Computer Science and Application 计算机科学与应用, 2023, 13(10), 1928-1937
Published Online October 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1310191

Hans汉斯

身份认证技术研究综述

卢长青

沈阳航空航天大学计算机学院，辽宁 沈阳

收稿日期：2023年9月16日；录用日期：2023年10月16日；发布日期：2023年10月24日

摘　要

身份认证技术是对信息接收方进行身份鉴别的技术，也是保障信息安全的重要手段；随着移动互联网时代的到来，人工智能技术飞速发展，传统身份认证技术已无法满足人们对于隐私保护的需求，基于生物特征的生物识别技术应运而生。本文回顾了传统身份认证技术的发展历程，并从身份认证相关技术着手，重点介绍了基于生物特征的身份认证技术及其优缺点，在此基础上进一步阐述与人工智能技术相结合的身份认证技术，细化了生物特征身份认证技术的研究方向，文章末尾列出两种新型身份认证技术，着重介绍了区块链数字身份验证技术，这可以给与该领域内研究人员新的研究方向启发。文章总体论述了现阶段身份认证技术发展情况和未来发展趋势，对进一步做好身份识别工作具有一定的理论指导意义。

关键词

身份认证，综述，生物特征，特征匹配

Overview of Research on Identity Authentication Technology

Changqing Lu

School of Computer Science, Shenyang Aerospace University, Shenyang Liaoning

Received: Sep. 16th, 2023; accepted: Oct. 16th, 2023; published: Oct. 24th, 2023

Abstract

Identity authentication technology is a technology to identify the recipient of information, and is also an important means to ensure information security. With the advent of the mobile Internet era and the rapid development of artificial intelligence technology, traditional identity authentication technology has been unable to meet people's needs for privacy protection, and biometrics based on biometrics technology came into being. This paper reviews the development process of traditional identity authentication technology, and starts with related technologies of identity au-

文章引用: 卢长青. 身份认证技术研究综述[J]. 计算机科学与应用, 2023, 13(10): 1928-1937.
DOI: 10.12677/csa.2023.1310191

thentication, focusing on the biometric-based identity authentication technology and its advantages and disadvantages. On this basis, it further elaborates the identity authentication technology combined with artificial intelligence technology, and details the research direction of biometric identity authentication technology. At the end of the paper, two new identity authentication technologies are listed. The paper focuses on the blockchain digital identity authentication technology, which can inspire new research directions for researchers in this field. This paper discusses the current status and future development trend of identity authentication technology, which has a certain theoretical guiding significance for further identification work.

Keywords

Authentication, Overview, Biometrics, Feature Matching

1. 引言

身份认证也称“身份验证”，是指用某些方法进行用户身份确认的过程，人们常把身份识别和认证两个工作放在一起，统称为身份认证。在现实生活中，身份认证是不可避免的，各式各样的场合均需要进行个人身份认证，正因为我们每个人都是独一无二的个体，由此衍生出种类繁多的身份验证技术，且不同的技术拥有各自不同的优缺点。

验证主体身份的方法主要分为三大类，第一类是只有主体了解的秘密，例如口令、印章等；第二类是主体携带的物品，例如公交卡、身份证等；第三类是主体具有的特征，例如人脸、指纹和虹膜等[1]。目前，身份认证技术仍在不断发展和演变，伴随着人工智能和区块链技术的发展，基于主体特征的身份认证技术正变得愈发安全和智能。

2. 身份认证技术

身份认证技术的发展演变进程是从早期的口令到简单密码，再到生物特征和多因素认证技术，最后发展到无感知的身份认证技术，每种技术均有自己的特点和适用范围。按照身份认证技术的发展进程，本文将从三个部分进行叙述，分别是传统身份认证技术、基于生物特征认证技术和新型身份认证技术三大类[2] [3]，其中，基于生物特征认证技术还包括基于人工智能技术的身份认证技术。

2.1. 传统身份认证技术

传统身份认证技术大致分为三类，分别是口令和印章技术、简单密码技术和磁卡技术，这三类认证技术是按照时间线依次发展的。

(一) 口令、印章

在现代社会，居民身份证和户口簿成为了我们证明个人身份的有效凭证，那么，古人是如何验证自己身份的呢？古代社会对身份认证同样重视，约公元前 3000 年左右口令技术开始发展，在古代战乱时期，官兵进出城池均需按原先设定好的口令，以此辨别双方身份。公元前 500 年左右个人印章开始出现，在中世纪，身份验证通常是通过印章完成的，持有印章的个人可以在公共活动中证明自己的身份和荣誉，类似的身份验证方式还有很多。

(二) 密码技术

个人密码技术发源于公元前 400 多年，密码学的发展大致分为 3 个阶段，分别是 1949 年前的古典密码学阶段，1975 年前的科学密码阶段，1975 年后的秘钥密码阶段。互联网技术的发展为密码技术应用和普及奠定了基础，如下图 1 所示，现代密码技术从应用上分为静态密码、动态密码和短信密码。

Figure 1. Cryptographic classification and authentication principle
图 1. 密码技术分类及认证原理

用户名加密码也是一种常见的身份认证方式，在登陆账号时经常会用到。简单来说，就是账号和密码组合在一起验证某个人的身份，账号代表使用者的身份，密码用来验证使用者身份是否真实。早期密码是固定的，但是固定密码过于简单且容易被监听甚至破解，需要定期修改，于是就有了动态密码、密保卡和短信令牌等认证技术出现。

(三) 磁卡

随着计算机飞速发展，磁卡、条形码等逐渐成为验证身份的新方式，磁卡技术起源于上世纪 60 年代，由法国人发明，由于它存储信息量大，读写方便且便携，很快在世界各地得到广泛应用。人们可以使用身份证、银行卡、门禁卡等磁卡验证个人身份，他们内部存储了用户的个人信息，包括姓名、身份证号等身份相关的数据。这给身份认证工作带来了极大的便利。

2.2. 基于生物特征的身份认证技术

传统身份验证技术的优点是使用便捷，可以由合法用户随身携带，但也容易丢失或遗忘。“911”事件之后，随着国际恐怖组织不断出现，世界各地开始重视研发并应用生物识别技术，与口令、印章、密码、磁卡认证技术相比，生物特征识别技术具有更高的安全性和方便性，同时又具有唯一性，可以精确识别使用者身份，基于上述特点，生物特征识别技术[4] [5]逐渐成为传统识别技术的补充，甚至是替代技术。

生物认证主要分为两大类，一类是身体特征，另一类是行为特征。身体特征包括指纹、掌纹、虹膜、人体气味、手背静脉血管、人脸、DNA、耳廓和唇纹等，行为特征包括步态、手写签名等，传统认证算法流程较为相似，大致流程如图 2 所示，首先采集生物特征信息，对原始数据进行预处理，然后再经过特征提取、特征匹配等环节，最后识别出认证结果。

2.2.1. 身体特征识别技术

(一) 指纹识别技术

我们的手指和脚趾表面具有凹凸不平的纹路，生物统计学显示，这些纹路在形状、断点和交叉点上各不相同，这就造成了每个人的指纹都具有唯一性，我们可以根据这种生物特征进行身份认证，这就是指纹识别技术[6]。指纹识别技术优点众多，它具有唯一性、便携性、不易丢失、技术成熟等特性，随着

现代科学技术的发展，指纹应用技术迅速实现了现代化和自动化，也成为现有身份识别领域使用率最高的技术之一[7]。

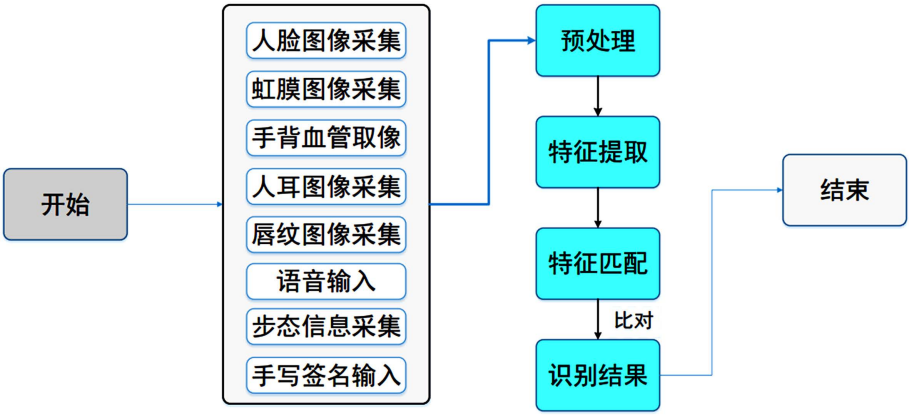

Figure 2. Authentication process based on template matching
图 2. 基于模版匹配的身份认证流程

(二) 掌纹识别技术

掌纹识别技术于 19 世纪晚期提出，是一种新型的利用生物特征识别身份的技术。掌纹是手指到手腕处的手掌纹路，这些纹路包括主线、皱纹、细小的纹理、脊末梢、分叉点等[8]，掌纹的形态由遗传基因决定，不可能完全一样，即使双胞胎兄弟，掌纹也会有细小的差别，因此掌纹同样具有唯一性。掌纹识别认证隐私性较好，通常在主动张开手掌时才能获取到，用户接受程度高，可靠性高，安全性好，不需接触便可识别，但是掌纹识别过度依赖于采集设备和具体场景，技术起步也较晚，因此并没有得到广泛应用。

(三) 虹膜识别技术

虹膜识别技术是根据人眼中的虹膜部位进行身份认证，人眼由虹膜、视网膜和晶状体等构成。虹膜处于眼角膜内部白色巩膜和黑色瞳孔之间，人类在胚胎发育时期就已经确定，并将终身保持不变，虽然肉眼很难分辨虹膜特征，但是通过红外线光照射可以清晰看到纹理[9]。虹膜识别是通过比对虹膜特征之间的相似度决定的，识别过程共分为以下四步：

a) 虹膜图像识别。

b) 图像预处理。

c) 虹膜特征提取和选择。

d) 特征匹配。

虹膜作为生物特征进行身份认证，具有唯一性、稳定性、可靠性高、不需物理接触等特点，该技术出现于 20 世纪 80 年代，发展起步较晚，与传统身份认证技术相比，虹膜具有 226 个生物特征点，因而具有更高的识别率，识别错误率也是所有生物识别技术中最低的，有数据显示，虹膜识别的错误率仅为 0.00077%，因此虹膜认证技术仍将是未来发展过程中重点研究对象[10]。

(四) 面部识别技术

面部识别技术起源于 20 世纪 50 年代的心理学研究，但是直到 60 年代才开始使用计算机展开面部识别研究工作[11] [12]。面部识别技术属于计算机视觉范畴，它是根据人体面部特征识别身份的技术，面部特征具有稳定性和唯一性，面部识别过程需要先识别输入的图片或视频流，识别出人脸，再根据人脸提取出身份特征，最后将该特征与事先已经存储的样本进行比对，从而识别出个人身份。虽然该技术已经被广泛应用到日常生活中，但是仍存在如下问题：

1) 算法准确度不够高。

2) 存在安全漏洞，出现人脸识别误判。

3) 人脸识别系统不完善，关键技术还需优化。

(五) 手背静脉血管识别技术

静脉识别技术是近十几年发展的一种新型身份识别方法，在诸多静脉识别技术分类中，研究和应用最多的是手背静脉识别。手背静脉血管是一种位于皮下的人体组织，相邻的静脉在手背相互连接起来组成独一无二的静脉网，用肉眼是很难观察到的。我们可以借用近红外设备产生光采集手背静脉图像，将采集到的图像使用滤波等方法处理，然后提取特征进行特征匹配，最后静脉识别[13]。

手背静脉血管身份识别技术的出现，是为了克服指纹识别、虹膜识别等生物特征识别技术的缺点，它不受皮肤表面粗糙等因素影响，也不会伤害人体组织，静脉识别的特点是具有较强的唯一性和普遍性，不会随着年龄的增加而改变。由于其位于表皮之下，采用非接触式采集，因此很难被复制或伪造。

(六) DNA 指纹鉴定技术

DNA 指纹是指具有完全个体特异的 DNA 多态性，它的身份认证能力可以和指纹相媲美，由此得名，这种方法具有绝对的权威性和准确性。DNA 指纹鉴定技术是使用生物学实验或计算机等手段提取 DNA 片段上的生物学特征，DNA 上包含所有的个体遗传信息，与身俱来，终身不变。这种生物遗传信息蕴含在所有人体组织和器官中，正因如此，DNA 指纹鉴定可以用于刑事案件侦查，但是 DNA 指纹鉴定也有一定的缺点，现阶段采样和提取时间长、设备成本高、身份认证速度慢、侵犯隐私等问题仍需进一步解决。

(七) 耳廓识别技术

耳廓识别技术是近年来新兴的生物识别技术，他是继面部识别、虹膜识别、指纹识别等成熟鉴定方式后，又一新型生物鉴定方法。人耳由外耳、中耳和内耳三部分组成，认证检测部位是外耳中的耳廓部分[14]，在 7~70 岁之间，耳廓形状、大小基本不会发生改变，这保证了耳廓作为生物认证部位的唯一性和稳定性，且它不受表情、妆容、胡子、眼镜等因素影响。人耳识别过程包括以下几个步骤：

a) 人耳图像采集。

b) 图像的预处理。

c) 人耳图像边缘检测与分割。

d) 特征提取。

e) 耳廓识别。

首先要做的是耳朵图像采集，由于图像尺寸小，数据处理量更小，因此整个采集过程用时很短。采集图像后最重要的部分是耳廓检测，检测性能可以影响整个认证效果，精准定位到有效耳廓后，再进行特征点定位和特征提取，最后将提取到的特征跟数据库中特征进行对比。耳廓识别技术的稳定性好、采集方便、生物特征明显，随着技术不断迭代，该技术会有更加广阔的应用空间。

(八) 唇纹识别技术

唇纹识别算法研究是近年的热点，正日趋成熟。唇纹指的是唇黏膜上皱纹和沟壑所形成的特定图案，每个人的嘴唇纹路都不一样，而且唇纹不会随着年龄的变化而变化，唇纹隐蔽性好，不易被复制，具有唯一性、特异性和遗传性，已在医学、司法鉴定等领域得到广泛应用。唇纹识别的具体步骤如下：

a) 首先进行唇纹图案定位，唇纹图案纹理通常不够清晰，需要做滤波处理。

b) 然后提取唇纹图像特征。

c) 最后进行特征匹配，一般采用距离和相似度两种方法。

唇纹应用还存在两大问题，第一个是嘴唇的活动能力较强，活动时力的大小、接触面积、干燥程度均会影响唇纹图案，会导致唇纹图案容易变形。第二个是虽然大街小巷布满了摄像装置，但是大部分摄像头普遍像素不高，难以拍清嘴唇纹路图案。

(九) 人体气味识别技术

人体气味识别是一种全新的生物身份认证技术，现在仍在探索阶段，人的身体是一种味源，每个人都有与众不同的气味，使用这种独特的气味便可以发现“你是谁”。但是这种技术还不够成熟，识别正确率较低，仍需不断完善实验算法，提高识别精度。

总的来说，以上所有生物识别技术最大的特点是具有唯一性，在安全性、便携性和适用范围广等方面也存在巨大优势，这使得该技术迅速普及。但也存在成本高、识别率低、隐私性差等问题，因此在生物识别技术的选择上，还需要结合具体应用场景进行合理选择。

2.2.2. 行为特征识别技术

基于生物特征的身份识别相对比较直观，而且具有较高的识别精度，但是生物特征采集时常常会侵犯生物个体隐私，因此我们仍然需要寻找非接触性的身份识别方法。随着身份识别技术的发展，声纹识别技术、步态识别技术和手写签名技术陆续应用到人们的日常生活中。

(一) 声纹识别技术

语音是人的一种自然属性，由于发声器官结构的细微差异和发声习惯不同，每个人的声音同样具有个人色彩。声纹是使用电声学仪器将声波特征转换成波普图形产生的，研究证明，声纹不会因为语气、声调等变化而改变，不仅具有特定性，还具有稳定性[15] [16]，声纹识别的原理是将未知语音通过电声学仪器转换成声纹，与数据库中已有的声纹样本进行对比，再根据语音特征判断是否是同一个人。声纹技术在各大领域均有广泛应用，例如银行、证券、公安司法、网络支付和声纹锁控等，缺点是不同的收声设备、环境噪音和多人混合说话均会对识别结果产生干扰。

(二) 步态识别技术

步态是一种较为复杂的行为特征，指的是人们行走时的姿态，步态识别是一种新的行为特征识别技术，目的是通过走路姿态进行身份认证。步态识别主要包括 3 项关键技术，分别是步态分割、特征提取和特征比对，其中步态分割是最基本的环节，需要用运动分割算法将人从不同的场景中识别出来，常用的运动分割算法有背景剪除法、时域差分法、光流法，步态特征提取是利用某种算法将检测到的步态进行表示，特征提取算法的好坏会直接影响最终的识别性能。与现有的基于生物特征的身份识别技术相比，步态识别的优势在于无接触，且不受距离影响，对图像的分辨率要求较低，步态识别技术现阶段主要应用于身份认定、犯罪嫌疑人追踪等方面。

(三) 手写签名技术

手写签名是一种生物行为特征，与其他行为特征相比，比较容易使人接受，没有侵犯性。手写签名认证分为离线签名和在线签名两大类，离线签名已经有几千年的历史，是自古以来最常见的身份鉴定手段，因为书写习惯一经形成很难改掉，每个人的签字都带有自己的个人特色，这种方法常被用于字迹鉴别这种特定领域。基于传统的离线签名技术，结合电子设备发展出了在线电子签名技术，在线签名除了记录笔迹，还可以记录书写速度、握笔压力和倾斜度等动态个人信息[17]。在线手写签名验证流程分为五个步骤，分别是签名采集、数据预处理、特征提取、模型特征训练和匹配算法等模块。

在线签名技术具有签署高效、管理快捷、节省成本和数据安全等特点，但是该技术发展至今仍然存在很多短板，例如书写环境、书写姿势、手写板材质、手写笔型号等都会影响身份认证识别率。如果使用扫描仪扫描签名，待扫描图片在转换成电子签名过程中，字迹可能会变模糊，从而降低识别准确率，签名还具有易模仿性，现有算法很难保证较高的准确性。

表 1 将上述基于生物特征的身份识别方法放在一起，从准确率、安全性、市场占有率等多方面进行对比，从表中可以很直观的看出各个方法的特点。从总体看来，生物认证技术的优缺点也很显著，优点是不易被坏人盗取，有较好的防伪性，可以随时随地使用，方便快捷，缺点是识别的稳定性和准确性较差，识别设备的研发成本和售价较高，推广难度大，无法做到真正的安全。

Table 1. Biometric authentication technology performance table
表 1. 生物特征身份认证技术性能表

生物特征	准确率	安全性	市场占有率	是否接触	应用成本
面部识别	高	中	高	否	低
虹膜	高	高	低	否	高
耳廓	低	中	低	否	低
气味	低	低	低	否	高
指纹	高	高	高	是	低
掌纹	高	高	低	否	低
声纹	高	中	中	否	低
步态	低	低	低	否	高
DNA	极高	极高	中	是	高

2.3. 基于人工智能技术的身份认证

在最近几年，人工智能技术(AI)一直被各行各业关注，它的应用极大提升了生产生活的便利性。人工智能包含机器学习、深度学习和计算机视觉等领域，它是一个十分广泛的学科，具有智能性和便捷性等特点，随着人工智能技术的飞速发展，身份识别领域也将随之迎来一场大变革。

(一) 基于 AI 的声纹识别技术

声纹识别技术的发展共分为两个阶段：

第一阶段(传统识别方法)：在 2000 年之前，主要使用模板匹配方法进行身份识别，这一阶段属于声纹识别技术发展初期，利用动态时间规整(DTW)等算法测试和训练特征序列，这一阶段的特点是只能识别相同内容，例如，如果要验证某个人的身份，他说的话仅限于数据库中已经存在的语句，否则将无法识别，这种方法需要录入大量数据，鲁棒性不强。

第二阶段(基于 AI 的声纹识别方法)：2010 年左右，声纹身份认证技术主要基于 iVector/PLDA，该技术可以通过因式分解，压缩每个音频长度，把语音映射到固定的低维向量上。再配合 PLDA(一种信道补偿算法)，这样就解决了模板匹配方法鲁棒性不强的问题。近几年，美国的约翰霍普金斯大学 David Snyder 等人又提出了 Siamese network (孪生神经网络)、xVector 等方法，这些方法比 iVector 具有更好的噪声鲁棒性。

在未来的声纹技术发展中，人工智能技术仍将占据主导地位。

(二) 基于深度学习的面部识别技术

传统面部识别技术是先进行人脸数据特征提取，再进行人脸特征相似度匹配。这种生物识别技术给人们生活带来了极大的便利性，但是同样面临很多问题，例如数据库数据不足、面部有遮挡物、光线弱、妆容过浓等。深度学习是人工智能技术的一个分支，更注重在应用过程中自主学习，深度学习与面部识

别的结合使得该技术有了突破性的进展[18] [19]，基于深度学习的面部识别技术可以应用在特定环境下，快速处理大量人脸数据、自适应各种场景，提高识别准确率。

3. 新型身份认证技术

由于传统生物特征技术存在一定的局限性，容易遭遇被仿造、隐私泄露等挑战，使得区块链数字身份验证、基于心电信号的身份识别等方法成为热门研究领域。

3.1. 区块链数字身份验证

传统身份认证方法存在较多弊端，很容易造成隐私泄露，也容易被伪造信息，区块链技术的出现为身份认证领域提供了一种全新的解决方案[20] [21]

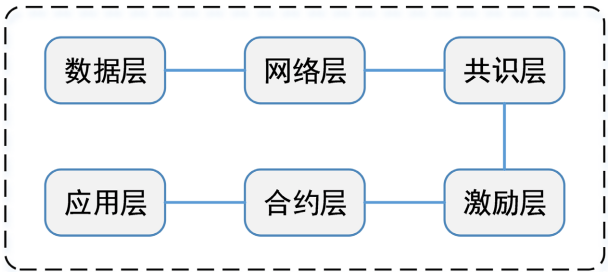

Figure 3. Blockchain model architecture
图 3. 区块链模型架构

区块链概念在 2008 年由中本聪提出，如上图 3 所示，区块链的模型架构由自下而上的数据层、网络层、共识层、激励层、合约层和应用层组成，主要原理是将保存信息的区块按时间顺序组成链条，并把他们链接在一起，与传统网络相比，区块链技术具有两大优点，一个是去中心化，另一个是数据难以被篡改[22]。基于区块链的数字身份认证方法是通过公钥和数字证书来实现身份验证的，用户将身份信息封装为各个区块，将签名信息上传到区块链网络，最后实现身份信息上链共享。这样，用户在区块链上的身份认证就得以实现。

3.2. 基于心电信号的身份识别

心电信号(ECG)是心脏跳动时产生的生物电势，也是心脏活动的直观体现，每个人的心脏大小、形状位置等都不同，这也就导致了每个人的心电信号都具有唯一性。基于心电信号的身份识别[23]包括两个阶段：训练阶段和测试阶段，训练阶段主要是对待测对象提取特征信息，保存到数据库中，测试阶段同样要提取心电图中的个人身份特征，最后使用分类器与数据库中的数据进行匹配[24] [25]。心电信号的最大优点是不容易造假、可信度高，不足地方在于目前尚未有统一标准定义波形边界位置，这会直接影响身份识别性能。

综上所述，传统识别技术、生物识别技术和新型身份识别技术各有优劣势，也拥有各自适合的应用场景，没有任何一种身份认证方式是完美适配所有场景的。随着科学技术的不断发展，未来还会有更多更新的身份认证技术涌现出来，为我们的生产生活带来更多便利。

4. 性能指标

身份认证技术常用的性能评价指标是 TP、TN、FP、FN 和 FAR、FRR。其中字母 T 表示 True (正确)，F 表示 False (错误)，P 表示 Positive (正样本)，N 表示 Negative (负样本)。

TP (TruePositive)：被分类器模型预测为正样本，实际也为正样本。

TN (False Negative)：被分类器模型预测为负样本，实际也为负样本。

FP (True Positive)：被分类器模型预测为正样本，实际为负样本。

FN (False Negative)：被分类器模型预测为负样本，实际为正样本。

FAR (False Accept Rate)一般称为误识率，意思就是将非法用户误认为合法用户，表示错误拒绝的比例，计算方式如公示 1 所示：

$$\mathrm{FAR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}\times 100\% \tag{1}$$

FRR (False Rejection Rate)一般称为拒识率，意思就是将合法用户误认为非法用户，表示错误接受的比例，计算方式如公示 2 所示：

$$\mathrm{FRR}=\frac{\mathrm{FN}}{\mathrm{FN}+\mathrm{TP}}\times 100\% \tag{2}$$

5. 展望

身份识别技术是未来数字化社会中不可或缺的一部分，在未来很长一段时间里，身份认证技术都将拥有广阔的前景和发展趋势。

一方面，无论是传统生物认证技术还是新型认证技术均有其不足之处，传统生物识别技术识别率较低且容易被伪造，如将生物认证技术与人工智能和机器学习等技术相结合，例如，将深度学习技术和人脸识别技术相结合，基于深度学习的人脸识别技术可以极大降低拒识率，该技术的本质是人工智能技术可以对生物特征数据进行更深层次的分析和处理，从而发现细节和特征，进而降低伪造可能性，提高认证准确率。未来，随着技术的不断进步和应用场景的不断扩大，我们有理由相信这一领域将会取得更多的突破和创新。

另一方面，在许多领域，包括电子商务、电子政务等，区块链加数字身份的结合具有巨大的应用价值，随着基于区块链数字身份验证、基于深度学习的特征识别等技术算法的不断改进，区块链身份认证可以与生物特征识别技术相结合，提高身份认证的准确性和安全性。例如，利用人脸识别和指纹识别等技术，可以在区块链上存储和验证用户的生物特征信息。区块链身份认证技术的发展前景广阔，它将为用户、企业、政府等提供更加安全、便捷、高效的身份认证服务，推动数字化社会的发展。

此外，虽然生物识别技术被各行各业应用，但是数据库数据无法统一，因此建立国家级身份认证特征数据库势在必行，随着特征库的建立，身份认证准确率必将大大提高。建立国家级身份认证特征数据库具有广泛的应用前景和潜力，它可以作为社会信用体系的基础设施之一，社会、经济、金融等多个领域提供更加安全、可靠、便捷的身份认证服务，推动数字化社会的快速发展。同时，需要加强技术研发、政策支持、隐私保护等方面的工作，以确保该数据库的顺利建设和应用。

总的来说，随着科技进步越来越快，数字化社会快速发展，各种新的技术和方法不断涌现，身份识别的准确性和安全性提高。因此身份认证技术也将更加多元化、自动化和智能化，同时也将在更多的领域得到应用，从而为网络安全和隐私保障提供更有效的保障。

6. 总结

身份认证技术已经渗透到生活中的各个角落，它是保护隐私、保证信息安全的重要手段，未来，身份认证技术还将进入到更多领域，为大家的生活带来更多便利。本文从传统身份认证技术、基于生物特征身份认证技术和新型身份认证技术三个方面阐述现有身份认证技术，剖析该技术的优缺点及总体发展趋势，有助于初次接触本领域的技术人员快速了解身份认证领域发展现状。

参考文献

[1] 李聪聪, 纪寿文, 范修斌, 等. 认证体制综述[J]. 信息安全研究, 2016, 2(7): 649-659.

[2] He, H.Y. (2014) Research on the Network Security and Identity Authentication Technology. *Advanced Materials Research*, **926-930**, 2819-2822. https://doi.org/10.4028/www.scientific.net/AMR.926-930.2819

[3] 贺斌. 身份认证的理论与技术[J]. 长江大学学报(自然科学版), 2004, 1(1): 19-22.

[4] Palma, D. and Montessoro, P.L. (2022) Biometric-Based Human Recognition Systems: An Overview. *Recent Advances in Biometrics*, **27**, 1-21. https://doi.org/10.5772/intechopen.101686

[5] Rajasekar, V., Saracevic, M., Hassaballah, M., *et al*. (2023) Efficient Multimodal Biometric Recognition for Secure Authentication Based on Deep Learning Approach. *International Journal on Artificial Intelligence Tools*, **32**, Article ID: 2340017. https://doi.org/10.1142/S0218213023400171

[6] Sarfraz, M. (2021) Introductory Chapter: On Fingerprint Recognition. IntechOpen, London. https://doi.org/10.5772/intechopen.95630

[7] 聂鹏, 耿文波. 指纹识别技术浅谈[J]. 电脑知识与技术(学术交流), 2007, 3(17): 1422-1423.

[8] 李绅龙, 宋鹏飞. 掌纹识别技术专利分析[J]. 中国科技信息, 2021(3): 31-33.

[9] 秦媛媛, 赵园园, 徐纪恒. 虹膜识别技术在门禁系统中的应用探究[J]. 湖北农机化, 2019(23): 92-93.

[10] 朱爱青. 基于虹膜的身份认证技术研究[J]. 计算机仿真, 2011, 28(10): 269-273.

[11] 宋振中, 王谦. 人脸识别数据处理法律问题研究[J]. 信息网络安全, 2021(S1): 82-85.

[12] Yuan, B., Du, C.Q., Wang, Z.Y. and Zhu, R. (2021) Research on Intelligent Algorithm of Identity Authentication Based on Facial Features. *Wireless Communications and Mobile Computing*, **2021**, Article ID: 5558578. https://doi.org/10.1155/2021/5558578

[13] 张馨午, 刘远远, 齐千妍, 等. 基于底层特征提取的手背静脉识别方法研究[J]. 电子设计工程, 2022, 30(15): 189-193.

[14] 孙晓鹏, 李思慧, 王璐, 等. 耳廓点云形状特征匹配的路径跟随算法[J]. 软件学报, 2015, 26(5): 1251-1264.

[15] 彭诗雅. 声纹识别技术研究[C]//中国通信学会. 第十六届全国青年通信学术会议论文集(上). 北京: 国防工业出版社, 2011: 253-256.

[16] Hanifa, R.M., Isa, K. and Mohamad, S. (2021) A Review on Speaker Recognition: Technology and Challenges. *Computers & Electrical Engineering*, **90**, Article ID: 107005. https://doi.org/10.1016/j.compeleceng.2021.107005

[17] Makkar, G.D. and Goyal, P. (2023) Combined Static and Dynamic Features Extraction from Handwritten Signature. *Scandinavian Journal of Information Systems*, **35**, 468-475.

[18] 付学桐. 基于深度学习的人脸识别技术研究[J]. 通讯世界, 2019, 26(2): 299-300.

[19] 张顺, 龚怡宏, 王进军. 深度卷积神经网络的发展及其在计算机视觉领域的应用[J]. 计算机学报, 2019, 42(3): 453-482.

[20] Chen, Z.X. and Wu, S.F. (2021) Research on Digital Identity Authentication Technology Based on Block Chain. *Journal of Physics*: *Conference Series*, **1802**, Article ID: 032091. https://doi.org/10.1088/1742-6596/1802/3/032091

[21] Wang, T.C., Shen, H.M., Chen, J., *et al*. (2023) A Hybrid Blockchain-Based Identity Authentication Scheme for Mobile Crowd Sensing. *Future Generation Computer Systems*, **143**, 40-50. https://doi.org/10.1016/j.future.2023.01.013

[22] 滕鹏国, 刘飞. 一种基于区块链的身份认证方法[J]. 通信技术, 2021, 54(5): 1214-1219.

[23] Rajani Kumari, L.V., Padma Sai, Y. and Balaji, N. (2021) R-Peak Identification in ECG Signals Using Pattern-Adapted Wavelet Technique. *IETE Journal of Research*, **69**, 2468-2477. https://doi.org/10.1080/03772063.2021.1893229

[24] 李伟, 原建平. 基于编码融合的心电图身份识别方法[J]. 网络新媒体技术, 2022, 11(5): 41-45.

[25] Prakash, A.J., Patro, K.K., Hammad, M., Tadeusiewicz, R. and Pławiak, P. (2022) BAED: A Secured Biometric Authentication System Using ECG Signal Based on Deep Learning Techniques. *Biocybernetics and Biomedical Engineering*, **42**, 1081-1093. https://doi.org/10.1016/j.bbe.2022.08.004