Секция «Технологии искусственного интеллекта в предоставлении государственных и муниципальных услуг»

Приложение авторизации пользователей с применением искусственного интеллекта

Научный руководитель – Исмагилова Альбина Сабирьяновна

Лушников Никита Дмитриевич

Аспирант

Башкирский государственный университет, Факультет математики и информационных технологий, Уфа, Россия

E-mail: luschnikovnikita@yandex.ru

Биометрические системы применяются в самых разных сферах деятельности, распознавание лиц необходимо для определения конкретной личности на изображении или в видеокадре из огромного массива данных идентифицированных субъектов [1]. В особенности, если это касается владельца определенного устройства и его информации на этом устройстве. Это одна из актуальных задач информационной безопасности [2]. Биометрические технологии в особенности используются в банках для обеспечения безопасности счетов в депозитарных ячейках, контроля доступа и учёта рабочего времени сотрудников для удаленных объектов. В России широкое применение получили такие производители биометрических систем, как Bio Link и Bio Smart. Лучшие показатели решения данной проблемы продемонстрировали нейронные сети. Основным достоинством нейронных сетей в задачах распознавания является то, что нейронные сети функционируют подобно человеческому мозгу, являясь искусственным интеллектом. Данная технология помогает адаптировать устройства под определенный алгоритм действий, заданный программным кодом [3].

Цель исследования - реализация математической модели программного комплекса многофакторной аутентификации, предназначенного для предоставления необходимого уровня защищенности информационных ресурсов пользователей системы с использованием искусственного интеллекта.

К задачам исследования относятся:

1) разработка программных модулей распознавания личности по фото, видео и аудио;

2) разработка голосового помощника операционной системы, который автоматически заполнит форму авторизации;

3) создание сверточной нейронной сети при реализации программного модуля распознавания личности по видео;

4) создание глубокой обучающей нейронной сети для шифрования и дешифрования биометрических данных пользователя;

5) создание искусственного интеллекта для автоматизированной обработки данных пользователя;

6) защита информационного пространства и учетных записей операционных систем в полной мере.

Уникальностью программного обеспечения является реализация режима многопоточности и комплексной обработки всех биометрических элементов, создание новой конфигурации обучающей нейронной сети.

Результатом исследования является созданная математическая модель многофакторной аутентификации на основе искусственного интеллекта.

Программный комплекс многофакторной аутентификации пользователя состоит из следующих программных модулей:

1) Модуль распознавания личности по аудио (считывание по 12 тонам голоса).

2) Модуль распознавания личности по фото (считывание 128 точек лица).

3) Модуль распознавания личности по видео (определение настоящего пользователя и объектов, его олицетворяющих. Например, распечатанное изображение, фотография, видео).

4) Форма авторизации (логин/пароль).

5) Голосовой помощник (для удобства пользования операционной системой)

6) Работа обучающей сверточной нейронной сети (использование рецептивных полей, компиляция модели категориальной кросс-энтропии, настройка и сохранение файла весов нейронной сети).

7) Программный модуль шифрования и дешифрования биометрических данных пользователя.

8) Разработка искусственного интеллекта и автоматизированных систем в области защиты информации.

9) Проведение требуемых экспериментов на устройстве.

Данное программное решение разработано на языке Python 3.8.3 с использованием тренировочных моделей, нейронных сетей, баз данных. Выбор языка программирования обусловлен наличием множества необходимых компонентов для реализации конечного программного кода. В ходе решения задачи разработана структурированная схема функционирования ПО, предлагается метод для распознавания лиц с помощью выделения признаков на основе кратномасштабного вейвлет преобразования [4].

Далее производится сравнение записанного на видео голоса с микрофона с голосом из имеющейся базы данных с помощью вычисления евклидова расстояния цветности и мощности звуковых образцов. Надо отметить, что этот подход используется в музыке, а в рассматриваемой области был применен впервые для наиболее четкого считывания массива данных мощности голоса. Приведенную технология работы со звуком дополнена звуком считыванием евклидова расстояния по мощности голоса и его 12 тонам. Точность определения характеристик любого голоса составляет 99,4 %. Также в базу данных автоматически генерируются два изображения, на которых представлены показатели голоса по каждому тону.

Следующим биометрическим фактором является процесс распознавания личности по фотографии пользователя. Назначаются переменные и реализуются функции детектора первой фотографии. Переход к сверяемому изображению производится сразу же после вывода в командную строку массива данных основного изображения. Веб-камера в промежутке от 10 до 15 секунд создает снимок второго изображения. Стоит обратить внимание, что снимки не сохраняются, и в контейнере «cam.jpg» остается только актуальный снимок. После всех выполненных действий производится расчет евклидова расстояния. В данном случае значение вычисляется по исходным, а не по стандартизованным данным. В библиотеке dlib рекомендуется использовать граничное значение евклидова расстояния между дескрипторами лиц, равное 0,6. Затем производится вывод окна с онлайн-видеозаписью со звуком. Детектор глаз и лица формирует массив данных на основе файла с протестированной нейросетью и определяет во время онлайн-видеозаписи наличие субъекта (пользователя) или объекта, олицетворяющего субъект (фото, видео пользователя). В случае выявления субъекта определяется имя легитимного пользователя либо пометка о наличии в системе неавторизованного пользователя. В основе фрагмента данного программного обеспечения разработана тренировочная модель [5].

Для дальнейшей реализации программного комплекса следует проверить работу видео-

потока, в результате которого будет зафиксировано изображение пользователя (изначально в базе данных уже находился образец изображения искомого пользователя системы). Изначально в базу данных был загружен образец изображения искомого пользователя системы. Для удобства пользования в программном продукте создана рабочая область персонального устройства с выводом онлайн-потока видео и автоматическим фиксированием скриншота видеопотока.

Далее детектор формирует массив данных изображения искомого пользователя, после чего составляется массив данных изображения с видеопотока. Для удобства пользования в программном продукте создана рабочая область персонального устройства с выводом онлайн видеопотока и автоматическим фиксированием скриншота видеопотока. Одним из ключевых функций работы детектора является формирование массива данных лица, состоящего из 128 точек [6].

Скриншот изображения с онлайн-видеозаписи сверяется с искомым изображением в созданной базе данных посредством вычисления евклидова расстояния представленных массивов изображений.

Для работы программного модуля видео необходимо создать в целевой папке базы данных изображения пользователя, в которых после действия сверточной нейронной сети каждый элемент массивов будет иметь числовое значение. Поэтому, для создания многомерного массива учитывается 3D-проекция лица. Для получения идентификатора любого участка лица необходимо создать снимки лица пользователя в различных положениях (профиль лица слева, профиль лица справа, поднятая голова, опущенная голова, стандартное положение). Далее детектор формирует массивы в проекциях x, y, w, h с помощью веб-камеры.

Доступ к системе предоставляется в случае совпадения всех биометрических параметров, тогда как при совпадении хотя бы одного биометрического элемента пользователь получает возможность ввести логин и пароль с помощью голосового помощника, который автоматически заполнит все необходимые поля и при удачной аутентификации станет удобным гидом. Все полученные результаты обработки биометрических элементов вносятся в электронную базу данных (целевая папка).

Таким образом, представленный программный продукт является удобным помощником для пользователя любой системы. Данное программное решение является универсальным продуктом при наличии собственного устройства, использовании сайтов, образовательных модулей и систем контроля, управления доступом. Помимо этого, стоит отметить, что интегрированный в программный код голосовой помощник является хорошим гидом абсолютно для всех пользователей, включая людей с ограниченными возможностями (особенно касается слабовидящих людей).

Источники и литература

1) Акилин Г.А., Грицкевич Е.В. Особенности имитационного моделирования информационных систем, использующих биометрическую идентификацию по лицу // Сборник статей по материалам международного научного конгресса «Интерэкспо ГеоСибирь». 2019. С. 61-65.

2) Ван Лянпэн, Петросян О. Г. Распознавание лиц на основе классификации вейвлет признаков путем вейвлет нейронных сетей // Информатизация образования и науки. 2018. № 4 (40). С. 129–139.

3) Гринчук О.В., Цурков В.И. Обучение мультимодальной нейронной сети для определения подлинности изображений // Известия Российской академии наук. Теория и системы управления. 2020. № 4. С. 103-109.

4) Гуртова К. С. Метод защиты информации цифровых документов с помощью невидимых цифровых меток и его реализация // Современные информационные технологии и ИТ-образование. 2022. № 1. С. 152-166.

5) Караваев Д.А. Вейвлет-подобная архитектура комплекснозначной сверточной нейронной сети для синтеза комплексных сигналов // Вестник кибернетики. 2020. № 2. С. 20-31.

6) Кручинина Е.В. Видеоидентификация – ключ в мире адресных услуг // Системы безопасности. 2016. № 6. С. 110-111.