个子系统。这 5 个子系统独立工作,相互之间不受影响,整个系统的安全性是通过保证各个子系统的安全来实现的。

数据采集子系统主要完成生物特征信息的采集。在该子系统中,应保证生物特征获取装置检测的是真正的用户特征,而不是照片或者记录,防止生物特征信息被篡改或替换;信号处理子系统主要完成图像预处理和特征提取等数字信号处理工作;存储子系统的任务是保存注册的用户模板,其安全性主要是防止恶意者对数据的破坏、盗用、篡改等;匹配子系统利用信号处理子系统输出的生物特征进行匹配判决;而传输子系统将其他 4 个子系统连接在一起,实现系统的信息流通,其安全方面的任务是防止传输过程中遭受未被授权者的恶意攻击,包括对传输数据的干扰、截取等。

因此,在开放的网络上,要设计一个基于生物特征的安全的网络身份认证系统,应该把加密技术和认证系统结合起来,对于存储和传输的数据,应使用高级加密工具来保障数据信息的安全。

2.2　基于三方认证的虹膜识别系统

为了有效地把加密技术和认证技术相结合,目前,在认证安全机制方面,比较流行的方法是引入可信第三方[5-6],把整个认证过程分成虹膜识别系统和三方认证系统两个逻辑系统,这两个系统相互渗透、同时工作,其中虹膜识别系统的安全由三方认证系统来保证。三方认证系统的结构如图 1 所示。

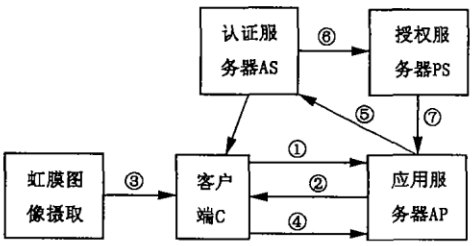

图 1　基于三方认证的虹膜识别系统结构图

假设在三方认证系统中,认证服务器 AS 为可信第三方,即客户端 C、授权服务器 PS 和应用服务器 AP 都信任 AS,并且都和 AS 有共享密钥,分别为 K_{C-AS}、K_{P-AS}、和 K_{A-AS}。AS 利用虹膜特征信息和加密技术提供安全认证,确保客户端 C 用户请求的有效性。如果认证被通过,授权服务器 PS 负责向应用服务器 AP 证明用户所拥有的权限,最后由应用服务器 AP 向用户提供应用服务。其中 PS 和 AP 都有自己的公私钥对,分别记为(K_{PSU},K_{PSR})、(K_{APU},K_{APR}),客户端 C 实现虹膜图像的特征提取功能。下面详细叙述该认证系统的认证过程。

设 EK 表示用密钥 K 进行加密, DK 表示用密钥 K 进行解密,其过程如下:

1)客户端 C 向应用服务器 AP 发出请求,希望得到某种服务;

2)应用服务器 AP 回应 C,要求客户端 C 提交虹膜特征信息;

3)客户端 C 从摄取的虹膜图象中提取特征信息;

4)客户端 C 向应用服务器 AP 发送包含虹膜特征信息 ID_{IRIS}、身份 ID_C和所请求的服务类型信息 S。为了保证自己的 ID_{IRIS}不泄露给 AP,C 首先用其与 AS 的共享密钥 K_{C-AS}对 ID_{IRIS}及 S 进行 DES 加密,即:$C_1 = EK_{C-AS}(ID_{IRIS},S)$。为了保证所有信息在传输过程中的安全,客户端 C 用 AP 的公钥 K_{APU}对信息 C_1、ID_C及服务类型信息 S^*(为了与 C_1中的 S 相区分) 进行 RSA 加密。即 C 最终传给 AP 的加密信息 C_2为

$$C_2 = EK_{APU}(C_1, ID_C, S^*) = EK_{APU}(EK_{C-AS}(ID_{IRIS}, S), ID_C, S^*)$$

5)应用服务器 AP 把从客户端 C 传来的加密信息用自己的私钥 K_{APR}进行解密,即:

$$DK_{APR}(C_2) = DK_{APR}(EK_{APU}(EK_{C-AS}(ID_{IRIS}, S), ID_C, S^*)$$

得到 $C_1 = EK_{C-AS}(ID_{IRIS},S)$ 、ID_C和 S^*3 个信息,并通过获得的明文 S^*验证客户端 C 所请求服务类型的有效性,若有效,AP 向认证服务器 AS 提交信息 C_1、ID_C及服务类型信息 S^*,并且要向 AS 证明自己参与了这次通信。为此,AP 首先对信息 C_1用自己的私钥 K_{APR}进行 RSA 数字签名,得:

$$C_3 = EK_{APR}(EK_{C-AS}(ID_{IRIS}, S))$$

最后再用其与 AS 的共享密钥 K_{A-AS}对 C_3、ID_C、信息 S^*及 AP 本身的识别号 ID_{AP}进行 DES 加密。AP 最终传给 AS 的加密消息 C_4 为

$$C_4 = EK_{A-AS}(C_3, ID_C, S^*, ID_{AP}) = EK_{A-AS}(EK_{APR}(EK_{C-AS}(ID_{IRIS}, S)), ID_C, S^*, ID_{AP})$$

6)认证服务器 AS 收到加密信息 C_4后,首先用其与 AP 的共享密钥 K_{A-AS}进行解密,得:

$$DK_{A-AS}(C_4) = DK_{A-AS}(EK_{A-AS}(EK_{APR}(EK_{C-AS}(ID_{IRIS}, S)), ID_C, S^*, ID_{AP}))$$

从而得到 C_3, ID_C, S^*, ID_{AP} 4 个信息,AS 再根据 ID_{AP}用 AP 的公钥 K_{APU}对 C_3解密,获得信息 C_1,即

$$C_1 = EK_{APU}(C_3) = ED_{APU}(EK_{APR}(EK_{C-AS}(ID_{IRIS}, S))) = EK_{C-AS}(ID_{IRIS}, S) = C_1$$

最后通过已经获得的 ID_C查阅他们的共享密钥 K_{C-AS},对 C_1进行解密得用户的虹膜特征信息 ID_{IRIS}和服务类型信息 S,比较 S 与 S^*是否一致来判断是否发生了篡改,将 ID_{IRIS}与系统中原有的模板数据库进行匹配,并把匹配判断结果 Result (包含用户 ID_C)分别发送给客户端 C 及授权服务器 PS。

AS 在给客户端 C 及授权服务器 PS 发送信息时,分别使用 AS 与他们的共享密钥进行加密。即:

AS 向客户端 C 发送的加密信息为:$C_6 = EK_{C-AS}(\text{Result})$;AS 向 PS 发送的加密信息为:$C_7 = EK_{P-AS}(\text{Result}, S)$。

7)授权服务器 PS 收到信息 C_7,用其与 AS 的共享密钥 K_{P-AS}解密获得认证结果 Result 及服务类型信息 S,针对用户请求的服务,产生服务授权票据 Ticket,此票据包含用户 ID_C、对服务的使用权限、时戳和生存周期。PS 应将此票据送往应用服务器 AP 告知此次认证的结果,同样 PS 应向 AP 证明自己的身份并确保票据在传输过程中的安全性,因此 PS 对此票据进行 RSA 数字签名。即授权服务器 PS 发送给 AS 的加密信息 C_8为:$C_8 = EK_{PSR}(\text{Ticket}, S)$。

应用服务器 AP 收到信息 C_8并进行解密,可获得票据 Ticket 和服务信息 S,进而为客户端提供相应的服务。

3 结论

把虹膜识别技术、加密技术和三方认证系统相结合所设计的网络身份认证系统,在理论上可以很好地上实现对身份的安全识别。一方面,对于用户而言,能够确保服务提供方的可信性,假冒者不可能伪装成服务提供方而达到非法目的,同时能够确保用户私有的虹膜信息在整个通信过程中的保密性;另一方面,对于服务提供方而言,服务提供方能够确信它把服务提供给了一个合法的授权者,即用户是可信的,它给用户提供的服务等级和用户的身份是相符的。

参考文献:

[1] 王育民,刘建伟. 通信网的理论与安全[M]. 西安:西安电子科技大学出版,1999.
[2] 付 鹏,裘正定. 生物特征识别技术及相关问题综述[J]. 中国数据通信,2003,(3):10-14.
[3] 李雄军,苏廷弼. 基于生物特征的 AUTO ID 技术——BioID[J]. 计算机工程与应用,2002,(16):. 88-89.
[4] 王蕴红,朱 勇,谭铁牛. 基于虹膜识别的身份鉴别[J]. 自动化学报,2002,28(1):38-42.
[5] Jain A K, Hong L, Pananli S,et al. An Identity Authentication System Using Fingerprints[J]. Proceedings of The IEEE,1995, 83:705-740.
[6] 孙冬梅,裘正定. 生物特征识别技术综述[J]. 电子学报,2001,29(12):1744-1747.

(编辑:门向生)

Network Security Authentication System Based on Iris - Identification

FU Yan-jun[1], XIA Jing-bo[1], SUN Kai-feng[2]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China; 2. Xi'an Precision Machinery Research Institute, Xi'an, Shaanxi 710075, China)

Abstract: With the rapid development of information technology, the traditional technology of identity - verification can not meet the requirements of electrical information security. This paper presents a trusted third party authentication system, which can provide a function of network authentication with very high security. The system is based on Iris - identification and is superior to other biometrics in respect of personal identification.

Key words: iris; biometric personal identification; encryption