



专题:智能终端与网络安全

基于生物特征和混沌映射的多服务器身份认证方案

章坚武,姚泽瑾,吴震东

(杭州电子科技大学,浙江 杭州 310018)

摘要:基于密码的用户远程认证系统已被广泛应用,近年来的研究发现,单一口令系统容易遭受字典分析、暴力破解等攻击,安全性不高。生物特征与密码相结合的认证方式逐渐加入远程认证系统中,以提高认证系统的安全水平。但现有认证系统通常工作在单一服务器环境中,扩展到多服务器环境中时会遇到生物特征模板和密码容易被单点突破、交叉破解的问题。为了克服以上问题,提出了一种基于生物特征和混沌映射的多服务器密钥认证方案,该方案基于智能卡、密码和生物特征,可明显提高多服务器身份认证系统的安全性及抗密码猜解的能力。

关键词:远程认证;生物特征;多服务器

中图分类号:TP393

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2017045

Multi-server identity authentication scheme based on biometric and chaotic maps

ZHANG Jianwu, YAO Zejin, WU Zhendong

Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: Password-based user remote authentication system has been widely used in recent years, the study found that a single password system is so vulnerable to dictionary analysis and brute force attack as well as other attacks that the security is not high. Biometric and password combination authentication method gradually added to the remote authentication system in order to improve the security level of authentication system. However, the existing authentication systems work in a single server environment, if extended to a multi-server environment, biometric templates and passwords will encounter single point breakthrough and cross-crack problem. In order to overcome the above problems, a multi-server key authentication scheme based on biometric and chaotic map was proposed. The scheme was based on smart cards, passwords and biometrics, which could significantly improve the security and the ability of anti-password guessing of multi-server authentication systems.

Key words: remote authentication, biometrics, multi-server

收稿日期:2017-01-22;修回日期:2017-02-13

基金项目:浙江省自然科学基金资助项目(No.LY16F020016);国家重点研发计划经费资助项目(No.2016YFB0800201);浙江省重点科技创新团队项目(No.2013TD03)

Foundation Items: Zhejiang Natural Science Foundation of China(No.LY16F020016), National Key Research and Development Program of China(No.2016YFB0800201), Zhejiang Province Science and Technology Innovation Program (No.2013TD03)

1 引言

近年来,无线通信和无线网络快速发展,人们越来越多地使用移动设备(如移动电话、手提电脑等)随时随地地接入各种各样的网络服务,如网络存储、网页浏览和音乐视频等。

网络服务需要远端认证机制保护合法用户的安全性,避免用户越权访问非授权服务。基于智能卡的远端认证机制是目前最简单也是最便捷的保护网络安全性的认证方式。1981年Lamport首先提出基于可靠信道的密码认证系统,该方案服务器需要保存密码列表,不能预防盗窃攻击。参考文献[1,2]中提出了改进的基于密码的远程认证方式,以防止盗窃攻击,但这种方式因为密码本身的低熵性,仍然容易遭受字典攻击,因此越来越多的研究者将用户的生物特征(例如指纹、虹膜等)结合密码以及智能卡设计验证系统,以提高安全性。参考文献[3]中提出了基于3种特征的认证系统,并验证了其安全性。参考文献[4-12]对结合生物特征信息的认证系统进行了研究,研究限于单服务器环境,对多服务器环境没有涉及。而大量跨域网络服务的出现,使得多服务器身份认证技术受到重视。图1描述的是一个多服务器接入框架,图1中表明用户只需注册一次,就能访问网络中各种各样的服务器。参考文献[13]对多服务器密钥管理方案进行了研究,提出了基于椭圆曲线加密(ECC)的轻量级密钥管理方案,方案不涉及基于生物特征的身份认证。参考文献[14]中提出了一种利用椭圆曲线加密的方法,然而在参考文献[15]指出椭圆曲线加密在非法

者获得智能卡和密码的情况下仍然能模仿用户登录。参考文献[16]中提出结合多种信息的匿名多服务器的认证方法。参考文献[17,18]中指出该方法容易受到服务器欺骗和拒绝访问攻击,且不为用户信息和会话密钥做任何的保护,并且提出了自己的改进方案。参考文献[19]对参考文献[17,18]所提方案的弱点进行了分析,指出方案尚不能很好地防止欺骗攻击。虽然密钥作为常用的加密方法,但是人类记忆密钥有明显的低熵性缺点,容易被破解。生物特征具有唯一、不易模仿、随身携带等特性,使得其成为当前研究的热点。

从上述分析中可以看出,设计一个安全的多服务器认证仍然是一个挑战。本文提出一个基于生物特征的混沌映射认证模型。该模型采用人脸—智能卡—密码认证方法。在人脸扫描之后立即对图片进行混沌映射,使之完全不具备人脸信息,进行加密传输。当把人脸图片上传到注册中心验证时,根据密钥进行解密,之后用人脸识别模型进行训练,保存训练后的匹配模板。从而,即使训练好的模板泄露,盗窃者也无法得到用户的有用信息,极大地提高了安全性。在人脸识别的过程,本文采用深度学习的方法,使用卷积神经网络(convolutional neural network, CNN)模型。

2 模型建立

2.1 混沌映射

混沌是一个非线性系统产生的伪随机序列的过程,它是非周期性的,且对初始值极端敏感^[20],一般混沌模型为:

$$X(n)=f(x(n-1)) \quad (1)$$

其中, $f(\cdot)$ 是映射模型, $x(n)$ 是由映射模型产生的伪随机序列。

混沌系统表现为对初始值和系统参数的敏感性、白噪声的统计特性和混沌序列的遍历特性,其吸引子具有十分复杂的分形结构,具有不可预测性。因此,基于混沌的保密技术被广泛应用于通信数据保密以及图像加密等众多领域。在本文中使用Logistic混沌映射方法,对输入的人脸图片进行加密。

Logistic混沌映射拥有良好的随机性以及简单的表达式,应用相当广泛,该表达式表示为:

$$x(n+1)=f(x(n))=\lambda \cdot x(n) \cdot (1-x(n)) \quad (2)$$

其中, $0 < x(n) < 1, n=1,2,3, \dots$,研究表明, $3.569 \leq \lambda \leq 4$ 时表现出混沌状态。混沌映射在加密过程中使用一个密

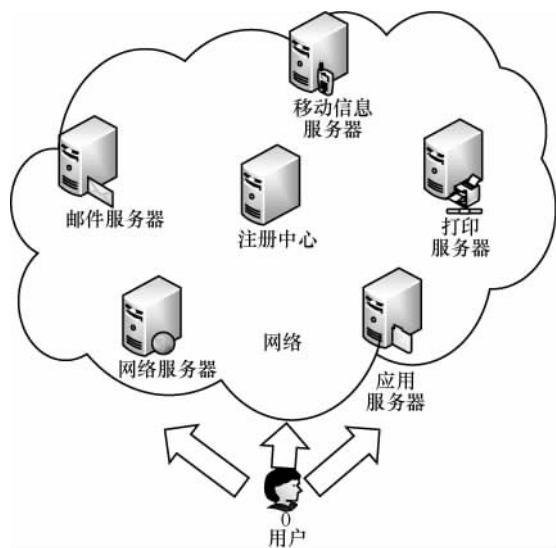


图1 用户接入多服务器服务

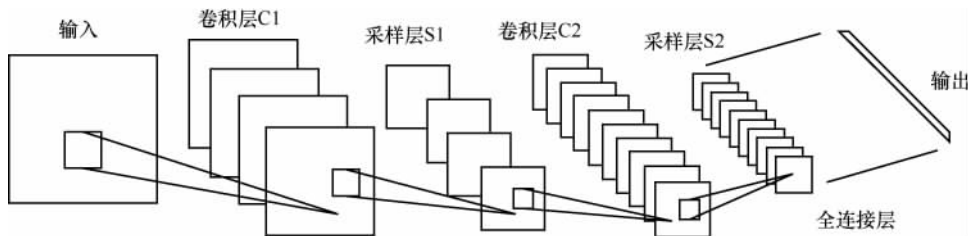


图2 卷积神经网络模型结构

钥,对应于解密使用的就是加密的密钥,由于盗窃者无法获得加密密钥,从而无法对加密后的图片正确解密,无法获得原图信息,使用混沌映射大大提高了图片的安全性。

2.2 卷积神经网络

在该系统中,本文采用人脸作为验证的生物特征。训练的人脸模型采用卷积神经网络。卷积神经网络是人工神经网络的一种,通过局部感受和权值共享减少了神经网络训练所需的参数个数,它的权值共享更类似于生物神经网络,降低了模型的复杂度。在图像识别领域,可直接选择图像作为输入,避免了传统识别算法中复杂的特征提取,同时这种网络结构对图像的平移、缩放和其他形变具有更好的顽健性。

2.2.1 卷积神经网络模型

卷积神经网络是一个多层模型,该多层模型由卷积层、池化层以及全连接层按一定顺序组合而成,如图2所示。

在神经网络的模型中,首先输入图像与一个卷积核进行卷积,输出第一个卷积层C1,每个卷积层中都有一定数量的特征图,特征图的每一个神经元与上一层的局部特征相连,通过卷积使原图中的某些特征得到加强,同时可以降低噪音干扰。卷积层之后紧接着一个池化层,该层作用是对图像进行降维,有3种池化方法:一般池化、重叠池化和空间金字塔池化。一般池化又分为平均池化和最大池化,在本文的模型中采用最大池化,若卷积核为2 dpi×2 dpi,则选取该区域最大的数作为池化

后的值,如图3所示。之后每层重复上述卷积过程,每层的卷积核可变。

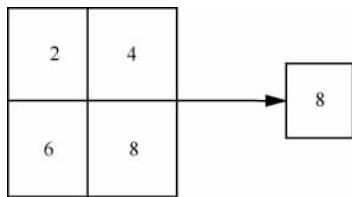


图3 最大池化

在卷积神经网络模型中,相连两层的神经元不是全连接的,全连接层除外。卷积神经网络中的神经元不需要感受全局图像,而是只感受图像的局部区域,这样的操作一直持续到最高层,这些局部感受的神经元结合到一起得到全局信息。局部感受的优势在于可以减少神经网络训练的权值参数个数。

2.2.2 人脸识别模型

卷积神经网络的人脸识别模型如图4所示,系统模型直接输入原始图片进行训练,输入图片的大小设为40 dpi×40 dpi,这是一个8层模型,包含4个卷积层、3个池化层以及1个全连接层。在第一个卷积层(C1)中,特征图的数量为20,尺寸为28 dpi×36 dpi,每个神经元与输入的4 dpi×4 dpi 邻域相连。C1有340个可训练参数(每个滤波器4×4=16个核参数和1个偏置参数,共20个滤波器,共(4×4+1)×20=340个参数),共340×(28×36)=342 720个连接。池化层pool1,选择池化大小为2 dpi×2 dpi,即对应于C1

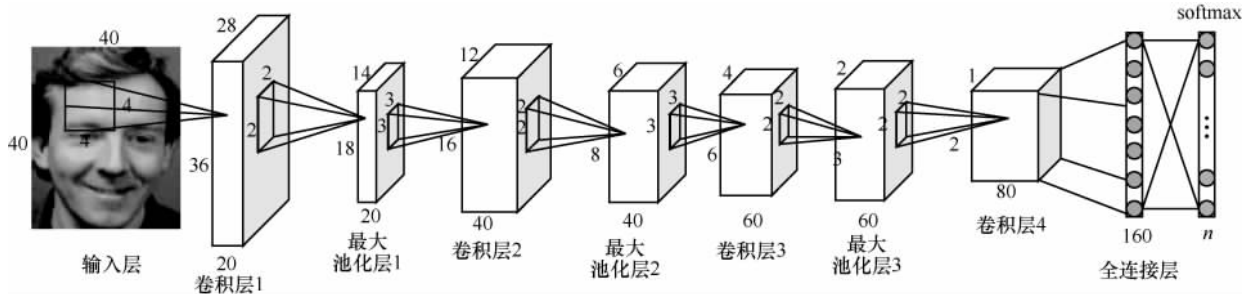


图4 人脸识别 CNN 模型

中的 $2 \text{ dpi} \times 2 \text{ dpi}$ 邻域, 选取 4 个值中的最大值作为采样后的结果, 从而使特征图大小变为原来的 $1/4$, 减少了训练参数。

C2 是由 pool1 与大小为 $3 \text{ dpi} \times 3 \text{ dpi}$ 的卷积核得到, 拥有 40 个特征图, 每个大小为 $12 \text{ dpi} \times 16 \text{ dpi}$ 。池化层 pool2, 仍然选择池化大小为 $2 \text{ dpi} \times 2 \text{ dpi}$, 从而有 80 个可训练参数 (每个特征图 1 个因子和 1 个偏置) 和 9 600 个连接。C3 由 pool2 与大小为 $3 \text{ dpi} \times 3 \text{ dpi}$ 的卷积核得到, 拥有 60 个特征图, 每个大小为 $4 \text{ dpi} \times 6 \text{ dpi}$ 。C4 有 80 个特征图, 大小为 $1 \text{ dpi} \times 2 \text{ dpi}$, C4 之后连接 1 个全连接层, 生成 160 维向量, 然后利用分类器进行判别。

3 基于混沌—生物特征的多服务器认证

3.1 系统方案设计

3.1.1 需求分析

服务器的设计一般根据用户需求以及安全性两部分进行考虑。对于用户而言首先要匿名, 保证真实信息不被透露, 密码的设置以及修改操作简单, 登录方便, 在一个多服务器环境下无需进行重复的注册, 仅注册一次就可实现各服务器之间的登录。对服务器而言, 安全性是一个必须考虑的问题, 在保证安全的情况下要求提高效率。在传统的认证方式基础上本文采用结合人脸识别的认证方式, 即采用智能卡—密码—人脸识别的认证方式, 增强系统的安全性。

3.1.2 系统设计

系统设计主要分为 3 个部分, 分别为注册中心、服务器和用户 (含智能卡), 大致流程如图 5 所示。首先, 服务器

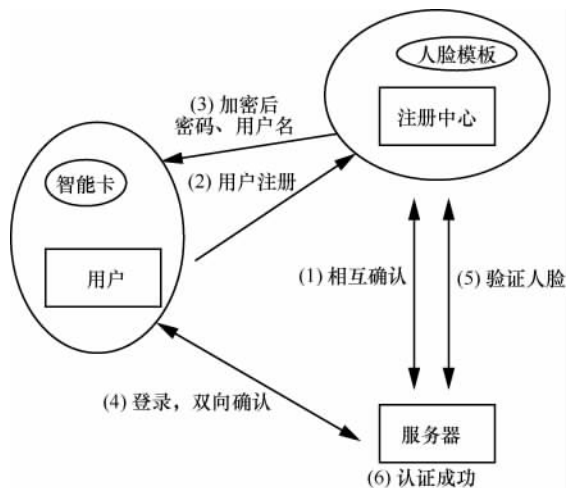


图5 方案设计流程

注册阶段要向注册中心申请授权为合法服务器, 两者之间会产生一对会话密钥。其次, 用户向注册中心注册, 并把人脸模板保存在注册中心中, 密码用户名则保存在智能卡中。当前两步完成之后用户才可以进行登录访问, 在认证登录时, 人脸识别在注册中心进行, 而用户与服务器之间要进行双向的认证, 所有认证项都符合, 则为合法用户, 可访问服务器资源。

3.2 服务器注册阶段

当一个服务器想成为授权服务器时, 首先向注册中心发送一个消息请求, 然后注册中心返回服务器一个预共享密钥 (PSK), 该服务器使用该密钥完成接下来的用户认证过程。

3.3 用户注册过程

首先, 假设经过一系列的加密用户注册信道是一个可靠的信道, 预共享密钥在注册中心和授权服务器之间不能被提取。图 6 表示了用户注册的过程。具体过程如下。

步骤 1 用户→注册中心。用户将自己的账号 (ID_i)、密码以及人脸图片 ($h(PW_i)$ 、 FAC_i) 通过可靠的信道传递给注册中心。在这过程中, 采集完人脸图片之后立即对图片进行混沌映射, 加密后的图片信息再传递给注册中心。

步骤 2 注册中心收到信息后, 利用密钥对混沌之后的人脸图片进行解密, 然后输入 CNN 中进行训练, 训练好的模型保存在注册中心。对其他信息进行如下加密: $A_i = h(ID_i || x)$, $B_i = h^2(ID_i || x)$, $C_i = h(PW_i) \oplus B_i$, $D_i = PSK \oplus A_i$, 其中 x 是注册中心的机器指纹。

步骤 3 注册中心返回用户。在注册中心把这些内容进行加密之后, 把生成的参数 (ID_i 、 B_i 、 C_i 、 D_i 、 $h()$) 通过可靠信道传输, 保存到智能卡中。

在注册中心不保存用户的信息 (例如密码和人脸信息), 能够防止盗窃攻击和内部攻击。另外, 注册的用户不能伪造合法用户的信息, 即使拥有这些参数 (ID_i 、 B_i 、 C_i 、 D_i 、 $h()$), 这是因为, 使用者不知道注册中心的机器指纹 (例如

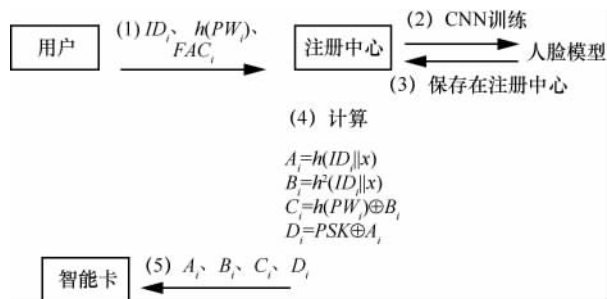


图6 用户注册流程



硬盘序列号)以及预共享密钥(PSK)。

3.4 登录过程

登录系统是验证的第一步,当使用者的密码或者用户名错误时智能卡能立即发现,登录过程如图7所示。

步骤1 使用者把智能卡插入卡槽中,卡槽读取用户的用户名以及密码,然后利用扫描器扫描人脸输入系统中。

步骤2 智能卡核对 $h(PW_i \oplus BIO_i) \oplus C_i$ 与 B_i 是否相等,如果验证符合,则智能卡产生一个随机数 N_1 ,然后计算 $M_1 = h(B_i) \oplus C_i$, $M_2 = h(N_1 || D_i)$,当中的 B_i, C_i 已经存在注册过程。

3.5 鉴权过程

经过上述的登录过程,首先通过了智能卡的第一轮验证,然后智能卡把验证消息发给多个服务器,具体过程如下。

步骤1 智能卡→服务器。智能卡把验证消息中经过混沌后的人脸发送到服务器,服务器把人脸信息传给注册中心,注册中心对加密图片解密后进行匹配,若成功则返回随机数 N_2 。

步骤2 服务器验证用户。当服务器接收到验证请求

消息时,先利用预共享密钥获得加密的用户信息 A_i ,其中 $A_i = D_i \oplus PSK$,然后重新计算获得智能卡生成的随机数 N_1 ,其中 $N_1 = M_1 \oplus h^2(A_i)$,然后判断 $h(N_1 || D_i)$ 是否成立,计算 $SK_g = h(N_1 || N_2)$,最后服务器计算 $M_3 = N_2 \oplus h^2(N_1)$ 和 $M_4 = h(SID_j || N_2)$ 。

步骤3 服务器返回 SID_j, M_3, M_4 到智能卡。

步骤4 智能卡确认该服务器的合法性。计算 $h^2(N_1)$,接收服务器产生的随机数 N_2 ($N_2 = M_3 \oplus h^2(N_1)$),然后判断 $h(SID_j || N_2) = M_4$ 是否相等,若相等则计算 $SK_g = h(N_1 || N_2)$,否则直接认证失败。

步骤5 智能卡将 $SK_g \oplus h(N_2)$ 发送给服务器。

步骤6 核对 $h(N_2)$,若符合则验证成功,用户成功访问。

3.6 密码修改过程

因为密码的信息是保存在智能卡中的,因此修改密码只需要修改智能卡中的信息即可。保存在注册中心的人脸信息在修改时作为一个认证项,保证该用户是合法用户,并不对该部分信息进行修改。修改密码过程,用户只要把验

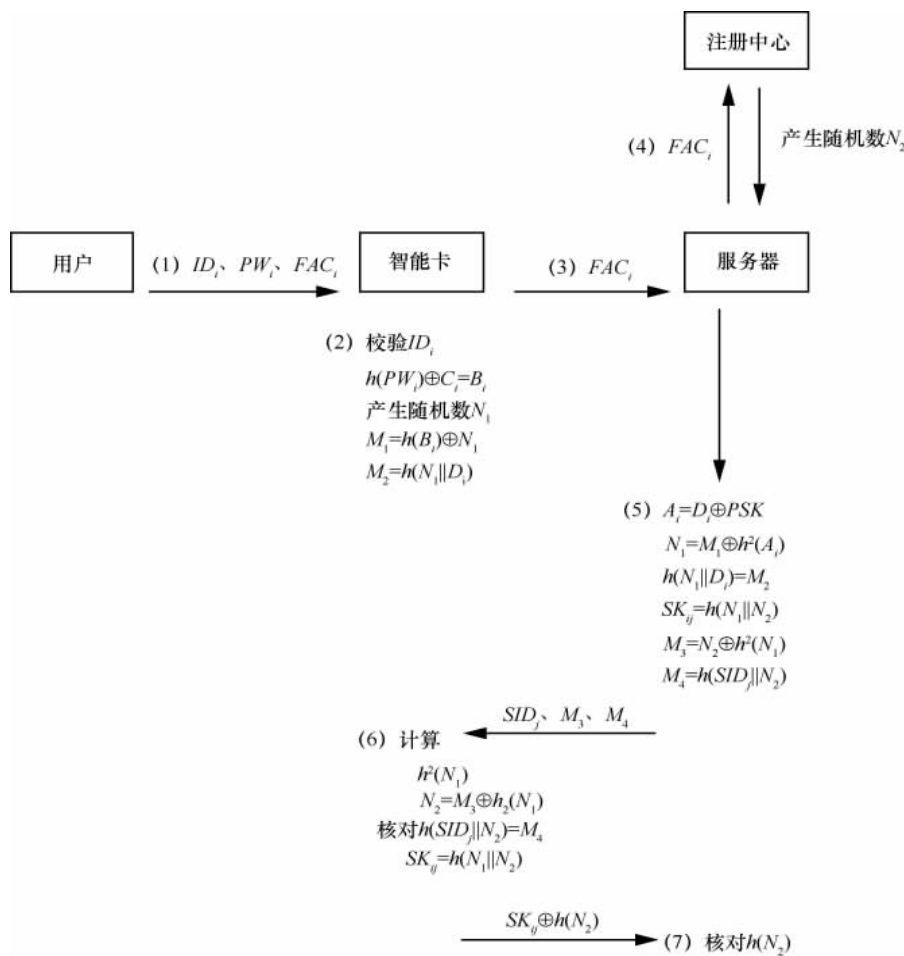


图7 登录过程

证信息输入,然后系统判断用户是否合法,若是则进入修改流程,输入新密码,完成信息更新。具体流程如图 8 所示。

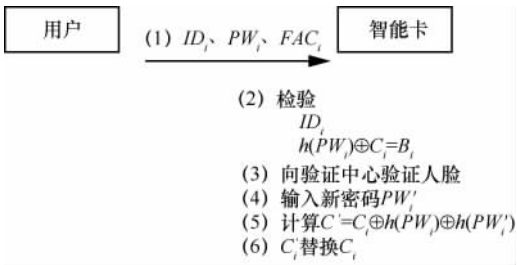


图 8 密码修改过程

- 步骤 1 首先用户输入用户名以及密码,然后扫描人脸。
- 步骤 2 智能卡核对用户名 ID_i 以及判断 $h(PW_i) \oplus C_i = B_i$ 是否成立。
- 步骤 3 智能卡把人脸信息传递给注册中心进行人脸识别,若通过则可进行密码修改过程,否则拒绝修改。
- 步骤 4 输入新密码 PW_i' , 计算 $C_i' = C_i \oplus h(PW_i) \oplus h(PW_i')$, C_i' 取代 C_i 。

4 安全性分析

分离保存注册信息:注册中心不保存用户名及密码,该部分经过一系列的加密过程保存在智能卡中,而经过 CNN 训练后的人脸模型保存在注册中心。这样即使注册中心数据被盗或者智能卡丢失,也无法拥有用户的完整信息。

相互认证过程:服务器需要确认该用户是合法用户,同理用户也要确定服务器并不是假冒的。在鉴权过程中,即使攻击者获得了用户的信息然后模仿用户也无法完成认证,因为攻击者无法知道服务器与注册中心的会话密钥,也无法获得随机数。而且随机数的设置防止了复制攻击。就算模仿者输入了之前所有的用户信息,也会被服务器拒绝,因为输入的随机数是非法的。

会话密钥协议:本文服务器与用户之间产生一个会话密钥,该密钥能保证会话的安全性,密钥是由随机数以及单向散列函数生成的(如 $SK_j = h(N_1 || N_2)$),该密钥非常难破解。

抵抗修改攻击:在认证过程时,攻击者会试图修改用户的认证消息。本文使用单向散列函数确保信息不被修改。这是由该函数的性质决定的,正向计算非常简单,但是逆向计算非常难,因此无法还原原始数据,攻击者试图修改时会很容易被检测到。

抵抗离线密码猜测攻击:对于攻击者,密码(PW_i)、密钥(PSK)、人脸信息以及注册中心的机器指纹都是未知

的,即使智能卡中的信息被偷取,系统也是安全的。而密码等是由单向散列函数加密的,因此想要猜测密码非常难,而人脸模板具有唯一性,即使猜对了密码特征模板也不可能猜对人脸模板。

快速检错:智能卡中直接核对密码和用户名信息,若这部分信息错误则立即拒绝访问,只有当这部分完成认证后,智能卡才会把人脸信息传递到注册中心进行识别。

简单的密码修改:由于密码是保存在智能卡中的,因此只要修改智能卡中的信息即可,无需对注册中心中的信息进行修改。

人脸模板的保护:虽然注册时输入的是用户的图片,但是在输入 CNN 系统中进行训练之前使用混沌模型对人脸图片进行加密,使肉眼不能分辨属于谁的脸,只有在训练之前才利用密钥进行解密,解密后的图片作为卷积神经网络训练样本,生成人脸模板。利用该方法,即使人脸模板信息泄露,盗窃者也无法确定用户信息。

抵抗内部攻击:由于注册中心不保存全部的用户信息(如用户名和密码),由于散列函数的单向性的性质,能很好地抵抗内部攻击。

支持多服务器:在本文提出的系统中,用户只需要在注册中心注册一次就能接入其他的多应用服务器。用户登录不同的服务器不需要进行重复的注册,因此系统属于多服务器认证系统。

将本文提出的方案与其他的多环境服务器认证系统进行比较,比较结果见表 1。表 1 中体现出本文提出的方案更具有安全性。

由表 1 可以发现,本文提出的系统有两点独到之处。首先,分离的保存生物特征和普通密码,使之单独一项丢失或者被信息被盗则不会被模仿者攻击。其次,本文提出

表 1 多服务器比较

安全项	本文方案	Chuang ^[22]	Tsai ^[21]	Mishra ^[16]	Shen ^[19]	Yoon ^[13]
分离保存信息	是	否	否	否	否	否
相互认证	是	是	是	否	是	是
会话密钥协议	是	是	是	是	是	是
抵抗修改攻击	是	是	是	是	是	是
抗离线密码猜测	是	是	是	是	是	是
快速检错	是	否	否	是	是	是
简单密码修改	是	否	否	是	是	是
人脸模板保护	是	-	-	-	-	-
抗内部攻击	是	否	否	是	是	是
支持多服务器	是	是	是	是	是	是



了基于人脸的验证方案,其他文献中只提出了生物特征,并没有具体验证人脸识别的可行性以及可靠性,本文验证了利用 CNN 人脸模板的认证识别率以证明利用人脸方法的可行性。

5 实验分析

5.1 混沌映射

混沌加密与解密过程是相对的过程,之间会产生一个密钥,在本实验中加密密钥和解密密钥对应的是同一个。为了方便实验的进行,本文选择 0~1 的任意值作为密钥,当然实际情况的密钥会更加复杂。加密过程使用密钥进行加密,会使加密后的图片呈现“雪花状”,根本无法获得任何信息,大大地加强了人脸图像的保护。解密是加密的一个逆过程,知道正确的密钥才能解密。图 9 是一个加密与解密的实验示例。在实验中,密钥选择是 0.3,经过加密后图片变成“雪花”状,而输入人脸识别系统之前要对图像进行解密,如果使用正确的密钥 0.3,则解密后得到原图,而使用错误的密钥,例如 0.2,则无法正确解密,得到的仍然是“雪花”状图形。

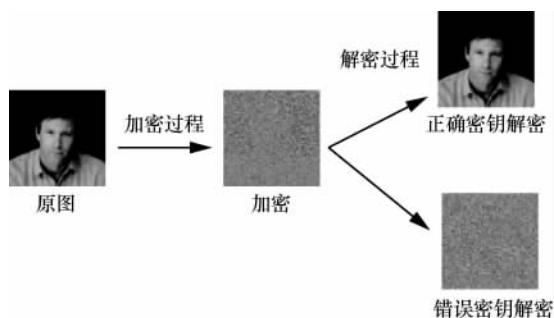


图 9 加密—解密结果示意

5.2 人脸识别分析

本实验中采用 ORL 人脸库作为实验数据,该数据库包含 40 个不同人的图片,每个人拥有 10 张不同的图片,总共 400 张图片,每张图片大小为 112 dpi×92 dpi。ORL 人脸图像是在不同时间、不同视角、各种表情(睁眼/闭眼、微笑/吃惊/生气/愤怒/高兴)和各种细节(有无眼镜、胡子)下拍摄得到。该数据库符合实验的要求。

5.2.1 识别流程

卷积神经网络的识别过程通常包括 3 个部分:预处理、训练、识别,如图 10 所示。预处理过程,直接把原图输入效率过低,因此在输入之前把图片格式变化为 lmbd 格式,然后输入 CNN 训练网络中。训练过程把样本分成两

类,一类作为训练样本,生成识别模型,另一类作为待识别图片,即测试样本。训练过程训练步长设置 0.001,迭代次数 5 000,从而得到最优识别模型。

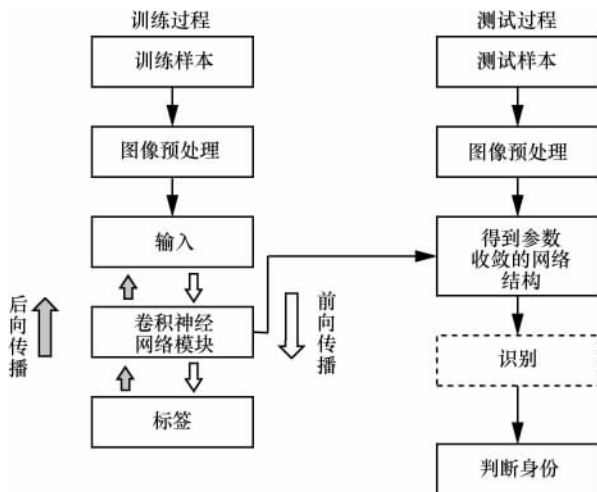


图 10 CNN 识别流程

不同人的图片经过卷积之后得到的特征图之间的特征有很大的差异,而且随着经过的卷积层的数量增加,不断地进行降维,肉眼所能得到的信息越来越少,最后变成了一个 160 维的向量,然后输入 softmax 分类器中进行分类。为了了解不同人的特征的差异,本文提取了两个人的所有中间层信息进行比较,如图 11 所示。最后一个 fc160 指的是一个全连接层,它的维数已经降低到了 160 维,然后系统可以根据该层信息进行分类识别。

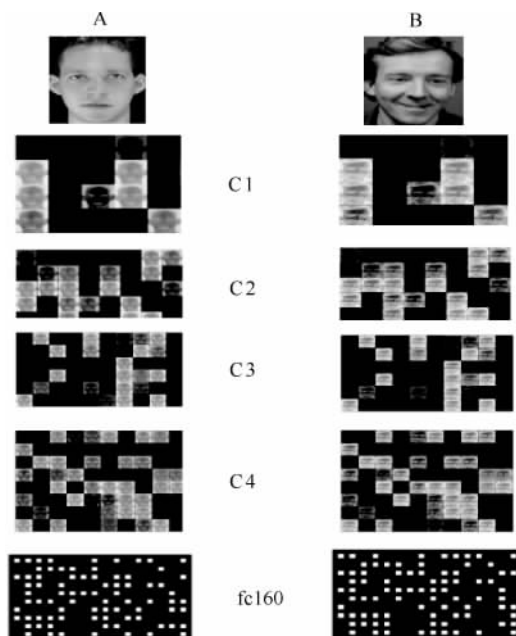


图 11 特征图比较

5.2.2 实验数据分析比较

实验模型采用四层卷积层模型,如图 4 所示。由于每个特征图是由图片与卷积核卷积而成,因此卷积核的大小会影响识别率,本文分别就不同的卷积核大小进行了实验,分别采取 2 dpi×2 dpi、4 dpi×4 dpi、6 dpi×6 dpi 共 3 种大小进行实验。识别率见表 2。

从识别率的角度分析,不同大小的卷积核对识别率确实有一定影响,但是本实验中识别率相差不是很大,因此直接从识别率角度判断使用哪种卷积核会过于牵强。卷积

表 2 不同卷积核大小识别率比较

卷积核	识别率
2 dpi×2 dpi	97.9%
4 dpi×4 dpi	98.1%
6 dpi×6 dpi	97.4%

神经网络中随着迭代次数的增加,识别率会不断地提高,最后稳定在一定数值,同时损失度曲线也一样,会下降到一个值附近稳定。根据训练日志本文生成不同卷积核大小的识别率和损失度曲线,如图 12 所示。

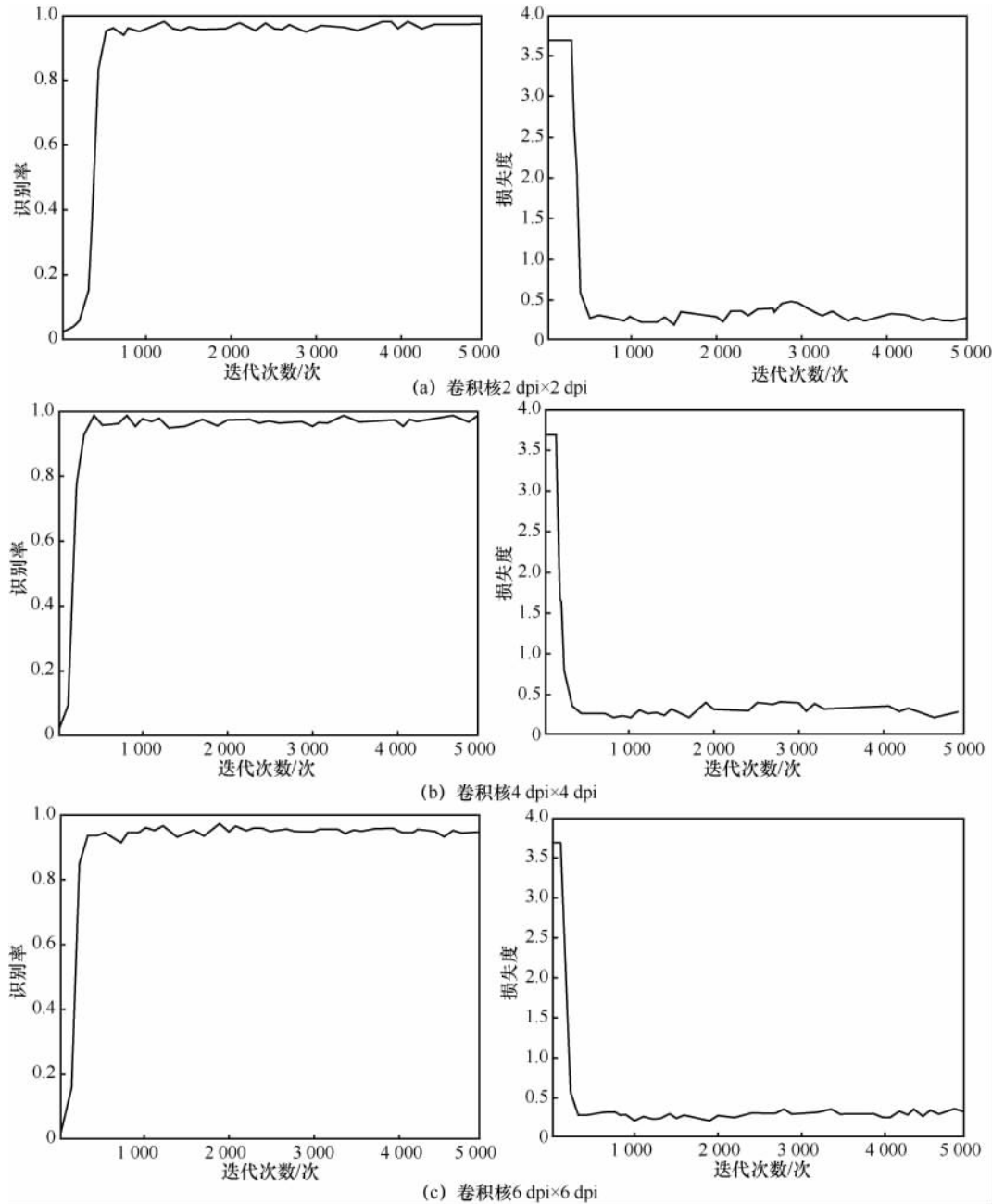


图 12 曲线比较



对图 12 中的识别率曲线进行比较,图 12 (a)与图 12(b)相比识别率曲线的收敛速度较低,需要迭代的步数更多。但图 12(b)与图 12(c)的收敛速度相差不大。损失度曲线中图 12(a)的波动最大,图 12(c)比图 12(b)略好,但是识别率比图 12(b)低。在所设计的系统中主要考虑识别率以及识别速率,结合表 2 与图 12 最后选择卷积核大小为 4 dpi×4 dpi。

利用 CNN 模型,与其他人脸识别算法的识别率进行比较,比较结果见表 3。

表 3 不同方法识别率比较

算法	识别率	加入机器指纹
PCA	87%	87.5%
LBP	70%	72.6%
SRC+LDA	85%	86%
CNN	97%	98.1%

表 3 中的识别率都是在 ORL 人脸库中,在训练样本为 5 张时的识别率。因为在进行注册时不宜采集过多的样本,以 5 张较为适宜,利用 CNN 模型识别时识别率达到 98.1%,则可以符合系统的验证要求。

6 结束语

本文提出的远程安全认证方案不仅支持多服务器环境,而且具有很高的安全性,以保护用户不被攻击。该方案增加了人脸图片的混沌映射方法,起到了保护图片的作用,有效提高了认证过程中的安全性。认证方式采用智能卡、密码和生物特征组合的形式,加入人脸识别方式能很大程度地提高认证的安全性、方便性。近几年机器学习的迅速发展,人脸的识别率不断提升,使提出的方案能适用于实际环境中。

参考文献:

[1] JUANG W S, CHEN S T, LIAW H T. Robust and efficient password-authenticated key agreement using smart cards [J]. IEEE Transactions on Industrial Electronics, 2008, 55 (6): 2551-2556.

[2] SUN D Z, HUAI J P, SUN J Z, et al. Improvements of Juang's password-authenticated key agreement scheme using smart cards[J]. IEEE Transactions on Industrial Electronics, 2009, 56 (6): 2284-2291.

[3] FAN C I, LIN Y H. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics[J].

IEEE Transactions on Information Forensics and Security, 2009, 4(4): 933-945.

[4] HE D, KUMAR N, LEE J H. Enhanced three-factor security protocol for USB consumer storage devices[J]. IEEE Transactions on Consumer Electronics, 2014, 60 (1): 30-37.

[5] KUMARI S, KHAN M K, LI X. An improved remote user authentication scheme with key agreement [J]. Computers& Electrical Engineering, 2014, 40 (6): 1997-2012.

[6] LEE N Y, CHIU Y C. Improved remote authentication scheme with smart card [J]. Computers Standards & Interfaces, 2005, 27(2): 177-180.

[7] KUMARI S, KHAN M K. Cryptanalysis and improvement of 'A robust smart-card-based remote user password authentication scheme' [J]. International Journal of Communications Systems, 2014, 27(12):3939-3955.

[8] CHANG C C, LE H D, CHANG C H. Novel untraceable authenticated key agreement protocol suitable for mobile communication[J]. Wireless Personal Communications, 2013, 71(1): 425-437.

[9] KUMARI S, KHAN M K. More secure smart card based remote user password authentication scheme with user anonymity [J]. Security and Communication Network, 2014, 7(11): 2039-2053.

[10] LI X, NIU J, MA J, et al. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards[J]. Journal of Network & Computer Applications, 2011, 34 (1): 73-79.

[11] KUMARI S, CHAUDHRU S A, WU F, et al. An improved smart card based authentication scheme for session initiation protocol [J]. Peer-to-Peer Networking Applications, 2015:1-14.

[12] WU F, XU L, KUMARI S, et al. A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks [J]. Computers& Electrical Engineering, 2015, 45:274-285.

[13] YOON E, YOO K. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem[J]. The Journal of Supercomputer, 2013, 63(1): 235-255.

[14] HE D, WANG D. Robust biometrics-based authentication scheme for multiserver environment[J]. IEEE Syst J, 2015, 9(3): 816-823.

[15] ODELU V, DAS A K, GOSWAMI A. A secure biometrics-based multi-server authentication protocol using smart cards[J]. IEEE Trans Inf Forensics Secur, 2015,10(9):1953-1966.

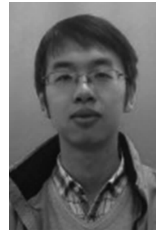
[16] MISHRA D, DAS A K, MUKHOPADHYAY S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards[J]. Expert Systems with Applications, 2014, 41 (18): 8129-8143.

- [17] LIN H, WEN F, DU C. An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics [J]. Wireless Personal Communications, 2015, 84 (4): 2351-2362.
- [18] LU Y, LI L, PENG H, et al. A biometrics and smart cards-based authentication scheme for multi-server environments [J]. Security & Communication Networks, 2015, 8 (17): 3219-3228.
- [19] SHEN H, GAO C Z, HE D D, et al. New biometrics-based authentication scheme for multi-server environment in critical systems [J]. Journal of Ambient Intelligence and Humanized Computing, 2015, 6(6): 825-834.
- [20] 范九伦, 张雪峰. 分段 Logistic 混沌映射及其性能分析 [J]. 电子学报, 2009, 37(4): 720-725.
FAN J L, ZHANG X F. Piecewise logistic chaotic map and its performance analysis [J]. Acta Electronica Sinica, 2009, 37(4): 720-725.
- [21] TSAI J L. Efficient multi-server authentication scheme based on one-wayhash function without verification table [J]. Computers & Security, 2008, 27(3-4): 115-121.
- [22] CHANG C C, LIN I C. Remarks on fingerprint-based remote user authentication scheme using smart cards [J]. ACM SIGOPS Operating Systems Review, 2004, 38(4): 91-96

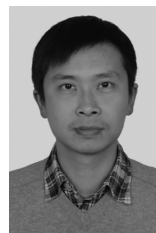
[作者简介]



章坚武 (1961-), 男, 杭州电子科技大学通信工程学院教授、博士生导师, 主要研究方向为移动通信系统、多媒体通信技术、网络安全等。



姚泽瑾 (1993-), 男, 杭州电子科技大学通信工程学院硕士生, 主要研究方向为基于深度学习的人脸识别研究等。



吴震东 (1976-), 男, 杭州电子科技大学网络空间安全学院讲师, 主要研究方向为生物特征识别、网络安全、人工智能等。