文章编号：2095-2163(2024)01-0140-04 中图分类号：TP393 文献标志码：A

基于区块链的多特征融合身份标识认证模型

薛 峰，李芳菊
（郑州经贸学院 计算机与人工智能学院，郑州 451191）

摘 要：身份标识认证模型节点设置多为单向结构，认证范围受限制，导致认证识别率下降，为此，本文提出基于区块链的多特征融合身份标识认证模型。预处理多特征基础认证环境，采用多阶段认证形式，布设一定数量的节点，部署模糊特征身份标识认证矩阵，以此为基础构建区块链 CNN 多特征融合认证模型框架，采用区块链自适应密钥修正，实现身份认证。测试结果表明：设计模型认证识别率可达 90%以上，认证准确度更高，认证速度快，误差可控。

关键词：区块链；多特征；融合身份；标识认证；认证模型

Multi-feature fusion identity authentication model based on blockchain

XUE Feng, LI Fangju
(College of Computer and Artificial Intelligence, Zhengzhou University of Economics and Business, Zhengzhou 451191, China)

Abstract: The node setting of identity authentication model is mostly one-way structure, and the authentication scope is limited, which leads to the decrease of authentication and recognition rate. Therefore, a multi-feature fusion identity authentication model based on blockchain is proposed. Multi-feature basic authentication environment is preprocessed, multi-stage authentication is adopted, a certain number of nodes are deployed, and fuzzy feature identity authentication matrix is deployed. On this basis, blockchain CNN multi-feature fusion authentication model framework is constructed, and identity authentication is realized by adaptive key correction of blockchain. The test results show that the authentication and recognition rate of the design model can reach more than 90%, indicating that the model has higher accuracy, faster authentication speed and controllable error for the test object.

Key words: blockchain; multi-feature; fusion of identity; identification and authentication; authentication model

0 引 言

多特征融合身份认证是最典型的一种认证方式，一般通过认证模型来实现。传统的多特征融合身份表示模型多为单向认证结构，如传统模糊多特征融合身份标识认证模型、传统错误检查和纠正零知识证明(ECC-ZKP)多特征融合身份标识认证模型，这一类身份认证模型虽然可以实现预期的处理目标，但是常常受到外部环境的影响，导致最终获取的认证结果不精准、不可靠[1]。

本文提出基于区块链的多特征融合身份标识认证模型，一定程度上扩大实际的认证范围，对于客户身份信息的筛查和核定也会更为迅速，利用部署的认证节点，不断采集更新相关数据，构建动态化的多特征融合身份认证标识结构，为后续相关行业及技术的进一步创新提供参考依据。

1 多特征融合身份标识区块链认证模型

1.1 预处理多特征基础认证环境

区块链认证主要包括公有链、联盟链以及私有链 3 种，可以先设定公有链为主控制程序，并搭建对应的认证节点，将三者搭接关联，形成定向的独立认证环境[2]。根据区块链技术的覆盖范围，设定具体的认证标准，见表 1。

根据表 1，完成对区块链基础身份认证标准的设定和分析。另外，基于区块链技术，还需要在公有链控制程序的基础上，增设联盟链以及私有链[3]。但私有链通常是封闭的，参与的认证控制节点受到不同程度的限制，所以为扩大实际的认证范围，强化身份认证的精准度与可靠性，可以综合区块链技术，

基金项目：河南省重点研发与推广专项项目(232102210197)。
作者简介：薛 峰(1983-)，男，硕士，副教授，主要研究方向：算法、计算机应用；李芳菊(1974-)，女，硕士，教授，主要研究方向：计算机应用。
收稿日期：2023-01-11

构建数据层、网络层、共识层、应用层的身份认证层级，通过层层筛选，增加认证的辨识度与识别效率，营造稳定的认证环境，为后续相关认证工作奠定基础。

表 1　区块链基础身份认证标准设定表

Table 1　Basic authentication standard setting table for blockchain

认证指标	预设标准	实测标准
认证目标	人脸、眼睛、身份证、密码等	人脸、眼睛、身份证、密码等
设定识别时间/s	0.33	0.21
密钥字节/位	256	277
动、静态认证	静态	动态+静态

1.2　设定多特征融合认证节点

综合建立的数据层、网络层、共识层、应用层的身份认证层级，建立对应的识别标准。此时，需要将可识别的特征进行分类，形成单向的特征认证识别程序[4]。搭接设置在控制平台中，构建循环式的多阶节点身份认证体系，如图 1 所示。

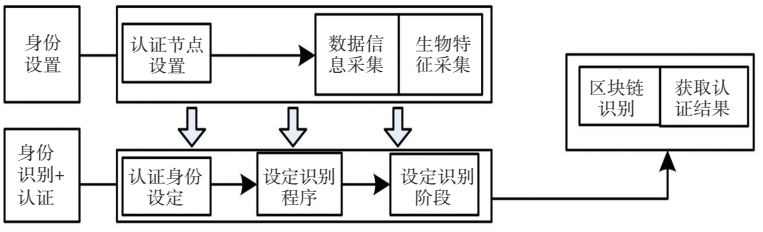

图 1　多阶节点身份认证体系结构

Fig. 1　Multi-level node authentication architecture

根据图 1，本文设计了一个多阶循环式身份认证体系结构，用于实现更高级别的身份认证。综合区块链技术，依据特征融合标准，部署具体的认证节点。通常情况下，为确保个人数据、信息的隐秘性与安全性，需要通过公钥和私钥结合设定加密结构，并将其与认证节点进行关联，组成多阶同步可控的认证结构。在公钥和私钥应用之前，标定明确具体的节点认证地址，形成数据信息的传输机制，为后续相关认证工作的执行营造环境。

1.3　部署模糊特征身份标识认证矩阵

结合认证需求，部署模糊特征标识认证矩阵。首先，根据模型的应用范围调整设定的公钥和私钥，并在初始的模型中预设固定的问题，形成身份标识认证矩阵的框架，通过各个区域设定的节点，采集实时数据以及信息，利用区块链技术测算此时的模糊认证单元 H，式(1)，完成对模糊认证单元的测算。

$$H = \frac{\beta_2}{(m+n)^2 \times \beta_1} + \sum_{i=1} n\beta_1 - mi^2 \qquad (1)$$

其中，m 表示预设认证范围；n 表示重复认证范围；β_1 和 β_2 分别表示认证偏差和认证模糊值；i 表示认证次数。

1.4　构建区块链 CNN 多特征融合认证模型框架

区块链技术的公有链、联盟链以及私有链之间也存在一定的应用联系，因此在多特征融合的背景下，结合卷积神经网络(CNN)，构建区块链融合 CNN 认证模型框架。依据上述部署的认证节点，采集实时的数据以及信息，将其以特定的形式转换为数据包，传输至认证矩阵的对应位置上。接收到数据包后，通过多个矩阵层级，再加上设定的区块链阶层作出数据的解析与比照核查。基于卷积神经网络，在公钥和私钥保护程序之前，设定一个加密识别结构。认证识别人员在输入密码或者生物识别之前，需要通过该加密识别结构。这部分主要是对相关人员的身份、证件号等进行核查，确保归属于该区域覆盖人员后，才可进行下一阶段的身份认证，具体结构如图 2 所示。

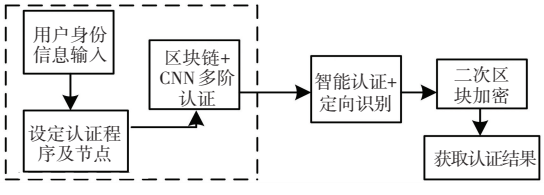

图 2　区块链融合 CNN 认证模型框架结构

Fig. 2　Block chain fusing CNN authentication model frame structure

根据图 2，本文设计并调整了区块链融合 CNN 认证模型框架结构，该身份识别认证框架是一对多识别，该模型的识别层级一定程度上可以接受多人同时进行身份认证，确保了认证的效率及质量，通过

若干卷积层和池化层进行降采样提取特征的形式，促使 CNN 区块认证最大池化，增强区块链融合 CNN 认证模型的实际应用能力。

1.5 区块链自适应密钥修正实现身份认证

自适应密钥修正主要是对错误的认证指令的一种定向修改和调节，多采用自适应识别认证，局限性较大，模型的表示认证错误往往会受到外部因素的影响，导致产生不可控的误差。此外，常见的认证方式如多维单幅人脸认证或虹膜认证，速度较快，但也面临较难控制的挑战。

因此，设定一个小型的密钥修正结构，在执行认证指令之前，需要提前调取识别人员的个人信息，预先进行核查与识别，确保无误差之后，才可以展开密钥输入页面，进行下一步的表示认证。

这种认证方式虽然可以提升认证的真实性与可靠性，但在设定修正的过程中，自身设定的标准并不是固定的，可以根据区块链技术的发展和应用情况的变动，对身份认证模型进行定期的调整，确保密钥修正结果的稳定，更好地完成多特征融合身份标识认证模型的构建。

2 实验结果及分析

本文针对基于区块链的多特征融合身份标识认证模型实际应用效果进行分析，考虑到最终测试结果的真实性与可靠性，选取 D 身份认证平台的执行模型作为测试目标。借鉴传统模糊多特征融合身份标识认证模型测试组、传统 ECC-ZKP 多特征融合身份标识认证模型测试组的设定，以及本文的区块链多特征融合身份标识认证模型测试组，根据实际的测定需求和标准，搭建基础的测试环境，并对最终获取的测试结果进行对比分析。

2.1 实验准备

首先，选定 100 人作为身份认证的对象，挑选 10 人作为模型需要识别的目标。在模型的控制平台输入这 10 人的定向识别特征，例如：脸部、眼睛等，同时完善这 10 人的身份认证信息，作为后续身份标识认证的参考信息。在控制程序中设置双向密钥，分别是公钥和私钥，同时达成实用拜占庭容错算法（Practical Byzantine Fault Tolerance，PBFT）认证共识协议，测算出此时的认证区块相似度标准。认证区块相似度 Q，式（2）：

$$Q = \nu + \sum_{e=1} \pi e - \frac{\tilde{\omega}\nu}{\nu e \times (\pi + \tilde{\omega})^2} \times \tau^2 \quad (2)$$

其中，ν 表示认证范围；π 表示预设认证单元值；e 表示认证次数；$\tilde{\omega}$ 表示相似认证偏差；τ 表示区块哈希值。

将认证区块相似度设定为目标对象身份标识认证的测定标准，综合区块链技术，进行具体的验证分析。

2.2 实验过程及结果分析

利用部署的认证节点进行技术数据、信息的采集，将其以特定的格式转换为数据包，传输至对应的认证矩阵；通过解析获取对应的认证档案；汇总整合后，将该信息存储至模型内部。

依据标准调整公钥和私钥的覆盖加密范围，对 100 人进行身份的定向识别，设定每个人的识别时间为 2 s，完成密码验证、人脸识别、身份核查、数据采集等环节，观察该模型对预设 10 人身份标识的认证情况，经过 5 次测定，测算出最终的认证识别率，具体的测试结果如图 3 所示。可见，对比传统测试组，区块链多特征融合身份标识认证模型的最终模型认证识别率可以达到 90% 以上，说明该模型对于测试对象的身份认证准确度更高，具有实际的应用价值。

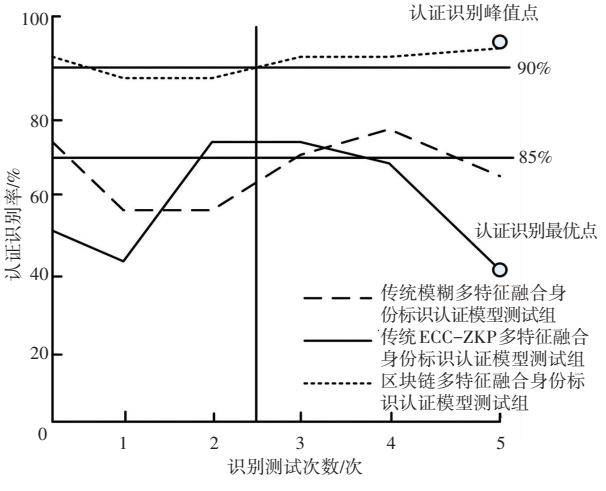

图 3 测试结果对比分析图

Fig. 3 Comparison analysis chart of test results

3 结束语

本文设计基于区块链的多特征融合身份标识认证模型。预处理多特征基础认证环境，构建循环式的多阶节点身份认证体系，设定多特征融合认证节点；结合认证需求，综合区块链技术，部署模糊特征标识认证矩阵；结合卷积神经网络，构建区块链融合 CNN认证模型框架；根据区块链技术的发展和应用

（下转第 146 页）