

Проектирование системы шифрования биометрических данных пользователя

А.С. Исмагилова
Уфимский университет науки и технологий
Уфа, Россия
ismagilovaas@yandex.ru

Н.Д. Лушников
Уфимский университет науки и технологий
Уфа, Россия
luschnikovnikita@yandex.ru

Аннотация — В настоящей работе предложен алгоритм шифрования биометрических данных пользователя информационных систем. Инструментом служит глубокая обучающая нейронная сеть, предназначенная для шифрования файлов в целевой папке с использованием математических методов.

Ключевые слова — аутентификация, биометрические данные, шифрование, нейронная сеть.

1. ВВЕДЕНИЕ

Сегодня почти не существует информационных систем, в которых отсутствуют этапы прохождения идентификации и аутентификации пользователем перед началом работы. Под аутентификацией подразумевается проверка принадлежности субъекту доступа предъявленного им идентификатора. Потребность в системах аутентификации есть у всех компаний и корпораций, представленных во всех рыночных сегментах. Неавтоматизированное управление доступом может привести к накладным расходам и ошибкам в области информационной безопасности.

К основным подрядчикам за 2022 год по количеству проектов внедрений аутентификации следует отнести такие структуры, как Информзащита (доля рынка – 5,56 %), Национальный аттестационный центр (5,56 %), Deiteriy (5,56 %), ИнфоТеКС (2,78 %).

Исходя из обозначенной актуальности, целью исследования является проектирование криптографического решения для полноценной защиты данных пользователей.

2. АЛГОРИТМ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Программный комплекс многофакторной аутентификации пользователя состоит из следующих программных модулей:

1. Модуль распознавания личности по фото (считывание 128 точек лица).
2. Модуль распознавания личности по видео (определение настоящего пользователя и объектов, его олицетворяющих. Например, распечатанное изображение, фотография, видео).
3. Модуль распознавания личности по аудио (считывание по 12 параметрам голоса).
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).

Модули распознавания личности по фото и видео предназначены для корректной работы определения настоящего искомого пользователя информационной системы.

Модуль распознавания личности по голосу определяет пользователя системы по всем тонам его голоса.

Дополнительной мерой безопасности является форма авторизации пользователя.

Для повышения качества и точности обработки данных программный комплекс дополнен глубокой нейронной сетью [2].

3. РЕАЛИЗАЦИЯ АЛГОРИТМА МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Алгоритм многофакторной аутентификации реализован с помощью языка программирования Python 3.8. Данный выбор обусловлен наличием дополнительных библиотек, необходимых для реализации программного комплекса. Стоит обратить внимание, что программный код, DataSet (300 образцов) и конфигурация обучающей нейронной сети были составлены и разработаны авторами самостоятельно. Однако для корректной программной реализации необходимо использовать такие библиотеки, как Tensorflow, Keras и Pytorch. Для создания главного меню и интерфейса также следует установить PyQt5 и Tkinter [4].

Разработанная авторами модель нейронной сети способна обучить выбранный авторами программный модуль распознавания личности по лицу. Модель генерирует новую базу данных обработанных образцов, количество шагов в эпохах обучения, директорию сохраненных результатов обучения.

Стоит обратить внимание на то, что в обучении нейронной сетью будет задействовано 512 нейронов.

С помощью утилиты HDFView есть возможность наиболее подробно изучить поведение нейронов после пройденных итераций обработки данных. Также доступен выбор определенного набора данных и его изменение при необходимости. Данная функция предназначена для реализации обучения нейронной сети по указанным настройками и параметрам [5].

Для оценки качества обучения нейронной сети следует обратить внимание на исходный вывод данной

модели, равной $Y_1, Y_2, \dots, Y_n$. Выход после процесса регрессии Softmax равен [6]:

$$\text{soft max}(y_i) = y_i' = \frac{e^{y_i}}{\sum_{j=1}^n e^{y_j}} \quad (1)$$

Соответственно:

$$\sum_{j=1}^n y_j' = 1 \quad (2)$$

4. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ШИФРОВАНИЯ

Немаловажным модулем в математической модели программного комплекса многофакторной аутентификации является модуль шифрования пользовательских данных изменения экспоненциальной функции и геометрической прогрессии.

Данный программный комплекс является для пользователя системы необходимым инструментом защиты его информации.

Вышепредставленные математические методы ранее не были использованы в области информационной безопасности и защиты информации. Выведенная авторами конечная формула (6) предназначена для программной реализации, обладающей высоким уровнем криптостойкости. В основе обработки данных будут неоднократно исполнены степенные функции и только после результата обработки будет присвоен идентификатор выбранных пользователем данных.

После запуска криптографического программного модуля в качестве входных данных будут представлены файлы из целевой папки пользователя.

После работы сверточной нейронной сети подсчет и вывод значений связан со знаменателем геометрической прогрессии. Под знаменателем геометрической прогрессии подразумевается множитель, вычисляемый по формуле [1]:

$$q_n = (q_{n-1})^2 \quad (3)$$

Для повышения криптостойкости программного модуля шифрования следует определиться с интервалом геометрической прогрессии:

$$b_n = b_{n-1} \times q_n \quad (4)$$

Экспоненциальная функция представлена в виде шагов (этапов) шифрования файлов. Таким образом [3]:

$$x = \sum \frac{1}{b_n} \quad (5)$$

Далее данные файлы будут интерпретированы в цифровом виде:

$$y = a^{\exp x} \quad (6)$$

В результате цифровые данные будут зашифрованы на протяжении выбранного количества циклов.

5. ЗАКЛЮЧЕНИЕ

Таким образом, шифрование данных предоставляет пользователю информационной системы необходимый уровень защиты. Для корректной работы спроектированной системы шифрования необходимы высокая производительность и вычислительная мощность устройства.

Представленный авторами результат исследования является необходимым компонентом в работе автоматизированных мест предприятия. В совокупности с нейронными сетями и искусственным интеллектом, данный программный комплекс представляет собой оптимизированное решение в области криптографии.

БЛАГОДАРНОСТИ

Исследование проводится при финансовой поддержке Исследования проводится при финансовой поддержке Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики» (МТУСИ) в рамках научного проекта № 40469-20/2022-к.

ЛИТЕРАТУРА

- [1] Гуртова, К. С. Метод защиты информации цифровых документов с помощью невидимых цифровых меток и его реализация / К. С. Гуртова // Современные информационные технологии и ИТ-образование. – 2022. – Т. 1. – С. 152-166.
- [2] Исмагилова, А.С. Многофункциональное ПО для защиты учетных записей пользователей с использованием биометрических технологий / А.С. Исмагилова, Н.Д. Лушников // Защита информации. Инсайд. – 2021. – Т. 2, №98. – С. 28-31.
- [3] Караваев, Д.А. Вейвлет-подобная архитектура комплекснозначной сверточной нейронной сети для синтеза комплексных сигналов / Д.А. Караваев // Вестник кибернетики. – 2020. – Т.2. – С. 20-31.
- [4] Крейнделин, В. Б. Защита аутентификационных данных сайтов и WEB-приложений / В. Б. Крейнделин, Н. А. Легков // Телекоммуникации и информационные технологии. – 2022. – Т. 1. – С. 6-10.
- [5] Лушников, Н.Д. Обучение и создание весов нейронной сети с применением категориальной кросс-энтропии / Н.Д.Лушников, А.С.Исмагилова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 года. – 2022. – С. 30-32. – DOI 10.33184/itokbco-2022-05-20.6.
- [6] Хайкин С. Нейронные сети / С. Хайкин – Полный курс – М.: «Вильямс», 2006. – 1104 с.