基于区块链和人脸识别的双因子身份认证模型

Two-factor Identity Authentication Model Based on Blockchain and Face Recognition

吕婧淑[1] 操晓春[1] 杨培[2]

[1](中国科学院信息工程研究所 信息安全国家重点实验室，北京 100093)

[2](32081 部队 北京 100093)

摘要 很多组织以中心化的方式存储用户的身份信息，然而一旦发生泄库事件会造成非常严重的后果。因此，如何确保用户身份信息的隐私性和安全性，如何安全可靠地鉴别用户身份，是保障用户和组织信息安全的必要条件。区块链的核心特征就是去中心化和非实名化，因此区块链技术很适合应用于身份认证的场景。首先，本文阐述了身份认证和区块链的发展历史和原理；其次，指出了传统身份认证机制中由于中心化存储而存在的安全性问题；并针对问题提出了基于区块链和人脸识别的双因子身份认证模型，对模型的参与方和组件进行了定义及描述，详细介绍了该模型涉及的各操作的具体流程。最后，通过模拟攻击与抵抗分析证明了模型的安全性、通过效率及存储分析证明了模型的可用性。

关键词 身份认证；区块链；人脸识别；双因子；去中心化

中图法分类号 TP309

Abstract Many organizations store users' identity information in the centralized way. In the leakage event, it will cause very serious consequences. Therefore, how to ensure the privacy and security of user identity information, how to securely and reliably identify users is a necessary condition to ensure the information security of users and organizations. Blockchain’s core features are "decentralized" and "non-real-name," so blockchain technology is well suited for authentication scenarios. Firstly, the paper expounds the history and principle of identity authentication and blockchain development. Secondly, it points out the security problems of traditional identity authentication mechanism due to centralized storage. On this basis, it also put forward two-factor identity authentication model based on blockchain and face recognition, defines and describes the participants and components of the model and details the specific processes of each operation involved in the model. Finally, the security of the model is proved by simulating attack and resistance analysis, and the availability of the model is proved by efficiency and storage analysis.

Key words identity authentication; blockchain; face recognition; two-factor; decentralized

1 引言

身份认证[1]是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，保证系统和数据的安全。它是保障信息安全的重要手段。

目前，身份认证的方式有以下三种：（1）以静态口令为代表的根据用户所知道的信息来证明其身份；（2）以动态口令为代表的根据用户所拥有的东西来证明其身份；（3）以人脸识别、虹膜识别等为代表的根据独一无二的生物特征来证明用户身份。

然而，前两种方式都有其不足之处。第一种身份验证方式将静态口令中心化地存储和管理，然而一旦发生泄库事件，用户的隐私信息就会大规模被暴露。例如，2014 年约 200 张大多为好莱坞女性艺人的私人照片（包括裸照等不雅隐私内容）被人盗取并上传至了各大社交媒体的网站[2]。经调查发现，盗取者非常有针对性地破解了中心化地存储在服务器的用户名及口令，并利用破解后的用户名及口令冒充合法用户登录

基金项目：国家重点研发计划(2016YFB0800603)；
This work is supported by National Key Research and Development Plan(No.2016YFB0800603).
收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00
CNKI 在线出版时间: 0000-00-00

应用，获取隐私性极强的信息并以此牟利；第二种身份认证方式用到的动态口令对移动终端设备有较强的依赖，一旦恶意用户得到合法用户的终端设备，那么恶意用户便可通过手机号及其动态短信口令冒充合法用户登录并窃取信息。

其中，第三种身份认证方式包括虹膜识别、指纹识别、声音识别等为代表的高级生物识别技术。它是基于用户个人独一无二的生理或行为特征进行身份鉴别的技术。因为生物特征具有唯一性、不可复制性。它不会像口令那样容易被忘记或被破解，也不会像持有物那样容易被窃取或转移。因此，目前生物特征识别技术[3]被认为是以上三种方式中更加可靠、方便、快捷的身份认证手段。

区块链技术具有去中心化、时序数据、集体维护和安全可信等特点[4]。1）去中心化：区块链数据的验证、记账、维护和广播等过程均是基于 P2P[5]（Peer-to-peer）分布式网络结构，采用纯数学方法而不是中心化机构来建立节点间的信任关系，从而形成去中心化的可信任的 P2P 分布式系统；2）时序数据：区块链采用带有时间戳的链式区块结构存储数据[6]，从而为数据增加了时间维度，具有极强的可验证性和可追溯性；3）集体维护：区块链系统采用特定的激励机制来保证所有节点均可参与新区块、新数据的验证过程；4）安全可信：采用哈希、数字签名等非对称加密方法对数据进行加密和签名，同时借助分布式系统各节点的工作量证明等共识算法形成的强大算力来抵御外部攻击，从而保证区块链数据不可篡改和不可伪造。

以上这些特点使区块链十分适合存储和保护隐私数据，以避免因中心化机构遭受攻击或权限管理不当而造成的大规模数据丢失或泄露。任意用户数据均可通过哈希运算打包写入区块链，通过区块链 P2P 网络系统内节点的共识算法和非对称加密技术来保证安全性。

由于区块链技术和生物识别技术对身份认证而言有其突出的优势，因此本文提出的模型利用了区块链与人脸识别两种技术，并将在下节本文选择解释两种技术的原因。

2　相关工作

本节将分别详细描述区块链和人脸识别技术的基本原理和发展历程。

2.1 区块链与身份认证

区块链是一种去中心化、不可篡改、可追溯、多方共同维护分布式数据库的技术，它的技术架构如图 1 所示。一般来说，区块链系统由数据层、网络层、共识层和应用层四层构成。

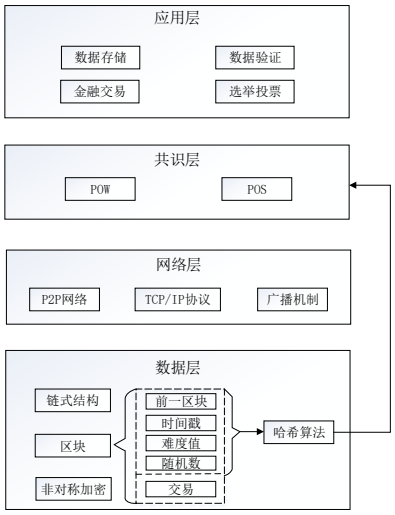

Fig.1 A technical framework of blockchain

图 1 区块链技术架构示意图

数据层包括区块、链式结构、非对称加密和哈希算法。以比特币为例，区块由区块头部和区块体组成；链式结构是区块与区块之间的连接方式，即当前区块的区块头存储前一区块的哈希值；非对称加密[7]通常在加密和解密过程中使用两个非对称的密码，分别称为公钥和私钥。比特币系统一般通过调用操作系统底层的随机数生成器来生成 256 位随机数作为私钥，公钥是由私钥通过 Secp256k1 椭圆曲线加密算法[8]生成 65 字节长度的随机数。比特币系统使用该公钥加密区块体中的交易数据并在验证时用私钥解密；并通过

SHA256[9]和 RIPEMD-160[10]对公钥进行双哈希运算生成 20 字节的摘要，再通过 SHA256 和 Base58 转换形成 33 字符长度的交易地址。

网络层封装了区块链系统的组网方式、节点连接的协议以及消息的传播机制。区块链系统的节点具有分布式、自治性等特点，因而采用了 P2P 网络来组织参与数据验证和记录的节点；基于 P2P 的网络结构，节点之间建立连接的方式是 TCP/IP 协议族的 TCP 三次握手协议，每个节点最多可建立 8 个传出连接和 117 个传入连接；当新区快、新交易产生时，节点向与其建立传出连接的节点发送封装了区块或交易数据的消息请求，以达到全网节点共同验证、记录新数据的目的。

共识层包括常见的共识协议 POW（Proof of Work，工作量证明）和 POS（Proof of Stake，股权证明），它们分别以节点的算力、持有特定数量货币的时长决定新区快的拥有权。以最常见的 POW 为例，节点的一次计算过程为将当前区块头部中的除难度值以外的元数据未确认的交易集合作为输入，经过哈希算法得到输出。不断尝试不同的随机数并重复该过程，最先算出符合难度值（由多个前导零构成的哈希值，零越多找到符合条件的随机数的难度越大）要求的输出的节点完成了工作量证明，获得新区块的拥有权。

应用层包括数据存储、数据验证、金融交易和选举投票等应用。本文提出的模型就属于数据验证的范畴，这类应用已有一定的研究基础，例如：ShoCard[11]是一个将实体身份证件数据加密并签名保存在区块链上的服务。用户用手机扫描并上传身份证件，ShoCard 应用将证件信息加密后保存在用户本地，将数据指纹保存到区块链。区块链上的数据签名受私钥控制，只有持有私钥的用户才有权修改，ShoCard 亦无权修改。

区块链的节点若仅仅拥有匿名地址而无法证明自己的身份，那么其应用场景相对狭窄。因此，将区块链技术应用于身份认证场景不仅能解决传统身份认证方式存在的问题，还能拓展出更多的应用。

2.2 人脸识别与身份认证

计算机人脸识别技术是利用计算机分析人脸图像，进而从中提取出有效的识别信息，用来“辨认”身份的一门技术[12]。该技术的输入是一张或者一系列含有未确定身份的人脸图像，以及人脸数据中的若干已知身份的人脸图像或者相应的编码；输出是待识别人脸与人脸数据库中一系列已知身份的人脸的相似度得分。可根据该得分设置阈值以判断待识别人脸的身份。

人脸识别算法的发展历史可以分为三个阶段。第一阶段为 1964 年至 1990 年，这一阶段人脸识别通常仅作为一般性的模式识别问题来研究，所采用的主要技术方案是基于人脸几何结构特征[13](Geometric feature based)的方法。第二阶段为 1991 年至 2013 年，这一阶段诞生了若干经典的传统人脸识别算法，如 eigenface[14]等，同时以 SVM[15]为代表的统计学习理论也在这一时期内被应用到了人脸识别与确认中。第三阶段为 2013 年至今，这一阶段的代表就是各类基于深度学习的人脸识别算法，如 2014 年 Facebook 公司提出的基于深度 CNN 的 DeepFace[16]算法、香港中文大学提出的 DeepID[17]算法、2015 年谷歌公司提出的 FaceNet[18]算法，CVPR2017 上发表的 SphereFace[19]算法提出了角度损失函数，给了深度人脸识别一个新的切入点。

人脸识别的流程如图 2 所示。其中，人脸 A 为待确定身份的人脸、人脸 B 为已确定身份的人脸、classifier 为人脸识别的某种算法。首先，通过人脸识别算法分别将人脸 A 和人脸 B 向量化为向量 A 和向量 B；其次，将两者连接为向量 AB；最后，通过 classifier 计算向量 AB 的相似度，以判别人脸 A 与人脸 B 的相似性——若相似，则输出 1，反之输出 0。

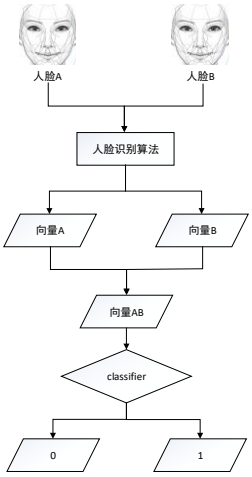

Fig.2 Face Recognition Process

图 2 人脸识别流程图

人脸识别技术的应用很广泛，例如：公安系统内的罪犯身份识别、驾驶执照及护照等与实际持证人的核对、银行及海关的监控系统及自动门卫系统等。因此，人脸识别技术与身份认证场景是息息相关的。

综上所述，本文结合了区块链和人脸识别两种技术作为双因子身份认证的认证方式，即结合了根据用户所拥有的信息和用户生物特征两种身份认证方式。这样的双因子认证方式优势在于利用了（1）区块链技术去中心化、不可篡改、非实名化的特点。一方面，极大地降低了由于中心化存储发生泄库事件而造成用户信息的泄露。另一方面，借助分布式各节点的工作量证明机制形成的强大算力能够抵御恶意节点的伪造，保证用户信息一旦被写入区块链则无法更改或注销。除此之外，各节点在区块链上交易或通信都是用的是各自公钥生成的地址，因此节点的虚拟身份无法与现实中的真实身份对应起来，保证数据公开的情况下的隐私性；（2）人脸识别的不可复制性、安全可信。在身份认证的三种方式中，人脸相对于静态或动态口令是独一无二的输入，并且仿制和造假的难度极高。人脸输入经过人脸识别模型的输出是二进制特征值，从输出到输入是不可逆的，保证了用户生物特征的安全性；（3）双因子身份认证结合了（1）和（2），安全地存储了用户的基本信息和人脸特征，保证在验证时二者的缺一不可，从而提高了身份认证的安全性。

3 基于 IdentiChain 和人脸识别的双因子身份认证模型

本节首先指出了传统身份认证方式存在的问题，并针对问题提出了解决模型。其次，对模型的技术组件进一步解释。最后，详细描述了模型流程。

3.1 问题描述

传统身份认证存在问题的模型如图 3 所示。问题模型的参与方为用户 U、服务供应商 S、攻击者 A。三者的关系在于 U 向 S 请求服务，S 需要验证该 U 的身份，因此 U 向 S 输入用户名和口令；S 向服务器发起身份注册或身份认证的请求，服务器向数据库发起读写请求，对输入信息进行注册写入或验证计算，并返回是否注册成功或验证成功的结果；A 利用漏洞攻击、SQL 注入[20]等手段攻击服务器的数据库以获得存储隐私数据的文件，再使用暴力破解等手段对该文件破解获得用户名和口令明文，便能获得 U 的更多信息甚至侵占其权益。

一方面，攻击者为了获得数据库文件会一直挖掘、利用数据库的漏洞；另一方面，数据库中心化地存储、管理用户的隐私信息，只要数据库存储在服务器上或是与服务器有读写操作，数据库文件就面临被盗取的风险。除此之外，某用户名及对应口令一旦被破解，攻击者便能冒充其合法身份登录对应的网站或应用。若该网站是实名制网站，攻击者甚至能追溯到用户在现实中的身份，可能会发生身份盗用的恶性事件。

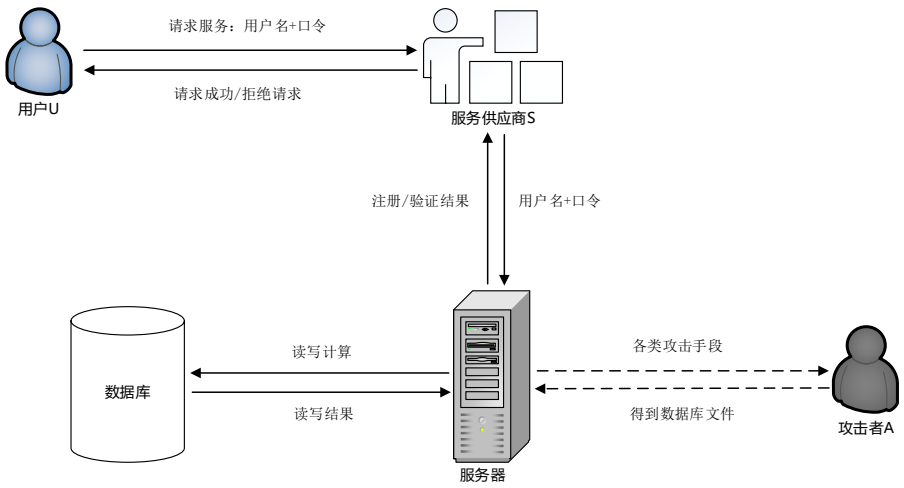

Fig. 3 Question model

图 3 问题模型 3.2 模型框架

针对 3.1 的问题模型，本文提出了基于区块链和人脸识别的双因子身份认证模型。该模型由三个参与方和两个技术组件构成。三个参与方分别是用户、移动端 APP 和服务供应商，两个技术组件分别是人脸识别神经网络模型和基于区块链的身份链 IdentiChain。

三个参与方之间的关系如图 4 所示：用户希望通过移动端 APP 使用服务供应商的服务，因此用户需要成为服务供应商的合法认证用户。用户初次通过移动端 APP 发起请求服务时，需要完成注册操作，注册成功后服务供应商返回服务和公钥；用户再次请求服务时，需要完成验证操作，验证成功后服务供应商返回服务和新公钥。

两个技术组件都与移动端 APP、服务供应商两个参与方有读写交互。其中，人脸识别神经网络模型接收移动端 APP 输入的人脸图像，进行训练输出该用户的特征值 ID，并对其哈希加密后返回给 APP。每个服务供应商都是 IdentiChain 的节点之一。APP 向获得注册权的服务节点输入 Hash(ID)和 Hash(证件信息)，服务节点在注册、验证等操作中进行不同的计算，如：竞争、写入、验证。

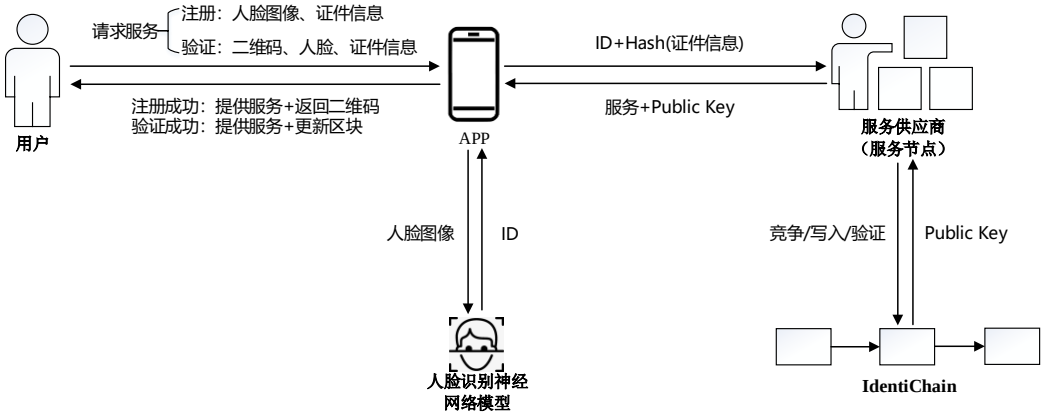

Fig. 4 Two Factor Authentication Model Framework Based on IdentiChain and Face Authentication

图 4 基于 IdentiChain 和人脸识别的双因子身份认证模型框架 3.3 组件定义

本模型中技术组件包括人脸识别模型和身份链 IdentiChain。本节将详细地阐述两个组件的定义和细节。

3.3.1 人脸识别神经网络模型

本文使用的人脸识别模型是基于深度学习技术的 SphereFace[19]人脸识别模型。Sphere 模型是对 open-set 的人脸识别，即测试集中的数据没有出现在训练集中，测试集是用输入的某 query(待检测的人脸)来与数据库中的数据计算相似度，找出与 query 最为相似的人脸。这也符合本模型的场景，即用户每次请求服务

基金项目：国家重点研发计划(2016YFB0800603)；
This work is supported by National Key Research and Development Plan(No.2016YFB0800603).
收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00
CNKI 在线出版时间: 0000-00-00

时输入的人脸图像都不相同，那么验证时输入的 query 不存在于数据库中已存的人脸数据集。

不同于其它基于深度学习的人脸识别算法，SphereFace 算法在对深度网络进行训练的过程中，采用了一种改进的基于角度距离的损失函数，使得其学习出的深度特征具有角度可分的特性，性能优于采用欧氏距离度量损失函数(euclidean loss)或者三元组损失函数(triplet loss)的传统度量学习网络。在训练过程中，假设训练数据集中的第i张人脸图像对应的身份标签为y_i，算法首先利用深度卷积神经网络（convolutional neural network, CNN）对该图像提取深度特征x_i，然后使用如下的基于角度距离的损失函数进行网络的训练：

$$L_{ang}=\frac{1}{N}\sum_i -\log\left(\frac{e^{\|x_i\|\varphi(\theta_{y_i,i})}}{e^{\|x_i\|\varphi(\theta_{y_i,i})}+\sum_{j\neq y_i}e^{\|x_i\|\varphi(\theta_{j,i})}}\right) \quad (1)$$

如公式(1)所示，其中的$\varphi(\theta_{y_i,i})=(-1)^k\cos(m\theta_{y_i,i})-2k,\ \theta_{y_i,i}\in\left[\frac{k\pi}{m},\frac{(k+1)\pi}{m}\right]$, $k\in[0,m-1]$, $\theta_{j,i}$表示神经网络最后一层分类层的第j个节点的参数向量和特征x_i之间的夹角，N表示训练图像的个数，m是一个大于等于 1 的整数参数，在训练过程中固定$m=4$。

在网络的目标损失函数设计完毕以后，SphereFace 算法对网络结构进行了精细设计——采用了基于残差网络[21]的网络结构，使得网络在保持一定深度的同时不会产生梯度消失或梯度爆炸等问题而影响识别性能。该算法采用了一种 20 层的卷积神经网络，其具体结构如图 5 所示。其中，图 5 上半部分是网络整体结构图，训练数据中的人脸图像首先经过四个由卷积层、PReLU 激活函数层构成的残差网络单元，然后通过一层 512 维的全连接层，该层的输出即为人脸图像的特征，最后该特征和人脸图像的身份标签一起进入损失函数层，计算损失函数并进行网络参数的训练。图 5 的下半部分给出了四个残差网络单元的具体结构，其中每个方块代表一个卷积层-PReLU 激活层的组合，以 3x3,64,s2 为例，3x3 指的是卷积层的卷积核大小，64 是该卷积层输出的特征图的数量，s2 指的是该卷积层的卷积核移动步长为 2。在残差网络单元 2、3 和 4 中，同样的网络结构被重复串联了多次，在图中用大括号和 x2 等字样表示。

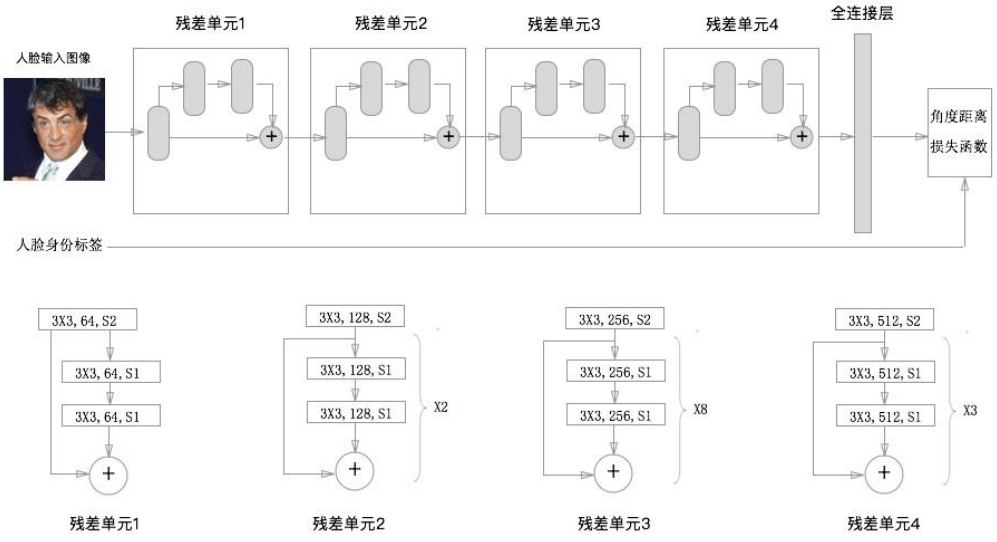

Fig. 5 SphereFace algorithm network structure diagram

图 5 SphereFace 算法网络结构示意图

给定上文描述的网络结构和损失函数后，Spherecafe 算法使用了公开数据集 CASIA-WebFace[22]用来对网络进行训练。CASIA-WebFace 数据集共有 494414 张人脸图像，来自 10575 个不同的人。在训练前，这些图像首先被水平镜像翻转，从而增加了训练数据的规模。在具体实现上，算法采用了深度学习框架 Caffe[23]对网络结构和损失函数进行实现，训练过程采用 4 个 GPU，每次迭代有 128 张训练图像被送进网络，网络的初始学习率为 0.1，随后在第 16000 和 24000 次迭代时，学习率变为原来的十分之一，整个训练共有 28000

次迭代。感兴趣的读者可以在参考文献[19]中得到算法的更多实现细节以及源代码实现。

在训练完毕后，对于给定的人脸图像，即可利用深度网络提出具有良好区分度的深度特征。

在得到人脸深度模型后，人脸身份认证的流程如图 6 所示：在认证过程中，对于给定的输入图像，本文首先利用 MTCNN[24]人脸检测算法对人脸以及其特征点进行检测，然后对于检测出的人脸，取其双眼，嘴角和鼻尖共 5 个特征点的位置，并利用这些位置信息求解变换矩阵，对人脸进行对齐操作。在获得对齐后的人脸图像后，将图像输入 SphereFace 模型进行特征提取，并利用特征间的余弦距离(cosine similarity)将提取的特征与已经在身份库中的人脸特征进行相似度比较，假设相似度得分大于一定阈值，则认为匹配成功，否则匹配失败。

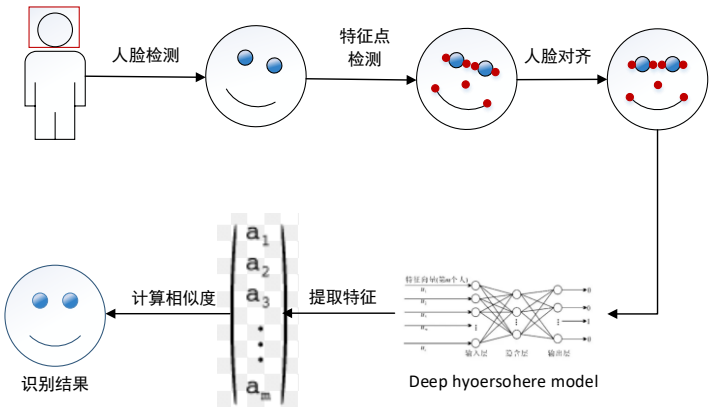

Fig. 6 Face recognition model process

图 6 人脸识别模型流程

3.3.2 身份链 IdentiChain

身份链 IdentiChain 是基于区块链技术的应用。每一个服务供应商都是开采 IdentiChain 区块的节点之一，因此也称其为服务节点，各服务节点共享同一个身份账本。用户在 APP 发起注册操作时，各服务节点使用工作量证明机制互相竞争新用户、新区块的注册权，即进行密集计算以最先找到一个随机数能满足广播的难度值（本模型的难度值为用户人脸特征值）。若某服务节点竞争到了新用户的注册权，那么该节点将得到一定程度的积分奖励，该积分奖励来自于各节点在开始竞争前上交的积分。IdentiChain 的区块结构与广为人知的比特币区块结构最大的区别在于第一，比特币的区块体存储着交易信息，而 IdentiChain 的区块体存储着证件信息；第二，比特币 POW 机制中的难度值是由多个前导零构成的哈希值，本文模型 POW 机制的难度值是经人脸识别神经网络模型计算并加密的特征值。

IdentiChain 区块的具体结构如图 7 所示(图中红框表示与比特币区块结构相比的创新之处)。每个区块分为区块头和区块体两部分。区块头包含 PrevHash(前一区块的哈希值，按照公式（2）计算出的当前区块哈希值作为下一区块头部的 PrevHash)、TimeStamp(时间戳)、Nonce(随机数)、ID(难度值)、SignInfo（加密且签名过的证件信息）；区块体包含 HashInfo(证件信息的摘要)。其中，ID 是通过人脸识别神经网络模型计算出人脸特征值并哈希加密后的输出。

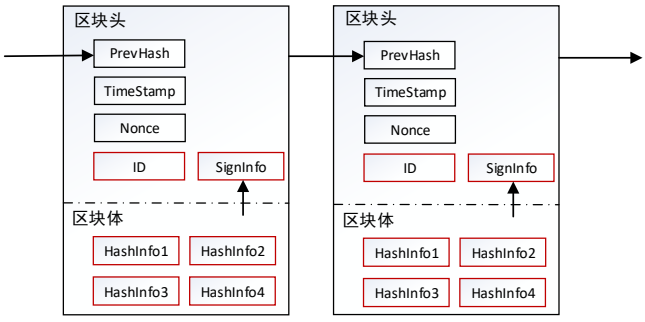

Fig. 7 IdentiChain block strcture

图 7 IdentiChain 区块结构

POW 共识机制的流程为：首先，希望注册的新用户经人脸识别模型和哈希加密的输出 ID 作为难度值被全网广播，哪个节点最先找到某随机数 Nonce 能够满足公式（3），该节点就能获得新用户的注册权，也获得了相应的积分奖励。其次，该节点将 ID、PrevHash、TimeStamp 和 Nonce 写入新区快的头部，将 HashInfo（1-4）四项证件信息写入区块体。然后，对各项证件信息(HashInfo)按照 Merkel 树[25]算法计算是输出 SignInfo。计算过程如图 8 所示：每两项HashInfo通过哈希算法计算并合并得到HashInfo_{12}和HashInfo_{34}，HashInfo_{12}与HashInfo_{34}通过哈希算法计算并合并得到 root 值，即HashInfo_{1234}。HashInfo_{1234}通过 RSA[26]算法签名生成 SignInfo 写入新区快的头部。其中，公式（2）、公式（3）用到的哈希(Hash)算法为 SHA256[27]算法。

$$\text{BlockHash} = \text{Hash}(\text{PrevHash} + \text{TimeStamp} + \text{Nonce} + ID + SignInfo) \quad (2)$$

$$\text{Hash}(\text{PrevHash} + \text{TimeStamp} + \text{Nonce} + SignInfo) \leq \text{ID} \quad (3)$$

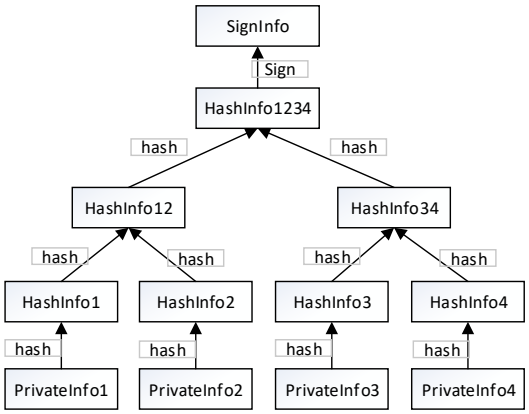

Fig. 8 Merkel tree strcture

图 8 Merkel 树结构

3.4 模型流程

本模型中，用户和移动端 APP 发起的请求包括注册和验证。本节将详细地阐述每一个请求的流程。

3.4.1 注册

用户希望获得某节点的服务，由于任何服务节点都使用 IdentiChain 进行身份验证，因此该用户需要成为 IdentiChain 的认证用户，即进行注册操作。注册流程如图 9 所示：1）用户向移动端 APP 上传包含人脸的照片及其证件信息；2）人脸识别模型训练出用户人脸特征值 ID 并将其返回给移动端 APP；3）APP 将 ID 和经过 Merkel 树算法计算的证件信息$HashInfo_{1234}$发送给用户请求的服务节点；4）该节点将 ID 作为难度值进行广播，各节点竞争新的身份区块，哪个节点优先计算出符合难度值的随机数，那么这个节点成为新区块的创建者并获得积分奖励；5）区块创建者将 ID 和签名后的证件信息 SignInfo 写入新区块中。其中，$\text{SignInfo} = \text{Sign}(HashInfo_{1234})$。服务节点返回签名对称的公钥和服务给 APP，APP 再将服务和封装了公钥的二维码返回给用户作为将来验证身份的凭证之一。

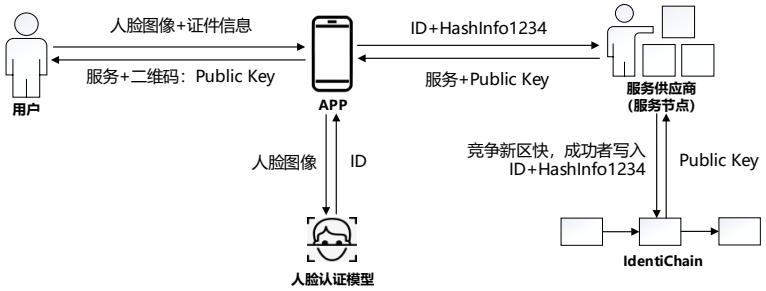

Fig. 9 Register process

图 9 注册流程图

3.4.2 验证

已经成为 IdentiChain 的注册用户希望获取某服务节点的服务，那么他需要通过 IdentiChain 的验证流程。验证流程如图 10 所示：1）用户向 APP 输入其人脸图像、证件信息和包含公钥的二维码；2）APP 将

人脸图像输入给人脸识别模型，该模型训练得到用户特征 ID，并将 ID 返回给 APP；3）APP 分别利用 Merkel 树算法计算证件信息得到$HashInfo_{1234}$、解析二维码得到 PublicKey，并将$HashInfo_{1234}$、ID 和 PublicKey 发送给用户请求的服务节点；4）该服务节点在 IdentiChain 中遍历是否存在与$HashInfo_{1234}$相等的 PublicKey(SignInfo)（用公钥解密后的 SignInfo）。若不存在，则证件信息不符，验证失败；若存在，则该用户证件信息验证通过；5）计算 APP 输入的 ID 与该区块 ID 的相似度，若不相似则认为是非法用户，验证失败。若相似，证明其生物特征验证通过；6）根据公式 3 计算 Hash(PrevHash+TimeStamp+Nonce)是否小于或等于 ID，若不满足则验证失败。若满足，验证成功。

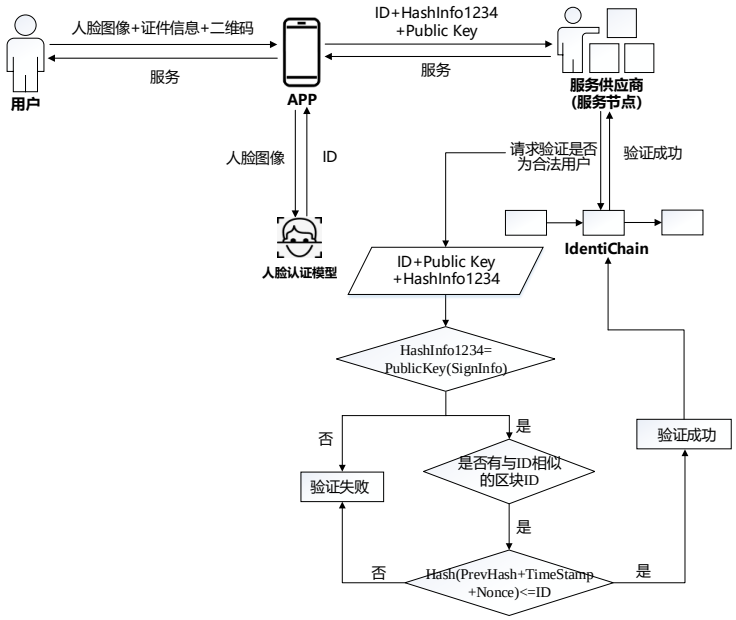

Fig. 10 Verification process

图 10 验证流程示意图

4 模型性能分析

为了证明基于区块链和人脸识别的双因子身份认证模型的有效性，本节分别对其安全性和可用性做了分析。其中，安全性分析在两种极端情况下分别定性、定量地证明了模型的安全性。可用性分析中分别定量地计算了 3.3 节的两个技术组件的准确率、效率和存储。

4.1 安全性分析

为了分析模型的安全性，假设了以下两种极端情况：分别是攻击者得到了合法用户的证件或通过某种攻击手段得到了本属于服务节点的 IdentiChain 入口。在两种极端情况下分析攻击者的攻击难度：

第一种情况：若攻击者获得了合法用户的证件原件或仿照原件伪造了假证件，那么攻击者也无法冒充合法用户验证通过。这是由于验证流程 1）需要用户上传的证件信息和区块链中已存的信息比对成功；2）需要扫描包含公钥的二维码才能在 1）验证证件信息的时候验证通过；3）需要人脸图像通过人脸识别模型的验证。这相对于普通的单因子认证，攻击难度变成了其三倍。在第一种情况下，攻击者只有流程 1）的输入，但 1）的验证成功也需要 2）中的公钥配合。因此，在此种情况下攻击者是无法通过本模型的验证流程的。

第二种情况：若攻击者获得了本属于服务节点的 IdentiChain 入口，那他也无法通过区块中的 SignInfo 反向推算出每一项证件信息。这是由于 SignInfo 的计算方式——Merkel 树算法造成的。若攻击者想计算出原始证件信息，首先，要尝试找到正确的公钥将 SignInfo 解密为$HashInfo_{1234}$（假设公钥有 m 项选择需要遍历）；其次，尝试将$HashInfo_{1234}$拆解为$HashInfo_{12}$和$HashInfo_{34}$；然后，将$HashInfo_{12}$拆解为$HashInfo_1$和$HashInfo_2$；$HashInfo_{34}$同理。最后，暴力破解$HashInfo_1$等四个单项哈希加密的信息。但是，由于哈希加密算法不可逆的特点，攻击者只能通过暴力破解等遍历的手段尝试找到四个单项 HashInfo 按照反向 Merkel 树算法计算等于 SignInfo。因此，其破解难度为$n^2 \times n^2 = n^4$（假设四个单项信息各有 n 项选择），

除此之外还要遍历 m 个公钥尝试解密。暴力破解单项 HashInfo 和 SignInfo 的难度对比如表 1 所示。

Table 1 Comparison of Crack Difficulty about HashInfo and SignInfo

表 1 HashInfo 与 SignInfo 破解难度对比表

破解内容	暴力破解单项 HashInfo	暴力破解 SignInfo
破解难度	n	$m \times n^4$

其中，若是为了保护用户的人脸特征，可以使用 DES[18]、AES[19]等对称加密算法对人脸特征 ID 进行加密，在计算相似度之前再解密，但这样做会牺牲一定的效率。

4.2 可用性分析

由于 3.3 节中两个技术组件是影响本模型是否可行的关键因素（即人脸识别模型和 IdentiChain），因此本节将对二者进行可行性分析。决定两者可用性的重要指标有准确率、效率和占用存储，分析结果如表 2 所示：

对于人脸识别神经网络模型，由于使用的是 SphereFace[10]算法，因此其在 LFW 数据集上、A-Softmax 损失参数为 4 的情况下准确率为 99.42%；在效率方面，完成一帧人脸图像的认证需要 20 毫秒；每帧人脸图像经模型训练后得到的 ID 为 1024 维向量，每维向量占用存储 4 个字节，因此一个 ID 共占用 4kB 存储。

对于 IdentiChain，由于证件信息和公钥在验证流程时都是保持不变的，只有人脸图像每次输入是不同的，并且需要用人脸识别模型训练出的 ID 在 IdentiChain 中遍历计算相似度。除此之外，本模型在验证流程时先比对证件信息，而证件信息比对的准确率是 100%，若证件信息验证失败则直接跳过后续的人脸识别。因此，本模型验证准确率大于等于人脸识别的准确率 99.42%；在效率方面，每次验证流程先比对证件信息再比对人脸，假设比对一次证件信息需要的时间为 ξ、IdentiChain 共 n 个区块，因此最多共需要 ξ × n 毫秒的时间遍历 n 个区块，加上计算一次 ID 相似度需要 0.05 毫秒，验证一个用户共需要 ξ ×n+0.05 毫秒；在存储方面，除了存储人脸特征 ID 以外，还需要存储 SignInfo、前一区块的哈希值 PrevHash、时间戳 TimeStamp 和随机数 Nonce。由上一段可知一个 ID 占用 4kB 存储，SignInfo 占用 85 字节、PrevHash 占用 85 字节、TimeStamp 占用 40 个字节、Nonce 占用 12 字节，因此一个区块占用存储 4222 字节，约为 4.22kB。

Table 2 Face Recognition Model and IdentiChain Usability Analysis Table

表 2 人脸识别模型与 IdentiChain 可用性分析表

组件	准确率	效率	存储
人脸识别模型	99.42%[19]	20ms/face	4kB /face
IdentiChain	≥99.42%	ξ × n + 0.05 ms/identity	4.22kB /block

5 总结

本文针对传统身份认证方式存在的问题，提出了一种基于区块链和人脸识别技术的双因子身份认证模型。本模型解决了传统身份认证中心化存储而造成的泄库风险，也降低了各服务供应商协作的成本。

本模型的创新点在于以下两方面：1）与传统中心化的身份验证方式相比，本模型采用去中心化的方式对用户信息进行存储与验证。传统的身份验证方式通常以用户名、口令组合验证为主，那么一旦泄库事件发生，攻击者获得了存储用户名和口令的数据库文件，其可以利用掌握的彩虹表、暴力破解等手段得到原始的用户名和口令。而本模型去中心化的存储和验证方式则避免了上述问题，即不会将用户信息存储到本地文件中，而是所有服务节点共享一个身份账本，虽然身份账本是在服务节点之间是公开的，但即使该账本被攻击者获得，也无法冒充合法用户的身份验证成功；2）与现有的区块链单因子身份认证相比的双因子认证。业界已有的区块链身份认证机制通常是单一地将所需信息进行加密后写入区块链并返回区块链地址，但若攻击者得到了该用户的身份信息及对应的区块链地址便能冒充其身份认证成功。但是在本项目中，攻击者即使得到了某用户的身份信息及对应的区块链地址也无法认证成功，因为还需要通过人脸的生物特征

认证。

本项目的意义存在于用户和服务供应商两方面。对普通用户来说，1）隐私信息的控制权更大。这是由于当某服务供应商（以下简称节点）向用户发起授权邀请时，用户只授权该节点所需信息即可；2）注册成本更低。所有节点共享了记录用户 ID 和信息的 IdentiChain 身份账本，因此用户通过某个节点注册一次后无须再通过剩余节点注册。对每个节点来说，3）去中心化地存储更安全。IdentiChain 能完全避免中心化存储用户隐私信息的文件泄库；4）人脸识别更安全且便捷。因为生物特征是每个人独一无二的特征；5）维护 IdentiChain 的成本更低。每个节点都共享身份账本，也都共同维护；6）重要证件的安全“备份”。通过使用 IdentiChain 节点之一注册后并成功认证过大于阈值的次数，即使未来证件遗失，也能通过多模态活体认证模型及 IdentiChain 中的认证历史成功认证；

经分析，本模型的安全性，准确率、效率与存储等可用性都得到了证明。其中，感谢学者耿梦悦对本文 3.2.1 节的技术支持。

参 考 文 献

[1] 李金库, 张德运, 张勇. 身份认证机制研究及其安全性分析[J]. 计算机应用研究, 2001, 18(2): 126-128.

[2] International Business Times: iCloud 裸照泄露风波：26 位明星深陷泥潭 [EB/OL]. (2014-09-23)[2018-01-17]. http://www.ibtimes.com.cn/articles/39253/20140923/icloud-nude-photoes.htm

[3] 孙冬梅, 裘正定. 生物特征识别技术综述[J]. 电子学报, 2001, 29(12): 1744-1748.

[4] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[5] 谭庆丰, 方滨兴, 时金桥, 等. StegoP2P: 一种基于 P2P 网络的隐蔽通信方法[J]. 计算机研究与发展, 2014, 51(8): 1695-1703.

[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

[7] Bellare M, Rogaway P. Optimal asymmetric encryption[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994: 92-111.

[8] Hankerson D, Menezes A J, Vanstone S. Guide to elliptic curve cryptography[M]. Springer Science & Business Media, 2006.

[9] Gilbert H, Handschuh H. Security analysis of SHA-256 and sisters[C]//International workshop on selected areas in cryptography. Springer, Berlin, Heidelberg, 2003: 175-193.

[10] Dobbertin H, Bosselaers A, Preneel B. RIPEMD-160: A strengthened version of RIPEMD[C]//International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1996: 71-82.

[11] Ebrahimi A. Identity management service using a blockchain providing certifying transactions between devices: U.S. Patent 9,722,790[P]. 2017-8-1.

[12] 张翠平, 苏光大. 人脸识别技术综述[J]. 中国图象图形学报: A 辑, 2000 (11): 885-894.

[13] Lamdan, Yehezkel, and Haim J. Wolfson. "Geometric hashing: A general and efficient model-based recognition scheme." (1988): 238-249.

[14] Zhang, Jun, Yong Yan, and Martin Lades. "Face recognition: eigenface, elastic matching, and neural nets." Proceedings of the IEEE 85.9 (1997): 1423-1435.

[15] Joachims, Thorsten. Making large-scale SVM learning practical. No. 1998, 28. Technical report, SFB 475: Komplexitätsreduktion in Multivariaten Datenstrukturen, Universität Dortmund, 1998.

[16] Taigman Y, Yang M, Ranzato M A, et al. Deepface: Closing the gap to human-level performance in face verification[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2014: 1701-1708.

[17] Ouyang W, Wang X, Zeng X, et al. Deepid-net: Deformable deep convolutional neural networks for object detection[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2015: 2403-2412.

[18] Schroff F, Kalenichenko D, Philbin J. Facenet: A unified embedding for face recognition and clustering[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2015: 815-823.

[19] Liu W, Wen Y, Yu Z, et al. SphereFace: Deep Hypersphere Embedding for Face Recognition[J]. arXiv preprint arXiv:1704.08063, 2017.

[20] Halfond, William G., Jeremy Viegas, and Alessandro Orso. "A classification of SQL-injection attacks and countermeasures."

Proceedings of the IEEE International Symposium on Secure Software Engineering. Vol. 1. IEEE, 2006.

[21] He, Kaiming, et al. "Deep residual learning for image recognition." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.

[22] D. Yi, Z. Lei, S. Liao, and S. Z. Li. Learning face representation from scratch. arXiv preprint:1411.7923, 2014.

[23] Jia Y, Shelhamer E, Donahue J, et al. Caffe: Convolutional architecture for fast feature embedding[C]//Proceedings of the 22nd ACM international conference on Multimedia. ACM, 2014: 675-678.

[24] Zhang K, Zhang Z, Li Z, et al. Joint face detection and alignment using multitask cascaded convolutional networks[J]. IEEE Signal Processing Letters, 2016, 23(10): 1499-1503.

[25] Szydlo M. Merkle tree traversal in log space and time[C]//Eurocrypt. 2004, 3027: 541-554.

[26] Biham E, Shamir A. Differential cryptanalysis of the data encryption standard[M]. Springer Science & Business Media, 2012.

[27] Daemen J, Rijmen V. The design of Rijndael: AES-the advanced encryption standard[M]. Springer Science & Business Media, 2013.