Artificial Intelligence and Robotics Research 人工智能与机器人研究, 2024, 13(3), 565-570
Published Online August 2024 in Hans. https://www.hanspub.org/journal/airr
https://doi.org/10.12677/airr.2024.133058

Hans汉斯

一种基于人脸的生物密钥派生方案

易　钢，岳笑含

沈阳工业大学信息科学与工程学院，辽宁　沈阳

收稿日期：2024年5月6日；录用日期：2024年8月20日；发布日期：2024年8月28日

摘　要

本文提出了一种基于人脸的生物密钥派生方案。该方案利用人脸特征作为生物识别的基础，通过采集、分析和提取人脸图像中的特征信息，并将其转化为数字化的生物密钥。在派生过程中，结合了图像处理技术和加密算法，确保生物密钥的安全性和唯一性。此外，本方案还考虑了人脸识别的准确性和实时性，通过优化算法和提高识别速度，提升了系统的性能表现。实验结果表明，所提出的基于人脸的生物密钥派生方案在生物识别领域具有良好的应用前景和可行性，可为安全认证系统的设计和实现提供一种有效的解决方案。

关键词

密钥派生，生物密钥，纠错码

A Face-Based Biometric Key Derivation Scheme

Gang Yi, Xiaohan Yue

Department of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning

Received: May 6th, 2024; accepted: Aug. 20th, 2024; published: Aug. 28th, 2024

Abstract

This paper proposes a facial-based biometric key derivation scheme. The scheme utilizes facial features as the basis for biometric recognition, by collecting, analyzing, and extracting feature information from facial images, and converting it into digital biometric keys. During the derivation process, a combination of image processing techniques and encryption algorithms is employed to ensure the security and uniqueness of the biometric keys. Additionally, the scheme considers the accuracy and real-time performance of facial recognition, enhancing system performance through

文章引用: 易钢, 岳笑含. 一种基于人脸的生物密钥派生方案[J]. 人工智能与机器人研究, 2024, 13(3): 565-570.
DOI: 10.12677/airr.2024.133058

algorithm optimization and increased recognition speed. Experimental results demonstrate that the proposed facial-based biometric key derivation scheme holds promising prospects and feasibility in the field of biometric recognition, providing an effective solution for the design and implementation of secure authentication systems.

Keywords

Biometric Features, Key Derivation, Error Correct Code

1. 研究背景

随着信息技术的迅速发展和智能设备的普及，个人数据的安全性和隐私保护成为了日益重要的议题。传统的密码学方法虽然在数据保护方面发挥了重要作用，但是密码管理和记忆的负担逐渐成为了用户的一大挑战。低熵的口令容易被猜测或破解，而且难以记忆，同时密码的管理和更新也会给用户带来诸多不便。为了解决这一问题，生物识别技术应运而生，其利用个体独特的生理或行为特征进行身份验证，为用户提供了更加便捷和安全的身份验证方式。在众多生物识别技术中，人脸识别因其无需接触、易于采集以及用户友好性等特点而受到了广泛关注。然而，传统的人脸识别系统往往存在着一定的局限性，如受光照、角度、表情等因素的影响，容易造成识别准确率的下降。因此，基于人脸生物特征的密钥派生方案成为了研究的热点之一。通过将个体的人脸特征信息转换为安全密钥，不仅可以提高身份验证的准确性和安全性，还能够简化用户的密码管理流程，从而更好地满足了现代信息安全的需求。

生物特征密钥技术是首先对人的生物特征进行取样，然后提取其唯一的特征并且转化成数字密钥的技术。生物特征密钥技术的输入是生物特征信息，输出是一个均匀、随机、安全的密钥。由于人的生物特征数据可以随身携带，方便使用。另外，从用户的生物特征中提取密钥不需要外部额外的信息，因此生物特征密钥技术已经出现就成为了研究热点。

从生物特征中提取密钥需要满足 4 个基本要求[1]：

1) 稳定性：从同一个生物特征中提取的密钥波动小。

2) 可区分性：从不同的生物特征中提取的密钥不相同。

3) 可撤销性：只要重新输入生物特征便可生成一个新的密钥。

4) 安全性：a) 生成的密钥长度应该满足安全性要求；b) 不能从密钥中泄露原始生物特征信息。从生物特征中派生密钥的基本原理是从单个生物特征信息(指纹，人脸图片，虹膜，声纹等)中提取足够多的特征点，然后利用密码学的原语形成密钥。但是生物特征信息的采集易受到采集设备、现场环境、光照和角度等外界条件的影响，因此很难采集出完全相同的生物特征数据。下图 1 是常用的 7 种生物特征。

2013 年，Venckauskas 等人[2]提出利用指静脉图像来生成生物密钥。该方案是首次将指静脉图像用于密钥提取。遗憾的是该文献只是一个理论模型，并没有给出实验仿真与分析。2006 年，Juels 等人[3]提出了一种称为模糊金库(Fuzzy Vault)的方法。其策略是利用用户的具有唯一性的某特征集合，如用户的特定喜好的数字化集合，来保存用户的数字化秘密信息。模糊金库其实是一种秘密共享的机制，目的是保护用户的生物特征模板和用于恢复用户的密钥。缺点也是显而易见的，需要额外的存储空间，安全性也不高。2016 年，魏宁等人[4]提出了一种利用 X.509 数字证书和模糊金库技术完成了密钥的绑定。这种方

案可以实现生物特征模板公开。2017 年，Anees 等人[5]提出了一个基于人脸细节特征的安全密钥生成算法。该算法提出一种二维特征学习算子，这个算子可以更准确地学习和提取人脸特征，然后可以直接量化生成生物密钥。但是密钥提取的成功率和鲁棒性较低。2021 年，Wang 等人[6]提出了一种基于 SENet 结构的深度神经网络生物密钥生成模型，结合深度学习技术实现了安全生物特征密钥派生。然而，由于生物特征的复杂性和不稳定性，以及端到端生成模型的低可解释性和低可控性，该模型在实际生物特征数据库中的测试效果并不理想。很多国内外的学者开发了很多基于模糊提取器的生物密钥生成方案[7]-[10]，实际上是对模糊提取器理论的改进和完善。2010 年，Wu [10]不仅提出了自己的生物密钥提取方案，还提出了生物密钥的恢复方案。

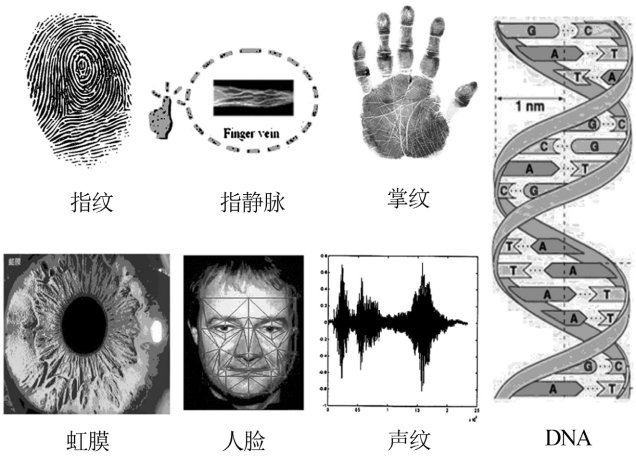

Figure 1. The seven common biometric features
图 1. 常用的 7 种生物特征

纵观国内外生物密钥领域的研究，本文发现生物密钥提取技术主要基于指纹和虹膜这 2 个生物特征，可以说从指纹和虹膜提取生物密钥的技术已经比较成熟。但是由于指纹和虹膜的生物特性，在使用时均需要用户近距离靠近识别设备进行采集，给用户带来一定的不便。近年来，对生物密钥的研究主要集中在模板保护、密钥生成和密钥应用三个方面。以上的研究主要是在密钥生成方面。在生物特征模板进行加密保护的技术研究方面主要有[11] [12]。2019 年，Droandi 等人[13]提出一种基于多生物特征的识别系统 SEMBA，该系统利用人脸和虹膜特征，依靠安全多方计算进行实现。在此背景下，本论文旨在提出一种基于人脸特征信息的密钥派生方案，并设计实现相应的原型系统，以评估其在安全性、功能性和性能方面的表现。通过对该方案进行综合的测试和评估，可以为生物识别技术在数据加密和身份验证领域的应用提供重要的理论和实践基础。

2. 方案的模型和形式化定义

算法定义

在本方案的系统模型中，用户首先用视频采集设备获取用户的人脸图像 img，然后进行图像的预处理后得到人脸特性信息，也就是特征模板 W_0，之后用 KDF 函数提取生物密钥 R_0，然后用 BCH 编码函数进行编码得到 R_0'，最后计算 $pd = w_0 \oplus R_0'$，把 pd 保存在云服务器中。

下面给出了本方案系统模型的形式化定义：

1) 人脸图像采集算法 Capture $(\text{img}) \to$ feature vector：该算法由用户执行，用户用图片采集设备采集人脸图像，然后提取脸部 68 个点，获取特征信息。

2) 预处理算法 $\mathrm{Pr}ocess(\text{feature vector}) \to w_0$：在用户端执行，根据用户的特征信息生成生物模板信息。

3) 密钥提取算法 $\mathrm{KDF}(w_0) \to R_0$：在用户端执行，根据用户的模板信息生成生物密钥。

4) BCH 编码算法 $\mathrm{BCH\_EN} \to R_0'$：在用户端执行。将用户的生物密钥编码成 R_0'。

5) 异或操作 $\mathrm{XOR}(R_0', w_0) \to pd$：该算法由用户执行，把 R_0' 和 w_0 异或成 pd 后保存在服务器端。

3. 方案的具体构建

基于第 2 章的所述的方案模型，本章给出了方案的具体构建，包括用户生物密钥注册和生物特征秘钥派生阶段的几个主要算法给出了详细的描述。

生物密钥派生

用户密钥注册步骤旨在提取面部生物特征模板 W 并构建未来恢复目的的辅助公共数据。在技术上，在注册阶段详细过程如下：

1) 脸部图像采集

采集用户脸部图像次，并从个样本从提取出脸部特征样本值分别为$(x_1, x_2, \cdots, x_n)$，然后根据这个样本值来计算均值和方差，然后计算出标准值。

$$\overline{x}_i = \frac{x_1 + x_2 + \cdots + x_n}{n} \tag{1}$$

$$\sigma^2 = \frac{\sum_{j=1}^{n}\left(x_j - \overline{x}_i\right)^2}{n} \tag{2}$$

$$f_i = \frac{x_i - \overline{x}_i}{\sigma} \tag{3}$$

将均值向量表示为 $\overline{x} = (x_1, x_2, \cdots, x_d)$，方差向量表示为 $\sigma = (\sigma_1, \sigma_2, \cdots, \sigma_n)$，样本特征向量表示为 $f = (f_1, f_2, \cdots, f_n)$。这里 d 表示生物特征的维数。

2) 数据预处理 $\mathrm{Pr}ocess(\text{feature vector}) \to W_0$

将特征向量值量化，并将其转换为高度可区分的二进制字符串(W_0)。W_0 的计算公式为：

$$f_i = \begin{cases} 0, x_i < 0 \\ 1, x_i > 0 \end{cases} \tag{4}$$

3) 密钥提取函数 $\mathrm{KDF}(w_i) \to R_0$：使用密钥派生函数生成一个均匀密钥 R_0。

4) BCH 纠错码编码函数 $\mathrm{BCH\_EN}(R_0) \to R_0'$。

5) 异或操作 $\mathrm{XOR}(w_0, R_0') \to pd$：计算公共数据 $pd = w_0 \oplus R_0'$，并将 pd 和 $H(R_0')$ 发送到云服务器或认证中心。

4. 仿真实验和性能分析

为了分析系统的实际性能并审查相关文献，搭建了本论文方案的原型系统，并利用面部图像数据集 ABERDEEN 和 dlib 库进行了一系列仿真实验。实验使用 Python 3.11 和 PyCharm 2022。在实验结果中，本文还展示了面部生物特征认证的准确性和性能。

4.1. 实验平台

本实验在笔记本 PC 上构建了实验环境，环境的各项配置参数如下表 1 所示。

Table 1. Configration of our experiments platform
表 1. 实验平台参数

操作系统	Windows 11 家庭中文版
CPU	12th Gen Intel(R) Core (TM) i5-12500H 2.50 GHz
内存	16.0 GB
开发环境	PyCharm 2022，Python 3.11
库	OpenCV 2.0
数据集	ABERDEEN

定位脸部的 68 个特征点，然后用 Open CV 模块获取到人脸的特征值 w_0 (128 维度)，然后从 w_0 提取出 $L=88$ 的中间信息 R_0。在使用哈希函数将进行哈希变换，并将哈希值 $H(R_0)$ 存入数据库文件；同时用 BCH (137, 5)对进行编码得到 R_1'，然后用 R_1' 和 w_0 进行异或操作得到公开信息 pd，也存入数据库文件。认证时，平台使用同样的方法获取人脸特征信息 w_1，将 w_1 与数据库中辅助信息 pd 进行异或操作得到 R_1'，然后对进行 BCH 译码操作得到 R_1。然后对 R_1 进行哈希操作用哈希值 $H(R_1)$ 与数据库中的 $H(R_0)$ 进行比对，如果比对成功，则认证成功。

4.2. 实验结果

实验分析

为了全面地分析本实验中方案的表现，本文采用生物特征加密中通用的评价标准：

1. 准确率(%)，是测试图像认证成功的概率。由于存在光照、遮挡、表情等外界因素的干扰，使得每次获取的图像都会存在差异，也就是说测试不能将每幅图像都认证成功，即认证率达不到 100%。识别率越高系统性能越好。

2. 错误接受率(FAR, %)，是非法用户通过认证的概率。FAR 越低系统排除非法用户的能力越高。

3. 认证时间(s)，是指系统从进入认证过程到得出认证结果所消耗的时间，认证时间越短，算法越好。

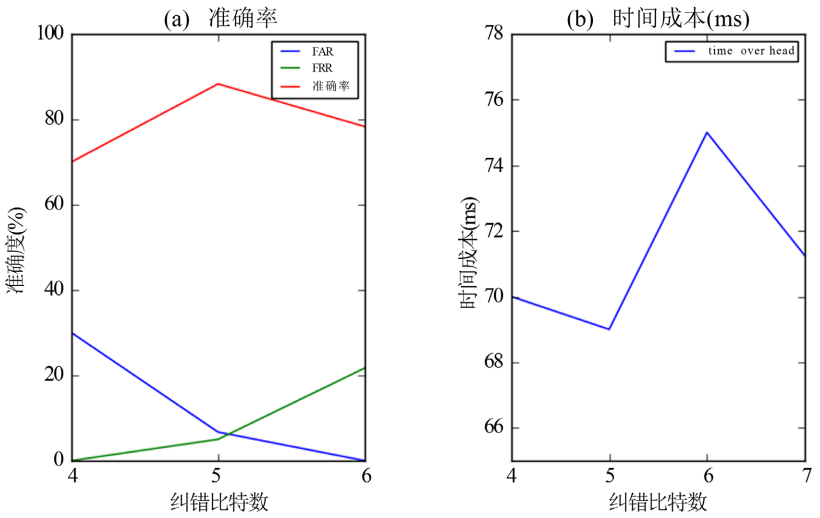

Figure 2. Accuracy and time cost
图 2. 系统模型准确度和时间代价

根据评价标准，本实验的实验验证结果如图 2 所示。从实验结果来看，纠错码 ECC 的纠错能力在 5

bit 时，能实现最好的准确率 88.7%，而且从时间成本来看，在纠错能力在 5 bit 时，也可以达到最优的时间消耗 69 ms。

5. 结论

通过本文的研究，我们成功提出了一种基于人脸的生物密钥派生方案，该方案利用了人脸特征作为生物识别的基础，并通过采集、分析和提取人脸图像中的特征信息，将其转化为数字化的生物密钥。在派生过程中，我们结合了图像处理技术和加密算法，以确保生物密钥的安全性和唯一性。此外，我们还考虑了人脸识别的准确性和实时性，通过优化算法和提高识别速度，有效提升了系统的性能表现。实验结果验证了所提出方案的有效性和可行性，在生物识别领域具有广阔的应用前景。本文的研究为安全认证系统的设计和实现提供了一种有效的解决方案，为应对日益复杂的安全挑战提供了新的思路和方法。未来的研究方向包括进一步优化算法、提高生物识别的准确性和鲁棒性，以及探索基于人脸生物密钥的更广泛应用场景。

综上所述，本文的研究为人脸识别技术和生物识别领域的发展做出了贡献，为构建更安全、高效的认证系统提供了重要参考和指导。作为未来工作的一部分，以下探索方向值得后来的研究学者们继续研究和探索。

参考文献

[1] 游林. 生物特征密码技术综述[J]. 杭州电子科技大学学报(自然科学版), 2015, 35(3): 1-17.

[2] Venckauskas, A. and Nanevicius, P. (2013) Cryptographic Key Generation from Finger Vein. *International Journal of Engineering Sciences and Research Technology*, **2**, 733-738.

[3] Juels, A. and Sudan, M. (2006) A Fuzzy Vault Scheme. *Designs, Codes and Cryptography*, **38**, 237-257. https://doi.org/10.1007/s10623-005-6343-z

[4] 魏宁. 基于生物特征模板公开的密钥生成与应用研究[D]: [硕士学位论文]. 天津: 天津工业大学, 2016.

[5] Anees, A. and Chen, Y.P. (2018) Discriminative Binary Feature Learning and Quantization in Biometric Key Generation. *Pattern Recognition*, **77**, 289-305. https://doi.org/10.1016/j.patcog.2017.11.018

[6] Wang, Y., Li, B., Zhang, Y., Wu, J. and Ma, Q. (2021) A Secure Biometric Key Generation Mechanism via Deep Learning and Its Application. *Applied Sciences*, **11**, Article 8497. https://doi.org/10.3390/app11188497

[7] Gaddam, S.V.K. and Lal, M. (2010) Efficient Cancelable Biometric Key Generation Scheme for Cryptography. *International Journal of Network Security*, **11**, 61-69.

[8] Li, N., Guo, F., Mu, Y., Susilo, W. and Nepal, S. (2017) Fuzzy Extractors for Biometric Identification. 2017 *IEEE* 37*th International Conference on Distributed Computing Systems* (*ICDCS*), Atlanta, 5-8 June 2017, 667-677. https://doi.org/10.1109/icdcs.2017.107

[9] Wang, P., You, L., Hu, G., Hu, L., Jian, Z. and Xing, C. (2021) Biometric Key Generation Based on Generated Intervals and Two-Layer Error Correcting Technique. *Pattern Recognition*, **111**, Article ID: 107733. https://doi.org/10.1016/j.patcog.2020.107733

[10] Wu, Y. and Qiu, B. (2010) Transforming a Pattern Identifier into Biometric Key Generators. 2010 *IEEE International Conference on Multimedia and Expo*, Singapore, 19-23 July 2010, 78-82. https://doi.org/10.1109/icme.2010.5583388

[11] 董锦锦. 基于混沌加密的多模态生物模板保护技术研究[D]: [硕士学位论文]. 哈尔滨: 黑龙江大学, 2018.

[12] 赵铖辉. 基于人脸模板保护的数字身份技术研究与实现[D]: [硕士学位论文]. 北京: 北京交通大学, 2020.

[13] Barni, M., Droandi, G., Lazzeretti, R. and Pignata, T. (2019) SEMBA: Secure Multi-biometric Authentication. *IET Biometrics*, **8**, 411-421. https://doi.org/10.1049/iet-bmt.2018.5138