DOI: 10.37791/2687-0649-2023-18-5-33-47

Система верификации личности по изображению лица в защищенном режиме на основе искусственных нейронных сетей

В.И. Васильев[1]***, И.Е. Панфилова***[2]***, А.Е. Сулавко***[3*]***, А.Е. Серикова***[3]
[1]*Уфимский университет науки и технологий, Уфа, Россия*
[2]*Самарский государственный технический университет, Самара, Россия*
[3]*Омский государственный технический университет, Омск, Россия*
sulavich@mail.ru

Аннотация. Работа посвящена проектированию и реализацию системы верификации субъектов по лицу на основе нейросетевой модели, исполняемой в защищенном режиме. Под защищенным режимом понимается режим, при котором система верификации личности обладает повышенной устойчивостью к деструктивным воздействиям, таким как состязательные атаки, и позволяет хранить и обрабатывать биометрические данные без их компрометации. В основе системы лежит нейросетевой преобразователь «биометрия-код», обучаемый по ГОСТ Р 52633.5, позволяющий связать образ лицевой биометрии субъекта с его криптографическим ключом или длинным паролем, который в дальнейшем может использоваться для аутентификации, и глубокие сверточные нейронные сети. Для детекции лица на изображении использована архитектура искусственной нейронной сети MTCNN, а для извлечения признаков апробировано несколько нейросетевых архитектур: InceptionResnet, Facenet512, VGG-Face и OpenFace. Наилучшие результаты показала нейросеть InceptionResnet. При оценке эффективности и тестировании надежности предложенной системы на специальном наборе данных лиц, собранном при различном освещении в помещении, удалось достичь сравнительно низкого значения равной вероятности ошибок первого и второго рода (EER = 0,0146 при длине ключа 278 бит), что подтверждает эффективность рассмотренного подхода к построению систем верификации по лицу.

Ключевые слова: преобразователь «биометрия-код», защищенное исполнение, лицевая биометрия, глубокое обучение, детекция лиц, распознавание лиц, извлечение признаков, система верификации, сверточная нейронная сеть

Для цитирования: *Васильев В.И., Панфилова И.Е., Сулавко А.Е., Серикова А.Е.* Система верификации личности по изображению лица в защищенном режиме на основе искусственных нейронных сетей // Прикладная информатика. 2023. Т. 18. № 5. С. 33–47. DOI: 10.37791/2687-0649-2023-18-5-33-47

Verification of the personality of subjects by face based on neural network algorithms of artificial intelligence performed in protected mode

***V. Vasilyev*[1], *I. Panfilova*[2], *A. Sulavko*[3*], *A. Serikova*[3]**
[1]*Ufa University of Science and Technology, Ufa, Russia*
[2]*Samara State Technical University, Samara, Russia*
[3]*Omsk State Technical University, Omsk, Russia*
sulavich@mail.ru

Abstract. The aim of the work is to develop a system for verifying subjects by face based on a neural network model that is executed in a protected mode. Protected mode means that the identity verification system is highly resistant to destructive influences, such as competitive attacks, and allows storing and processing biometric data without compromising it. The system is based on a biometrics to code converter trained according to GOST R 52633.5, which allows you to associate the subject's facial biometrics image with its cryptographic key or long password, which can later be used for authentication, and deep convolutional neural networks. For face detection in the image, the MTCNN artificial neural network architecture was used, and several neural network architectures were tested for feature extraction: InceptionResnet, Facenet512, VGG-Face and OpenFace. The best results were shown by the InceptionResnet neural network. When evaluating the effectiveness and testing the reliability of the proposed system on a special dataset of faces collected under different lighting conditions in a room, it was possible to achieve a relatively low value of equal probability of errors of the first and second kind (EER = 0.0146 with a key length of 278 bits), which confirms the effectiveness of the considered approach to building face verification systems.

Keywords: biometrics to code converter, AI protected execution mode, facial biometric, deep learning, face detection, face recognition, features extraction, verification system, convolution neural network

For citation: Vasilyev V., Panfilova I., Sulavko A., Serikova A. Verification of the personality of subjects by face based on neural network algorithms of artificial intelligence performed in protected mode. *Prikladnaya informatika*=Journal of Applied Informatics, 2023, vol.18, no.5, pp.33-47 (in Russian). DOI: 10.37791/2687-0649-2023-18-5-33-47

Введение

Достигнутый уровень развития информационных технологий позволяет человеку доверять искусственному интеллекту (ИИ) принятие решений в самых различных сферах деятельности. Не является исключением и область информационной безопасности, где ИИ используется для распознавания компьютерных атак, анализа рисков, верификации субъектов на основе биометрических данных. К системам аутентификации на базе ИИ должны предъявляться дополнительные требования с точки зрения надежности и защищенности знаний от компрометации, так как в процессе функционирования они обрабатывают биометрические персональные данные. Биометрическая система должна функционировать в защищенном режиме, который не позволяет осуществлять обратную разработку нейросетевых моделей, лежащих в ее основе, производить манипуляции с этими моделями и извлекать из их памяти знания в обход алгоритма анализа данных,