АЛГОРИТМ ПРЕОБРАЗОВАНИЯ ИСХОДНЫХ БИОМЕТРИЧЕСКИХ ПРИЗНАКОВ НЕЙРОННОЙ СЕТИ В КРИПТОГРАФИЧЕСКИЙ ЗАКРЫТЫЙ КЛЮЧ

[1]Агзамова М.Ш., [2]Рустамова С.
[1,2]ТУИТ

https://doi.org/10.5281/zenodo.7857102

Abstract. *This paper discusses an algorithm for converting raw biometric features of a neural network into a cryptographic private key. The proposed algorithm is based on leveraging the properties of neural networks to generate unique cryptographic keys that can be used for user authentication. The article describes the process of converting raw features into keys and conducts an analysis of the resilience and security of the generated keys. The results show that the proposed algorithm has a high level of protection and can be used to enhance the security of authentication systems.*

Keywords: *authentication, biometrics, cryptographic methods, neural network, confidentiality, security.*

Введение

Биометрическая аутентификация является одним из наиболее эффективных методов защиты данных и систем от несанкционированного доступа. Биометрическая аутентификация имеет высокую степень надежности, поскольку использует уникальные физиологические или поведенческие характеристики человека, которые трудно подделать или подменить. Однако, несмотря на это, возможны атаки на системы биометрической аутентификации, такие как использование поддельных биометрических данных, обман алгоритма распознавания или компрометация хранилища данных.

Криптографические методы, в свою очередь, позволяют обеспечить защиту данных путем использования математических алгоритмов и ключей. Криптографические ключи являются специальными значениями, которые используются для шифрования и расшифрования данных. Их длина и уникальность определяют степень защиты системы.

Поэтому, комбинация биометрической аутентификации и криптографических методов обеспечивает более надежную защиту данных и систем от несанкционированного доступа. Реализация алгоритма преобразования исходных биометрических признаков нейронной сети в криптографический закрытый ключ является одним из способов достижения этой цели. В данной статье описывается алгоритм преобразования исходных биометрических признаков нейронной сети в криптографический закрытый ключ.

Описание алгоритма

Для начала необходимо подготовить набор данных лиц для обучения нейронной сети. Этот набор данных должен содержать изображения лиц и соответствующие им биометрические признаки. Например, это может быть размер носа, глаз или ушей. Для сбора таких данных необходимы специализированные приборы, такие как сканеры лиц или камеры высокого разрешения.

После сбора данных происходит обучение нейронной сети. Для этого используется набор данных лиц, который был подготовлен ранее. Нейронная сеть проходит через несколько этапов обучения, где ей показываются изображения лиц и соответствующие им

биометрические признаки. На этом этапе важно выбрать оптимальные параметры для обучения нейронной сети, чтобы достичь максимальной точности распознавания.

Алгоритм преобразования исходных биометрических признаков нейронной сети в криптографический закрытый ключ состоит из следующих шагов:

1. Обучение нейронной сети на наборе исходных биометрических данных с использованием метода обратного распространения ошибки.
2. Получение вектора весов нейронной сети, который является уникальным идентификатором данного набора биометрических данных.
3. Преобразование вектора весов нейронной сети в криптографический ключ с использованием алгоритма хэширования.
4. Хранение криптографического ключа в базе данных или на устройстве пользователя для последующего использования в процессе аутентификации.

Для обеспечения высокой степени защиты биометрических данных необходимо использовать сильные алгоритмы хэширования, такие как SHA-256 или SHA-512. Также важно обеспечить безопасность хранения и передачи криптографических ключей. Для этого можно использовать различные методы, такие как шифрование ключей с помощью сильных алгоритмов шифрования, например AES-256, а также использование многофакторной аутентификации и протоколов обмена ключами, таких как SSL и TLS.

Математическое описание алгоритма

Алгоритм преобразования биометрических признаков основан на использовании нейронной сети. Нейронная сеть обучается на исходных биометрических данных, после чего производится вычисление криптографического ключа. Для этого используется алгоритм преобразования, основанный на дискретном преобразовании Фурье.

Пусть имеется набор исходных биометрических признаков $X = \{x1, x2, ..., xn\}$, где каждый xi является вектором признаков. Нейронная сеть обучается на этом наборе данных и производит вычисление вектора $Y = \{y1, y2, ..., yn\}$. Для преобразования вектора Y в криптографический ключ используется следующий алгоритм:

1. Применить к вектору Y дискретное преобразование Фурье.
2. Отфильтровать высокочастотные компоненты.
3. Применить обратное дискретное преобразование Фурье.
4. Получить криптографический ключ K.

Таким образом, полученный криптографический ключ является функцией от исходных биометрических признаков и обладает высокой степенью уникальности и надежности.

Результаты исследования

Алгоритм преобразования исходных биометрических признаков нейронной сети в криптографический закрытый ключ был реализован и протестирован на наборе данных лиц. Результаты показали, что полученные криптографические ключи были уникальны для каждого лица и обладали высокой степенью защиты.

Для тестирования был использован набор данных лиц, содержащий биометрические признаки, такие как форма лица, глаз и рот, а также текстуры кожи и пр. Использование нейронной сети позволило точно определить эти признаки для каждого лица в наборе данных.

Затем был применен алгоритм преобразования, который основывается на преобразовании исходных биометрических признаков нейронной сети в криптографический закрытый ключ. Алгоритм использует дополнительные параметры, такие как случайные числа и защитный вектор, для повышения уникальности и безопасности полученных ключей.

Результаты показали, что полученные криптографические ключи были уникальны для каждого лица и обладали высокой степенью защиты. Ключи были успешно использованы для аутентификации пользователей в системе и доказали свою надежность и эффективность.

Реализация алгоритма была проведена на языке Python с использованием библиотек для машинного обучения и обработки сигналов. Исходные данные были представлены в виде набора изображений лиц. Для обучения нейронной сети была использована архитектура сверточной нейронной сети, которая позволяет эффективно работать с изображениями.

Однако, следует отметить, что алгоритм имеет некоторые ограничения, такие как необходимость использования большого количества дополнительных параметров для получения более точных ключей. Кроме того, для успешной работы алгоритма необходимо иметь доступ к большому количеству биометрических данных, что может быть проблемой в реальных условиях.

Тем не менее, результаты исследования показали, что алгоритм преобразования исходных биометрических признаков нейронной сети в криптографический закрытый ключ является перспективным направлением в области биометрической аутентификации и может быть использован в различных сферах, включая финансовые услуги, государственную безопасность, медицину и т.д.

REFERENCES

1. Yang Liu, Fei Wang, Jiankang Deng, Zhipeng Zhou, Baigui Sun, Hao Li. MogFace: Towards a Deeper Appreciation on Face Detection. URL: https://openaccess.thecvf.com/content/CVPR2022/papers/Liu_MogFace_Towards_a_Deeper_Appreciation_on_Face_Detection_CVPR_2022_paper.pdf
2. Roberto Pecoraro, Valerio Basile, Viviana Bono, Sara Gallo. Local Multi-Head Channel Self-Attention for Facial Expression Recognition. URL: https://arxiv.org/pdf/2111.07224v2.pdf
3. Kai Wang, Xiaojiang Peng, Jianfei Yang, Debin Meng, Yu Qiao. Region Attention Networks for Pose and Occlusion Robust Facial Expression Recognition. URL: https://arxiv.org/pdf/1905.04075v2.pdf
4. Andrey V. Savchenko. Facial expression and attributes recognition based on multi-task learning of lightweight neural networks. URL: https://ieeexplore.ieee.org/abstract/document/9582508/authors#authors
5. Minchul Kim, Anil K. Jain, Xiaoming Liu. AdaFace: Quality Adaptive Margin for Face Recognition. URL: https://arxiv.org/pdf/2204.00964.pdf