17. *Proskuryakov A.V.* Realizatsiya bezetalonnogo sposoba obrabotki meditsinskikh rentgenograficheskikh i tomograficheskikh snimkov dlya diagnostiki zabolevaniy [Implementation of a non-etalon method of processing medical radiographic and tomographic images for the diagnosis of diseases] *Mater. Vserossiyskoy nauchnotekhnicheskoy konferentsii s mezhdunarodnym uchastiem imeni professora O.N. P'yavchenko «KomTekh-2019»* [Materials of the All-Russian Scientific and Technical Conference with international participation named after Professor O.N. Piavchenko "kOmtEch-2019"]. Rostov, Taganrog, 2019, pp. 156 -164.
18. *Proskuryakov A.V.* Verifikatsiya sostoyaniya fragmentov biologicheskikh ob"ektov po kom'yuterno-tomograficheskim izobrazheniyam [Verification of the state of fragments of biological objects by computer tomographic images], *Mater. Vserossiyskoy nauchnotekhnicheskoy konferentsii s mezhdunarodnym uchastiem imeni professora O.N. P'yavchenko «KomTekh-2019»* [Materials of the All-Russian Scientific and Technical Conference with international participation named after Professor O.N. Piavchenko "kOmtEch-2019"]. Rostov, Taganrog, 2019, pp. 169-175.
19. *Proskuryakov A.V.* Sintez informatsionnoy sistemy verifikatsii fragmentov meditsinskikh biologicheskikh ob"ektov dlya diagnostiki zabolevaniy na baze metodov sistemno-kontseptual'nogo podkhoda [Synthesis of an information system for verifying fragments of medical biological objects for the diagnosis of diseases based on methods of a system-conceptual approach], *Sb. materialov XVII Vserossiyskoy nauchnoy konferentsii studentov, aspirantov i molodykh uchenykh «Informatsionnye tekhnologii, sistemnyy analiz i upravlenie» (ITSAiU-2019)* [Collection of materials of the XVII All-Russian Scientific Conference of Students, postgraduates and young scientists "Information technologies, system analysis and management" (ITSAIU-2019)]. Rostov, Taganrog, 2019, pp. 207-213.
20. *ProskuryakovA.V.* Meditsinskaya avtomatizirovannaya informatsionnaya sistema podderzhki prinyatiya resheniya dlya diagnostiki zabolevaniy s ispol'zovaniem verifikatsii sostoyaniya fragmentov mediko-biologicheskikh ob"ektov po komp'yuterno-tomograficheskim izobrazheniyam [Medical automated information system for decision-making support for the diagnosis of diseases using verification of the state of fragments of biomedical objects using computed tomographic images], *Informatizatsiya i svyaz'* [Informatization and communication], 2020, No. 3, pp. 55-60.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Проскуряков Александр Викторович – Южный федеральный университет; e-mail: avproskuryakov@sfedu.ru; г. Таганрог, Россия; тел.: +78634371673; кафедра математического обеспечения и применения ЭВМ; старший преподаватель.

Proskuryakov Alexander Viktorovich – Southern Federal University; e-mail: avproskuryakov@sfedu.ru; Taganrog, Russia; phone: +78634371673; the department of mathematical support and computer application; senior lecturer.

УДК 681.03.245 DOI 10.18522/2311-3103-2022-2-212-225

В.В. Золотарев, А.О. Поважнюк, Е.А. Маро

МЕТОДЫ УСИЛЕНИЯ ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ LIVENESS DETECTION*

Биометрические системы идентификации и контроля доступа содержат методы распознавания личности субъекта на основе уникальных физиологических и поведенческих характеристик. Целью данной работы является разработка системы безопасного взаимодействия (аутентификации) участников геймифицированных образовательных проектов, включающая в себя противодействие угрозам безопасности, возникающим при использова-

* Работа поддержана Российским фондом фундаментальных исследований, проект № 19-013-00711.

нии биометрических характеристик пользователей. Выполнен сравнительный анализ эффективности распознавания поддельных биометрических образцов методами liveness detection на основе выявления подмены образца с помощью фото, видео на дисплее, 3D-модели, маски. В ходе исследования предложен способ применения метода liveness detection для внедрения в системы геймифицированной образовательной среды. Предложена модификация метода liveness detection (гибридный метод) и спроектирована система биометрической идентификации в реальном времени с использованием предложенного метода. Разработан двухэтапный гибридный метод биометрической идентификации на основе совместного использования пассивных и активных программных методов выявления поддельных биометрических образцов. Метод адаптирован для использования с минимальным количеством дополнительных используемых устройств, единственным сканером биометрических признаков является 2D-камера. Проведено тестирования работы сети видов двуслойный персептрон, трехслойный персептрон и сверточная нейронная сеть. Обучение сети проводилось на собственных обучающих примерах. Положение диктора при записи обучающих примеров: расстояние лица от камеры – 60см, режимы записи при повороте головы на 0 (взгляд прямо в камеру), 30 (голова немного повернута в сторону) и 45 (голова сильно повернута в сторону) градусов. По итогам тестирования лучшие показатели распознавания были выявлены у сверточной нейронной сети с 3 сверточными слоями и 1 полносвязным. Получена точность распознавания произнесенного слова до 100% при повороте головы пользователя до 30° и до 70% - при повороте головы пользователя до 45°. При тестировании на выборке, состоящей из 1000 примеров, значение FAR данной системы составило 1%, значение FRR составило 0%.

Биометрические системы идентификации; спуфинг-атаки; определение живучести.

V.V. Zolotarev, A.O. Povazhnyuk, E.A. Maro

METHODS OF IMPROVED USER IDENTIFICATION BASED ON LIVENESS DETECTION TECHNOLOGY

Biometric identification and access control systems contain methods for recognizing a subject's personality based on his unique physiological and behavioral characteristics. The purpose of this work is to develop a system for secure interaction (authentication) of participants in gamified educational projects, which includes countering security threats that arise when using biometric user characteristics. A comparative analysis of the efficiency of recognition of fake biometric samples by liveness detection methods based on the detection of sample substitution using a photo, video on a display, a 3D model, and a mask has been performed. During research a method of using the liveness detection for include to a gamified educational environment system was proposed. A modification of the liveness detection method (hybrid method) has been proposed and a biometric identification system in real time has been designed using the proposed method. A two-stage hybrid biometric identification method has been developed based on the joint use of passive and active software methods for detecting fake biometric samples. The method is adapted for use with a minimum number of additional devices, the only biometric feature scanner is a 2D-camera. The network of types two-layer perceptron, three-layer perceptron and convolutional neural network was tested. The network was trained on the author's training examples. The position of the announcer when recording training examples: the distance of the face from the camera is 60cm, the recording modes when the head is turned by 0 (look directly into the camera), 30 (the head is slightly turned to the side) and 45 (the head is turned strongly to the side) degrees. Based on the testing results, the best recognition rates were found in a convolutional neural network with 3 convolutional layers and 1 fully connected one. Accuracy of recognition of the spoken word is obtained up to 100% when the user's head is turned up to 30° and up to 70% - when the user's head is turned up to 45°. The FAR value of this system was 1%, the FRR value was 0% for testing on 1000 samples.

Biometric identification systems; spoofing attacks; liveness detection.

Введение. В зависимости от реализации способов проверки соответствия проверяемого пользователя зарегистрированному, могут быть применены способы взлома биометрической системы: при идентификации по голосу злоумышленником могут быть представлены записи, сгенерированные на основе полученных

образцов голоса пользователя. При идентификации по изображению лица злоумышленником могут быть представлены фотографии и видеозаписи пользователя, полученные непосредственно от него или из общедоступных источников, социальных сетей; изъятые или скопированные с устройств пользователя (мобильного телефона, персонального компьютера); маски из бумаги или специальных материалов; 3D-модели головы и др. [1, 2].

Живучесть (Liveness) – качество или признаки жизни субъекта, выявленные анатомическими характеристиками, непроизвольными реакциями, физиологическими функциями, добровольными реакциями, или поведением субъекта [3]. Liveness detection представляют собой методы, применяемые для усиления процедуры идентификации и защиты от взлома в биометрических системах идентификации и контроля доступа [4–6].

Известной проблемой в данном случае является угроза похищения аккаунта через подмену изображением считываемого с камеры лица пользователя, и, соответственно, взлом системы аутентификации. Для геймифицированных сред характерны требования безопасности, определяемые с учетом особенностей систем электронного обучения и сервисов-поставщиков образовательного контента.

На этапе обработки биометрического признака, поступающего с камеры или иного устройства считывания, может быть применены различные методы атак, например, может проводиться многократное сканирование биометрического признака (при неограниченном числе попыток возможно ложное определение и пропуск злоумышленника), Подделка биометрического признака (изменение собственных биометрических характеристик с целью имитации биометрических данных зарегистрированного пользователя, предоставления ранее записанных на специальные носители биометрических данных зарегистрированного пользователя).

Атаки, в которых биометрические данные реального пользователя системы подменяются мошенником с помощью поддельных идентификаторов, называются спуфингом [7]. Таким разновидностям атак противодействуют методы проверки признака жизни – liveness detection.

Liveness detection технологии. Технологии liveness detection – методы повышения безопасности систем распознавания, в задачу которых входит проверка идентификатора на принадлежность «живому» пользователю. Технологии liveness detection могут быть адаптированы для анализа различных биометрических показателей: отпечатка пальца, голоса, лица и др.

Для дальнейшей работы в качестве ключевого биометрического признака выбрано изображение лица, так как при этом не требуется непосредственного контакта с оборудованием (сканерами). Далее будут рассмотрены методы определения «признака жизни» лица человека, находящегося перед камерой, в режиме реального времени.

Распознавание лица – распространенный метод аутентификации, использование которого возможно с устройствами, содержащими камеру (мобильный телефон, ноутбук, компьютер с веб-камерой, банкомат и др.), но аутентификация на основе распознавания лиц без применения дополнительных средств проверки является уязвимой для атак злоумышленников. Изображение лица человека легче получить, чем другие биометрические идентификаторы, такие как отпечаток пальца или радужная оболочка. Любая фотография пользователя, полученная путем съемки крупным планом без согласия пользователя или из Интернета, социальных сетей, может быть использована для обмана системы.

Различными исследователями уже проводилась работа над созданием решений по реализации методов liveness detection. Они направлены на то, чтобы отличить лицо живого человека от распечатанной фотографии, маски или видеозаписи.

В работе [8] представлен метод, позволяющий отличить фотографию или видео от настоящего человеческого лица. В процессе проверки выявляется, что поверхность фотографии – плоскость, а поверхность лица – сложная 3D-текстура, для чего используется дорогостоящее оборудование – оптико-электронная система Vectra 3D, содержащая источники света и комплекс камер. Другое решение с использованием анализа 3D-текстур представлено в устройстве iPhone X, оснащенном инфракрасной камерой, извлеченные данные с которой обрабатываются сверточной нейронной сетью [9]. Однако подобные подходы не являются универсальными, так как требуют применения дорогостоящего оборудования, которое не всегда может применяться в системах биометрической идентификации с точки зрения экономической целесообразности, поэтому стоит рассмотреть разработки в данной области, предполагающие применение доступных 2D-камер.

В работе [10] представлено решение на основе анализа качества изображения. Входящее изображение переводится в серый цветовой режим (на выходе изображение I), к нему применяется фильтр Гаусса (на выходе изображение $\hat{I}$). Вычисляются различия между характеристиками I и $\hat{I}$ (среднеквадратичная ошибка, коэффициент шума, разницы границ, углов и др.). Предполагается, что показатель потери качества после применения фильтра Гаусса различается для «настоящих» (биометрический признак живого человека) и «ложных» (фотография, видеовоспроизведение) изображений. Метод уязвим к атаке 3D-модели.

Метод с использованием анализа текстур изложен в работе [11], где исследователи выявляют различие текстур настоящего лица и распечатанной фотографии с помощью LBP (Local Binary Patterns) метода – представления пикселей изображения в виде бинарных чисел, зависящих от интенсивности соседних пикселей. Выявляются LBP-векторы, которые различаются в зависимости от текстуры поверхности фиксируемого камерой изображения.

Предложен и метод повышения защищенности биометрической системы с помощью анализа фокуса, то есть выявления особенностей фокусировки камеры на настоящем человеческом лице или фотографии [12].

В работе [11] выражено предположение о том, что обнаружение фотографии в кадре может быть установлено при помощи анализа движений, так как движение человеческого лица отличается от принципов движения 2D-объекта. Анализировались оптические потоки, генерируемые 3D и 2D объектами и выявлено, что перемещения, повороты и движение точек объектов в числовом виде давали идентичные результаты, а сокращения (движение мышц лица) являлись признаком различия данных объектов. Метод уязвим к атаке представления видеозаписи лица.

Исследования в работе [13] посвящены анализу таких неконтролируемых движений, как моргание глаз: исследуются длительность, частота, случайность или преднамеренность моргания, статистические закономерности появления данного движения. Для данных методов применима следующая атака: на распечатанной фотографии подлинного пользователя злоумышленник вырезает глаза, прикладывая данную маску к своему лицу, имитирует моргание.

В работе [14] предлагается использование активного метода liveness detection, когда пользователю предоставляется задание проследить за анимацией, движущейся по экрану. Камерой фиксируется реакция пользователя, с помощью алгоритма Виолы-Джонса обнаруживаются лицо и глаза в кадре, выделяются опорные точки глаз (центры зрачков, края глаза), которые впоследствии используются для интерпретации реакции пользователя на задание и правильности выполнения. Анализируются отклонения траектории движения центров зрачков от заданной траектории. Выявлено, что данные показатели реального пользователя, выполняющего задание, значительно меньше, чем злоумышленника, показывающего

камере фотографию и пытающегося выполнить задание и повторить траекторию, передвигая изображение. Однако у злоумышленника есть вероятность успешно пройти аутентификацию. FAR = 13,3%.

В работе [15] представлен метод анализа движения губ при выполнении пользователем чтения чисел. Анализируется движение ключевых точек рта. Используется метод опорных векторов SVM [16] – линейный алгоритм, используемый в задачах классификации. Обучающими примерами служат видео-фрагменты произношения человеком вслух чисел от 0 до 9. Недостатком метода является ограниченность словаря, что позволяет злоумышленнику имитировать выполнение данного задания: к примеру, путем обмана пользователя получить видеозапись, на которой субъект произносит число; извлечь фрагмент произношения числа из существующих видео, находящихся в открытом доступе (интервью в социальных сетях, записи речи, выступлений человека). Вероятность получить подходящее задание довольно высока, так как их всего 10. Злоумышленник не ограничен в том, чтобы перезапускать программу проверки и ожидать попадания нужного задания, для которого имеется вырезанный фрагмент.

В работе [17] предлагается отличать реального человека от фотографии и видеозаписи с помощью СНС – сверточной нейронной сети. Используется СНС AlexNet для получения векторов признаков изображения и метод опорных векторов SVM для классификации.

Существуют и другие разработки методов liveness detection на базе нейронных сетей, например, в работе [18] с помощью СНС анализируется способность субъекта моргать. Предполагается, что моргать может только живой человек (данная реализация не содержит защиты от представления видео в качестве поддельного идентификатора).

Сравнение возможностей распознавания методов приведено в табл. 1. Задача состоит в том, чтобы выбрать или создать модификацию метода, позволяющего закрыть максимальное количество уязвимостей, выполняющего все критерии распознавания, приведенные в табл. 1.

Таблица 1

Сравнение методов liveness detection

Метод	Возможность распознать фото	Возможность распознать видео на дисплее	Возможность распознать 3D-модель	Возможность распознать человека в маске
Анализ 3D-текстур [8]	+	+	-	+
Анализ 3D-текстур [8], инфракрасная камера [9]	+	+	+	+
Анализ качества изображения [9]	+	+	-	-
Анализ 2D-текстур [11]	+	+	-	-
Анализ фокуса [12]	+	+	-	-
Анализ моргания [13]	+	-	+	-
Активное взаимодействие [14, 15]	+	-	+	-

В разрабатываемой биометрической системе идентификации предполагается осуществить комплексный подход к анализу получаемой информации и предотвратить максимальное количество возможностей реализации угроз применением гибридного метода liveness detection.

С помощью предложенного метода можно идентифицировать ложное изображение пользователя: фото, видео на экране устройства, проверить 3D-объект – является ли человеческим лицом или 3D-моделью (3D-маской). Однако возможен обход системы при представлении системе маски с вырезанной областью рта и возможностью злоумышленника использовать это для выполнения задания. Возможное решение: анализ дополнительных точек лица и их движения относительно друг друга. Выявление зависимостей между движением точек при перемещении в кадре статичного объекта (распечатанной фотографии, маски) и динамичного – настоящего лица.

Гибридный метод liveness detection. Для того, чтобы исключить максимальное количество возможных способов проведения спуфинг-атак, предлагается использовать двухэтапный гибридный метод биометрической идентификации и совместить пассивные и активные программные методы. Для первоначального выявления текстуры предоставленного идентификатора используется сверточная нейронная сеть. Сетью анализируются выделенные в кадре параметры изображения – таким образом, производится анализ его цветовой палитры и качества.

На данном этапе определяется, находится ли в кадре некий субъект или видеозапись (или фотография) на экране планшета/смартфона. На данном этапе невозможно различить среди субъектов реального человека, цветную фотографию на бумаге, маску и 3D-маску, так как при фиксации их камерой качество изображения такое же, как при фиксации реального человеческого лица, в отличие от изображения на экране планшета/смартфона, которое при фиксации камерой будет иметь сниженное качество, измененные структуру и цвет изображения, блики.

Если выявлено, что в кадре зафиксирована не фотография или видеозапись на экране устройства, проверяется, находится ли в кадре человек или цветная бумажная фотография, 3D-модель или маска, при помощи анализа возможности выполнить задание. Алгоритм принятия решения показан на рис. 1.

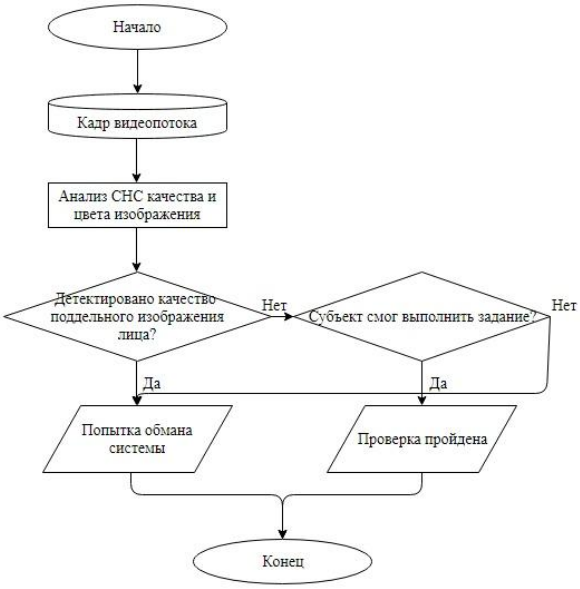


Рис. 1. Алгоритм принятия решения

Предполагается добиться улучшенных результатов по сравнению с результатами, представленными в приведенных ранее работах [8, 9, 11–15], или выявить рекомендации по улучшению проектируемой системы.

Реализация идентификации с поддержкой технологии liveness detection. Система представляет собой программный модуль, который реализует функции проверки признака жизни лица пользователя.

Для работы системы необходимо наличие камеры, которая будет фиксировать действия пользователя: ноутбук с встроенной камерой или персональный компьютер с подключенной веб-камерой.

Функции системы:

- обработка данных в режиме реального времени;
- идентификация пользователя без использования дополнительных сканеров биометрических идентификаторов (инфракрасных, термальных, 3D-камер);
- работа на различных платформах операционных систем.

Модуль первоначального распознавания признака «жизни» основан на предварительно обученной сверточной нейронной сети (СНС) и заключается в проведении анализа параметров изображения в каждый момент времени. Предлагается использовать реализацию данной СНС, предложенную в работе [19].

Используемая для классификации изображений в данной реализации СНС состоит из 4 сверточных слоев и 2 полносвязных. Используемую СНС необходимо предварительно обучить. Данные, подаваемые на вход СНС для обучения – изображения реальных пользователей из папки «real» или фотографии и видео пользователей, отображаемые на экране смартфона из папки «fake». Для получения собственных обучающих примеров необходимо снять несколько видео, изображающих реальных пользователей или фотографии и видео пользователей, отображаемые на экране смартфона. Схема формирования обучающего набора приведена на рис. 2.

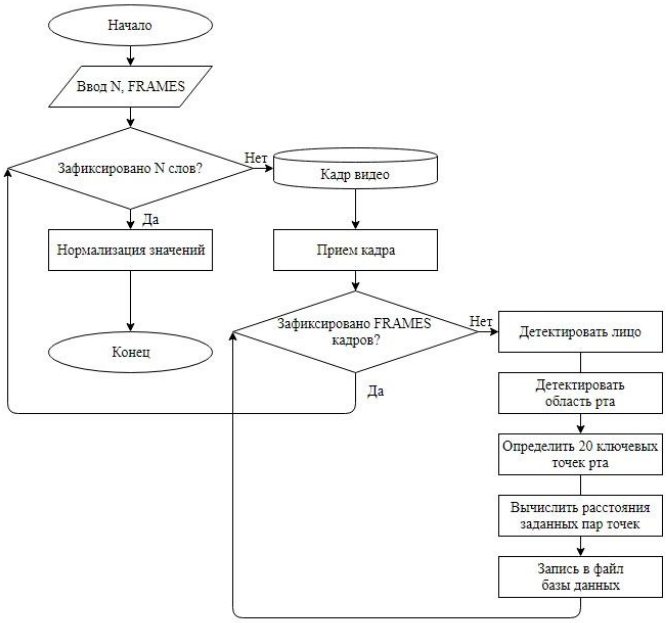


Рис. 2. Алгоритм создания обучающих примеров

С использованием специального модуля программы видео разбивается на кадры, в которых детектируется область лица и сохраняется в формате .png в папке «real» или «fake» соответственно. Для выполнения разбиения видеозаписей на кадры и сохранения изображений лиц в качестве параметра передаются названия видео и папок, в которые сохраняются изображения, а также частота – будут ли сохраняться изображения со всех кадров или пропуская некоторое количество (например, через каждые 4 кадра).

Также применена Dlib [20] – библиотека алгоритмов машинного обучения, содержащая средства распознавания лиц. С использованием средств данной библиотеки будут определяться границы лица в кадре и фиксироваться ключевые точки лица. Из данной библиотеки используется предварительно обученная модель для выделения 68 ключевых точек лица (рис. 3).

Метод адаптирован для использования с минимальным количеством дополнительных используемых устройств, единственным сканером биометрических признаков является 2D-камера (веб-камера, встроенная камера ноутбука, камера смартфона). Для использования разработанной программы необходимо наличие камеры с характеристиками:

- число мегапикселов матрицы не менее, чем 0,3;
- частота кадров не менее 20 Гц.

Рис. 3. 68 ключевых точек лица

Для записи обучающих примеров и контроля работы системы используется камера Dialog WC-05U (разрешение 640x480; 0,3 мегапикселов; скорость записи до 30 кадров/сек).

Использование метода liveness detection в целевых задачах. Предложенный метод может применяться в системах биометрической идентификации в условиях минимизации количества дополнительных используемых устройств для контроля доступа пользователя к ресурсам системы.

Данная разработка предназначена для использования в системе геймифицированной образовательной среды, включающей групповое взаимодействие пользователей различных ролей. Обычно в образовательных системах не используется двухфакторная аутентификация или другие дополнительные методы проверки пользователя, и используется проверка по логину и паролю. Пользователь может быть обманут злоумышленником посредством проведения социально-инженерных атак, может умышленно или неумышленно передать парольную или другую важную информацию для аутентификации. Для повышения защищенности аккаунтов пользователей предложено использовать биометрическую идентификацию и аутентификацию (с согласия пользователя). Использование биометрической иденти-

фикации позволяет обеспечивать безопасность взаимодействия участников и защиту аккаунтов и авторской информации; исключает возможность проведения злоумышленником социально-инженерной атаки.

Основным преимуществом использования биометрической идентификации является минимальный риск потери, кражи, взлома или подделки ключевой информации при условии повышения безопасности процедуры идентификации с использованием выбранного метода liveness detection; избавление пользователя от необходимости запоминать или хранить парольную информацию, так как для идентификации используется биометрический признак – лицо пользователя.

Для использования в системе геймифицированной образовательной среды предлагается 2 варианта распознавания пользователя по лицу:

а) система аутентификации;

б) система верификации.

В первом случае пользователи предварительно регистрируются в системе (регистрируется лицо и уникальное имя), база данных хранит в некотором виде признаки лица и соответствующее имя. При прохождении процедуры аутентификации пользователь предъявляет только свое лицо на камеру. Производится перебор вариантов и определение, кем является представленный камере пользователь. Системой предоставляется ответ: логин обнаруженного пользователя либо «пользователь не обнаружен».

Во втором случае пользователи также предварительно регистрируются в системе (регистрируется лицо и уникальное имя), база данных хранит в некотором виде признаки лица и соответствующее имя. При прохождении процедуры верификации пользователь первоначально предъявляет свое имя (логин), после чего представляет лицо камере. Производится сравнение признаков только с одним набором данных, соответствующем представленному логину. Системой предоставляется ответ «да/нет» (соответствуют ли признаки пользователя зарегистрированным).

Второй вариант является более быстрым, особенно при большом количестве зарегистрированных пользователей.

Получение задания и доказательство «живучести» в процессе активного взаимодействия производится после получения логина от подсистемы аутентификации или положительного ответа от подсистемы верификации, и позволяет пользователю получить доступ к аккаунту. На данном этапе также работают алгоритмы текстурного анализа.

Предложенная модификация метода выбрана таким образом, чтобы исключить максимальное количество возможностей проведения попыток взлома и предоставления поддельных биометрических идентификаторов.

Применение технологии Liveness Detection. В каждый момент времени должны анализироваться поступающие кадры. Выполняется первоначальное определение, является ли представленный идентификатор фотографией или видео. Процесс идентификации прерывается, если в данный момент проверка показывает, что представлены фото или видео.

Если проверка пройдена (не распознаны фото или видео данные), но в кадре распознано лицо, следовательно, в качестве идентификатора представлено реальное человеческое лицо, маска или 3D-маска. Чтобы среди этих объектов произвести проверку, живой ли человек в кадре, выдается задание произнести определенное слово и проверяется способность субъекта справиться с этим заданием. Возможность подмены идентификатора в процессе исключается, если параллельно с проверкой выполнения задания продолжает работать первый модуль, средства проверки качества изображения.

Кадры, на которых детектируется область лица, вырезаются и сохраняются в формате .png как изображение в папках «real» или «fake» соответственно. Изображения подаются на вход СНС уменьшенными до размеров 32x32. Сеть состоит из 4 сверточных слоев и 2 полносвязных. Производится обучение на данном множестве примеров и сохранение обученной модели.

Реализация функции обнаружения лица и выделения ключевых точек занимают определенное время, из-за чего обрабатываются не все поступающие от камеры кадры, но их количества достаточно для выделения значимой информации.

В качестве значащей информации, отражающей особенности произношения слов, предложено использовать расстояние между точками рта человека. Набор таких значений будет обрабатываться нейронной сетью для принятия решения, было ли верно выполнено задание, что позволяет уменьшить количество обрабатываемых нейронной сетью параметров по сравнению с методом [19], в котором анализируются все значения координат всех точек. Также метод [19] принуждает проводить дополнительную нормализацию значений координат в случае, когда положение фиксируемого субъекта отличается от ожидаемого (имеют место отклонения головы от нормального положения, повороты), в то время как расстояния не имеют зависимости от положения головы в пространстве, кроме случая отдаления от камеры или приближения к ней. При приближении/отдалении лица от камеры расстояния между точками рта изменяются пропорционально, следовательно, достаточно вычислить коэффициент, определяющий это изменение, и увеличивать/уменьшать с его помощью обрабатываемые значения.

Специальная функция позволяет определить коэффициент, используемый для выравнивания значений расстояний между точками рта. Сравнивается расстояние между двумя крайними точками рта пользователя с эталонным расстоянием между крайними точками рта диктора, записывавшего обучающие примеры. Для вычисления расстояний между точками используется формула Евклидова расстояния.

Обучение сети проводилось на собственных обучающих примерах. Положение диктора при записи обучающих примеров: расстояние лица от камеры – 60см, режимы записи при повороте головы на 0 (взгляд прямо в камеру), 30 (голова немного повернута в сторону) и 45 (голова сильно повернута в сторону) градусов. Для тестирования на данном этапе выбраны 2 слова с четко различимыми фонемами: «жимолость», «параплан». Обучающая выборка содержит 100 примеров – по 50 примеров произношения этих слов.

За время произношения диктором слова фиксируется определенное количество кадров (15 кадров – каждые 0.2сек) за заданное время. В каждом кадре получено 16 значений расстояний между точками рта. Таким образом, произношение одного слова представлено матрицей значений 15x16. Для нормализации значений в пределах [0,1] применяется линейная нормализация – формула (1).

$$\widetilde{x_{ik}} = \frac{\mathrm{x}_{ik} - \mathrm{x}_{min_i}}{\mathrm{x}_{max_i} - \mathrm{x}_{min_i}}. \quad (1)$$

Нейронная сеть реализована средствами библиотеки keras. Было принято решение реализовать и протестировать нейронные сети архитектур многослойный персептрон и сверточную нейронную сеть, выбрать сеть с лучшими показателями эффективности работы (точность и скорость распознавания).

Персептрон с двумя слоями, 50 обучающих примеров. В качестве функции активации в слоях используется ReLu – возвращает значение x, если x положительно, и 0 в противном случае. Применение ReLU повышает скорость сходимости градиентного спуска [21] по сравнению с сигмоидой и гиперболическим тангенсом.

В качестве функции активации последнего полносвязного слоя используется функция мягкого максимума softmax (2).

$$\sigma(\mathrm{z})\mathrm{i} = \frac{e^{z_i}}{\sum_{k=1}^{N} e^{z_k}}, \quad (2)$$

где z_i – значение на выходе из i-*го* нейрона до активации, а N – общее количество нейронов в слое.

Для улучшения показателей принято решение добавить дополнительный полносвязный слой и расширить обучающую выборку до 100 примеров.

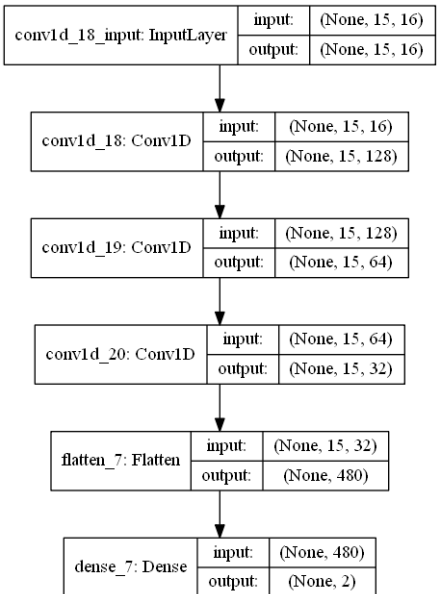
Результаты тестирования работы сети видов двуслойный персептрон, трехслойный персептрон и сверточная нейронная сеть приведены в табл. 2.

Таблица 2

Тестирование сети вида двуслойный персептрон, трехслойный персептрон и сверточная нейронная сеть

Параметр	Значение для двуслойного персептрона (50 обучающих примеров)	Значение для персептрона с тремя слоями (100 обучающих примеров)	Значение для сверточной нейронной сети
Средняя точность распознавания среди тестовых данных	92,00%	96,00%	96,00%
Среднее время распознавания произношения пользователя	0,0001 сек	0,0001 сек	0,0001 сек
Тест 0101011000, 0° (средняя точность распознавания)	80%	90%	100%
Тест 0101011000, 30° (средняя точность распознавания)	80%	90%	100%
Тест 0101011000, 45° (средняя точность распознавания)	70%	80%	70%
Тест 0001111100, 0° (средняя точность распознавания)	80%	90%	100%
Тест 0001111100, 30° (средняя точность распознавания)	80%	80%	100%
Тест 0001111100, 45° (средняя точность распознавания)	60%	80%	70%

По результатам тестирования лучшие показатели распознавания имеет третий вариант сети – СНС с 3 сверточными слоями и 1 полносвязным. Архитектура данной сети приведена на рис. 4.



Наименование слоев:
1. Conv1D – сверточный слой;
2. Flatten – слой преобразования двумерного вектора признаков в одномерный;
3. Dense – полносвязный слой.

Рис. 4. Архитектура выбранной сверточной нейронной сети

Заключение. В работе предложена модификация метода liveness detection (гибридный метод) и спроектирована система биометрической идентификации в реальном времени с использованием предложенного метода для задач геймифицированного обучения. По итогам тестирования лучшие показатели распознавания были выявлены у сверточной нейронной сети с 3 сверточными слоями и 1 полносвязным. Получена точность распознавания произнесенного слова до 100% при повороте головы пользователя до 30° и до 70% – при повороте головы пользователя до 45°. Для данной системы по результатам тестирования выявлены значения FAR и FRR при тестировании на 1000 примерах. Значение FAR данной системы составило 1%, значение FRR составило 0%.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ ISO/IEC 19794-1-2015. Информационные технологии (ИТ). Биометрия. Форматы обмена биометрическими данными. Ч. 1. Структура; введ. 01.07.2016. – М.: ФГУП «СтандартИнформ», 2016. – 25 с.
2. PSA: Your Note 8's Face Unlock can easily be fooled / Sean Hollister. – URL: cnet.com/news/samsung-note-8-fooled-face-unlock-not-secure.
3. Единая биометрическая система. Методические рекомендации по удаленной идентификации для руководителей проектов. Версия 1.0. – URL: https://bio.rt.ru/upload/iblock/4ba/MR-po-udalennoy-identifikatsii-dlya-rukovoditeley-proektov_v1.0.docx.
4. *Shweta Policepatil, Sanjeevakumar M. Hatture* Face Liveness Detection: An Overview // International Journal of Scientific Research in Science and Technology. – 2021. – URL: https://ijsrst.com/paper/8266.pdf.
5. *Chen H., Chen Y., Tian X. and Jiang R.* A Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP // IEEE Access. – 2019. – Vol. 7. – P. 170116-170133. – DOI: 10.1109/ACCESS.2019.2955383.

6. *Yousef A., Yaojie L., Amin J., Xiaoming L.* Face anti-spoofing using patch and depth-based CNNs // 2017 IEEE International Joint Conference on Biometrics (IJCB). – 2017. – P. 319-328.
7. *Trader J.* Liveness Detection to Fight Biometric Spoofing // M2SYS Blog: сайт. A KernellO Company, 2017. – URL: m2sys.com/blog/scanning-and-efficiency/liveness-detection-fight-biometric-spoofing.
8. *Lagorio A., Tistarelli M., Cadoni M., Fookes C., Sridharan S.* Liveness detection based on 3d face shape analysis // Conf. on Biometrics and Forensics (IWBF), April 2013.
9. Face ID Security, Apple Inc. – URL: apple.com/business-docs/FaceID_Security_Guide.pdf.
10. *Galbally J., Marcel S.* Face Anti-Spoofing Based on General Image Quality Assessment // Conf. on Pattern Recognition (ICPR), January 2014.
11. *Kim G., Eum S., Suhr J.K., Kim D.I., Park K.R., Kim J.* Face Liveness Detection Based on Texture and Frequency Analyses // 5th IAPR International Conference on Biometrics (ICB), 2012. School of Electrical and Electronic Engineering. – Yonsei University, Republic of Korea, 2012. – 6 c.
12. *Kim S., Ban Y., Lee S.* Face Liveness Detection Using Defocus // Department of Electrical and Electronic Engineering. – Yonsei University, Korea, 14 Jan, 2015. – P. 1537-1563.
13. *Jee H.-K., Jung S.-U., Yoo J.-H.* Liveness detection for embedded face recognition system // International Journal of Computer, Electrical, Automation, Control and Information Engineering. – 2008. – Vol. 2, No: 6. – P. 2142-2145.
14. *Ali A., Deravi F., and Hoque S.* Liveness detection using gaze collinearity // Proc. IEEE Int. Conf. Emerg. Secur. Technol. (ICEST), Sep. 2012. – P. 62-65.
15. *Kollreider K., Fronthaler H., Faraj M.I., and Bigun J.* Real-time face detection and motion analysis with application in “liveness” assessment // IEEE Transactions on Information Forensics and Security. – 2007. – 2 (3-2). – P. 548-558.
16. *Воронцов К.В.* Лекции по методу опорных векторов. – URL: ccas.ru/voron/download/SVM.pdf.
17. *Волкова С.С., Матвеев Ю.Н.* Применение сверточных нейронных сетей для решения задачи противодействия атаке спуфинга в системах лицевой биометрии // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – Т. 17, № 4. – С. 702-710.
18. *Eetveldt J.V.* Real-time face liveness detection with Python, Keras and OpenCV // Towards Data Science, 2019. – URL: https://towardsdatascience.com/real-time-face-liveness-detection-with-python-keras-and-opencv-c35dc70dafd3.
19. *Rodebrock A.* Pyimagesearch // Author archive. – URL: https://www.pyimagesearch.com/author/adrian.
20. Dlib C++ Library. – URL: http://dlib.net/.
21. *Krizhevsky A., Sutskever I., Hinton G.E.* ImageNet Classification with Deep Convolutional Neural Networks // Article in Advances in neural information processing systems, January 2012. – 9 p.

REFERENCES

1. GOST ISO/IEC 19794-1-2015. Informatsionnye tekhnologii (IT). Biometriya. Formaty obmena biometricheskimi dannymi. Ch. 1. Struktura; vved. 01.07.2016 [GOST ISO / IEC 19794-1-2015. Information technology (IT). Biometrics. Biometric data exchange formats. Part 1. Structure; entered 01.07.2016]. Moscow: FGUP «StandartInform», 2016, 25 p.
2. PSA: Your Note 8's Face Unlock can easily be fooled, Sean Hollister. Available at: cnet.com/news/samsung-note-8-fooled-face-unlock-not-secure.
3. Edinaya biometricheskaya sistema. Metodicheskie rekomendatsii po udalennoy identifikatsii dlya rukovoditeley proektov. Versiya 1.0 [Unified biometric system. Methodological recommendations for remote identification for project managers. Version 1.0]. Available at: https://bio.rt.ru/upload/iblock/4ba/MR-po-udalennoy-identifikatsii-dlya-rukovoditeley-proektov_v1.0.docx.
4. *Shweta Policepatil, Sanjeevakumar M. Hatture* Face Liveness Detection: An Overview, *International Journal of Scientific Research in Science and Technology*, 2021. Available at: https://ijsrst.com/paper/8266.pdf.
5. *Chen H., Chen Y., Tian X. and Jiang R.* A Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP, *IEEE Access*, 2019, Vol. 7, pp. 170116-170133. DOI: 10.1109/ACCESS.2019.2955383.

6. *Yousef A., Yaojie L., Amin J., Xiaoming L.* Face anti-spoofing using patch and depth-based CNNs, *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 319-328.
7. *Trader J.* Liveness Detection to Fight Biometric Spoofing, *M2SYS Blog: сайт. A KernellO Company, 2017*. Available at: m2sys.com/blog/scanning-and-efficiency/liveness-detection-fight-biometric-spoofing.
8. *Lagorio A., Tistarelli M., Cadoni M., Fookes C., Sridharan S.* Liveness detection based on 3d face shape analysis, *Conf. on Biometrics and Forensics (IWBF), April 2013*.
9. Face ID Security, Apple Inc. Available at: apple.com/business-docs/FaceID_Security_ Guide.pdf.
10. *Galbally J., Marcel S.* Face Anti-Spoofing Based on General Image Quality Assessment, *Conf. on Pattern Recognition (ICPR), January 2014*.
11. *Kim G., Eum S., Suhr J.K., Kim D.I., Park K.R., Kim J.* Face Liveness Detection Based on Texture and Frequency Analyses, *5th IAPR International Conference on Biometrics (ICB), 2012. School of Electrical and Electronic Engineering*. Yonsei University, Republic of Korea, 2012, 6 c.
12. *Kim S., Ban Y., Lee S.* Face Liveness Detection Using Defocus, *Department of Electrical and Electronic Engineering. Yonsei University, Korea, 14 Jan, 2015*, pp. 1537-1563.
13. *Jee H.-K., Jung S.-U., Yoo J.-H.* Liveness detection for embedded face recognition system, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 2008, Vol. 2, No: 6, pp. 2142-2145.
14. *Ali A., Deravi F., and Hoque S.* Liveness detection using gaze collinearity, *Proc. IEEE Int. Conf. Emerg. Secur. Technol. (ICEST), Sep. 2012*, pp. 62-65.
15. *Kollreider K., Fronthaler H., Faraj M.I., and Bigun J.* Real-time face detection and motion analysis with application in “liveness” assessment, *IEEE Transactions on Information Forensics and Security*, 2007, 2 (3-2), pp. 548-558.
16. *Vorontsov K.V.* Lektsii po metodu opornykh vektorov [Support vector machine lectures]. Available at: ccas.ru/voron/download/SVM.pdf.
17. *Volkova S.S., Matveev Yu.N.* Primenenie svertochnykh neyronnykh setey dlya resheniya zadachi protivodeystviya atake spufinga v sistemakh litsevoy biometrii [Application of convolutional neural networks for solving the problem of countering spoofing attacks in facial biometrics systems], *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and technical bulletin of information technologies, mechanics and optics], 2017, Vol. 17, No. 4, pp. 702-710.
18. *Eetveldt J.V.* Real-time face liveness detection with Python, Keras and OpenCV, *Towards Data Science, 2019*. Available at: https://towardsdatascience.com/real-time-face-liveness-detection-with-python-keras-and-opencv-c35dc70dafd3.
19. *Rodebrock A.* Pyimagesearch, *Author archive.* Available at: https://www.pyimagesearch.com/author/adrian.
20. Dlib C++ Library. Available at: http://dlib.net/.
21. *Krizhevsky A., Sutskever I., Hinton G.E.* ImageNet Classification with Deep Convolutional Neural Networks, A*rticle in Advances in neural information processing systems, January 2012*, 9 p.

Статью рекомендовал к опубликованию д.ф.-м.н. А.А. Кытманов.

Золотарев Вячеслав Владимирович – Сибирский государственный университет науки и технологий; e-mail: amida.2@yandex.ru; г. Красноярск, Россия; тел.: 83912227639; к.т.н.; доцент.

Поважнюк Алина Олеговна – e-mail: alina.l22@mail.ru;; тел.: 83912227639.

Маро Екатерина Александровна – Южный федеральный университет; e-mail: eamaro@sfedu.ru; г. Таганрог, Россия; тел.: 88634371905; к.т.н.; доцент.

Zolotarev Vyacheslav Vladimirovich – Siberian State University of Science and Technology; e-mail: amida.2@yandex.ru; Krasnoyarsk, Russia; phone: +73912227639; cand. of eng. sc.; associate professor.

Povazhnyuk Alina Olegovna – e-mail: alina.l22@mail.ru; phone: +73912227639.

Maro Ekaterina Aleksandrovna – Southern Federal University; e-mail: eamaro@sfedu.ru; Taganrog, Russia; phone: +78634371905; cand. of eng. sc.; associate professor.