Концепция системы принятия решений для подтверждения личности клиента

П. А. Шелупанова*, П. Ю. Давыдченко, Р. М. Муромцев,
Д. В. Иванова, М. А. Чолокоглы, С. А. Чудина
Томский университет систем управления и радиоэлектроники
*Polina.a.Shelupanova@tusur.ru

***Аннотация*. В настоящее время отмечается рост киберпреступлений. Распространение дистанционного оказания большинства услуг требует повышенного внимания к обеспечению безопасности пользовательских данных. В данной работе описывается программный продукт "DoubleCheck", который позволяет с помощью видеоидентификации с высокой точностью подтвердить личность клиента при выполнении некоторой банковской операцию.**

Ключевые слова: биометрия, нейронная сеть, мошенничество, киберпреступность, видеоидентификация, система дистанционного банковского обслуживания, единая биометрическая система, разработка программного обеспечения

I. Введение

В современном мире автоматизация играет все большую роль в различных сферах деятельности, позволяя повысить эффективность и экономичность процессов. Технологии искусственного интеллекта, машинного обучения и автоматизации процессов уже существенно улучшили многие аспекты нашей жизни, от производства товаров до медицинской диагностики. Однако, несмотря на множество преимуществ, автоматизация также может привести к определенным упущениям, особенно в банковской сфере, где требуется высокий уровень безопасности и защиты данных клиентов.

При автоматизации процессов в банковской сфере, критически важные операции, такие как крупные переводы или выдача кредитов, могут быть автоматически подтверждены без участия человека. Для автоматизации в том числе используются и системы поддержки принятия решений.

Системы поддержки принятия решений играют важную роль в банковской сфере, позволяя эффективно анализировать большие объемы данных и принимать решения на основе предоставленной информации. Они также могут помочь улучшить процессы принятия решений, уменьшить риски и повысить эффективность работы банка в целом.

Системы поддержки принятия решений могут быть основаны на различных алгоритмах и методах анализа данных. Например, они могут использовать машинное обучение для анализа и классификации данных, а также для прогнозирования будущих результатов. Они также могут использовать методы искусственного интеллекта, такие как нейронные сети, для определения и прогнозирования поведения клиентов и выявления подозрительных операций.

В данной статье рассматривается возможность использования для решения таких задач методов видеоидентификации пользователя, в отношении которого принимается решение об одобрении или отклонении банковской операции. Видеоидентификация позволит также снизить риск использования мошеннических методов, включая DeepFake технологии, для обмана системы и получения доступа к критическим данным.

II. Альтернативы

В некоторых компаниях – Фонбет, Банк ВТБ, X5 Retail Group – применяются системы поддержки принятия решений для автоматизации процессов и повышения эффективности бизнеса.

Например, в Фонбете система поддержки принятия решений используется для оптимизации работы букмекерской конторы, анализа информации о клиентах, принятия решений по управлению рисками и прогнозированию спроса на различные виды ставок.

В Банке ВТБ система поддержки принятия решений применяется для автоматизации процессов кредитования и подбора наиболее подходящих кредитных продуктов для клиентов.

X5 Retail Group использует систему поддержки принятия решений для оптимизации работы магазинов и повышения эффективности управления запасами. Система анализирует данные о продажах и прогнозирует спрос на товары, что позволяет магазинам быстро реагировать на изменения спроса и поддерживать необходимые запасы товаров.

Amazon Go – это сеть магазинов, где покупатели могут покупать товары, не стоя в очередях на кассу, благодаря системе поддержки принятия решений, основанной на технологиях компьютерного зрения, сенсорной технологии и машинном обучении. Система автоматически распознает товары, которые покупатель берет с полки, и автоматически списывает стоимость товара с его учетной записи. Это ускоряет процесс покупки и облегчает обслуживание клиентов.

Все описанные примеры свидетельствуют об активном применении систем поддержки принятия решений в разных сферах, но при их реализации в полной мере не раскрыты возможности использования биометрического фактора для классификации клиентов.

Однако использование видеоидентификации на основе биометрических данных может значительно усилить системы принятия решений в различных сферах деятельности. Такая технология позволяет точно идентифицировать человека по его уникальным

биометрическим признакам, таким как форма лица, глаз, губ, голос, и т. д.

III. Решение

Для решения задачи идентификации клиента банка для последующего принятия решения о том, одобрить запрашиваемую им операцию или нет, предлагается использование технологии видеоидентификации. Суть метода заключается в комбинированном использовании биометрических данных человека и выполняемого им индивидуального жеста (при идентификации пользователь выполняет некоторое действие, которое закреплено за ним при регистрации биометрии). В качестве входных данных, по которым происходит проверка, используется видео длительностью не более пяти секунд.

В ходе идентификации клиента с использованием нейронной сети видеоизображение проходит три этапа проверки:

- Исключение имитации живого присутствия – это мера безопасности, применяемая в банковской сфере для предотвращения мошенничества. Она заключается в том, что при выполнении операций с клиентом запрещается использование статического изображения клиента (например, фотографии) в качестве подтверждения личности.
- Идентификация клиента банка – это процесс сравнения биометрических данных клиента, полученных в процессе взаимодействия с ним, с его подлинными данными, хранящимися в единой биометрической системе (ЕБС). Это позволит установить подлинность личности клиента и предотвратить мошенничество, связанное с подделкой личности или использованием украденных данных.
- Проверка динамики поведения – это технология, которая направлена на исключение использования заранее подготовленного видео с участием клиента в качестве подтверждения личности. Проверка динамики поведения заключается в том, что модуль видеоидентификации отслеживает поведение клиента в режиме реального времени, чтобы убедиться в том, что операцию совершает не мошенник, а именно подлинный клиент. Этот этап и включает упоминаемый ранее индивидуальный жест пользователя.

Нельзя исключать вероятность некорректного распознавания личности клиента, что особенно критично при принятии решений. Это обусловлено возникновением ошибок первого и второго рода.

- Ошибки первого рода – это ложное срабатывание системы, когда человека, который не имеет доступа к системе, она признает за авторизованного пользователя. Эта ошибка также известна как ложное срабатывание или ложное положительное определение. Ошибка первого рода может произойти, когда система находит сходство между биометрическими данными пользователя и шаблоном, сохраненным в системе, но на самом деле это не тот пользователь, которого система должна распознавать.
- Ошибки второго рода – это несрабатывание системы, когда система не определяет авторизованного пользователя и отказывает в доступе человеку, который должен был бы иметь доступ. Эта ошибка также известна как ложный отказ или ложное отрицание. Ошибка второго рода может произойти, если система не распознает биометрические данные пользователя, или если данные были повреждены, их неудачно сняли, пользователь находится в другом физическом состоянии, чем при регистрации данных.

Важно понимать, что ошибки первого и второго рода являются неизбежными при использовании биометрических технологий, и задача состоит в минимизации их количества. Говоря о системах поддержки принятия решений, стоит заметить, что особенно важно сокращение доли ошибок первого рода. В кредитно-финансовой сфере этот аспект особенно важен, например, при принятии решения об одобрении банковских операций.

Техническая реализация модуля видеоидентификации включает в себя процесс сбора и обработки данных, нейронную сеть, формирует классификацию пользователей и оценку её результатов в зависимости от ошибок первого и второго рода.

A. Этап сбора

Для начала видеоидентификации совершается запись с фронтальной камеры устройства пользователя длительностью не более 5 секунд. Таким образом, может быть получен видеопоток, с помощью которого и проводится идентификация пользователя..

B. Этап обработки

Видеопоток разбивается на кадры следующим образом: 1 секунда видеозаписи – 30 кадров (количество кадров было подобрано с учетом возможностей пользователя). Затем совершается векторизация: представив кадры как некоторый массив матриц (NxN)*n (где N – разрешение кадра, а n – количество кадров), будет произведена нормализация: значения ячеек матрицы, находящиеся в диапазоне от 0 до 255, нужно разделить на 255 для улучшения работоспособности нейронной сети. Таким образом, каждая ячейка матрицы будет иметь значение в диапазоне от 0 до 1. В результате будет получен многомерный массив (NxN)*n.

Описание архитектур нейронных сетей и сравнительный анализ. Архитектура Meso-4 начинается с последовательности четырех полносвязных слоев свертки и объединения, а затем следует сеть с одним скрытым слоем. Для улучшения работоспособности сверточные слои используют функцию активации ReLU, которая вводит нелинейность. Также используется пакетная нормализация для упорядочения предотвращения эффекта исчезающего градиента. Затем полносвязные слои используют Dropout для борьбы с переобучение нейронной сети. На выходном слое устанавливается функция активации Sigmoid для проведения бинарной классификации: идентифицирован пользователь по видеопотоку или нет. Таким образом, данная архитектура имеет в сумме 27,977 обучаемых параметров. Дальнейшие детали представлены на рис. 1. Использование данной архитектуры позволяет определить, является ли видеоизображения DeepFake.

После предварительного этапа проверки на DeepFake видеоизображение может быть проверено другой нейронной сетью для идентификации пользователя по его биометрическим показателям. Для выполнения данной задачи применима архитектура Temporal Convolutional Neural Network (TCNN) [1, 2]. Процесс классификации с использованием TCNN построен следующим образом (рис. 1):

- На один вход TCNN подается матрица биометрических признаков человека, а на другой вход подается исходная матрица признаков человека, которая закреплена за ним [3, 4].
- Затем TCNN выделяет эмбеддинги с обеих матриц признаков, вычисляет ошибку между входным и исходным эмбеддингом.
- На завершающем этапе происходит идентификационная оценка с помощью мультимодального классификатора (EER), который оценивает область допустимой погрешности для входных эмбеддингов. Если входной эмбеддинг выходит за область допустимой погрешности, то пользователь классифицируется как несанкционированный. Данный метод является актуальным ввиду соблюдения баланса между False Negative Rate (FNR) и False Positive Rate (FPR).

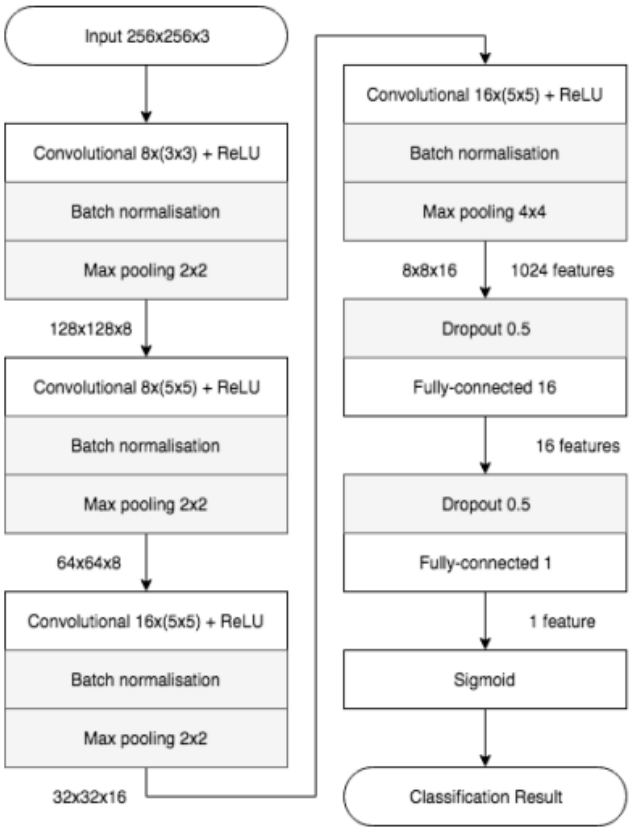

Рис. 1. Детализация архитектуры нейронной сети Meso-4

Классификация пользователя. Как было сказано ранее, может проводиться бинарная классификация (идентифицирован пользователь или нет) по видеопотоку, основываясь на метрике F-score. Однако, если видеопоток пользователя не сможет преодолеть некоторое пороговое значение (выбранное в зависимости от цели применения системы поддержки принятия решений), то должно быть принято решение об отклонении операции [5].

Все рисунки и диаграммы делаются в формате jpg или eps с хорошим разрешением (не менее 300 dpi). Если в состав рисунка входят надписи, формулы или нумерация, они должны быть единым файлом, а не надписями, сделанными в редакторе Microsoft Word.

IV. Заключение

Итак, технология поддержки принятия решений используется в банковской сфере, чтобы подтверждать личность клиента перед осуществлением критически важных операций: рассмотрение заявок на кредит и принятия решений о выдаче кредитов, для определения риска и для принятия решений о вложениях в различные инвестиционные проекты, для одобрения других финансовых операций. В результате, банки могут обеспечить более высокий уровень безопасности для своих клиентов и защитить их данные от мошеннических атак.

Несмотря на то, что системы поддержки принятия решений могут помочь улучшить процессы принятия решений в банковской сфере, они не могут заменить роль человеческого фактора в принятии решений. Некоторые решения, особенно те, которые касаются крупных сумм денег или важных бизнес-операций, требуют участия опытных профессионалов, которые могут анализировать данные и принимать решения на основе своего опыта и знаний.

Подводя итог, видеоидентификация на основе биометрических данных может стать перспективной технологией для использования в системах поддержки принятия решений в кредитно-финансовой сфере. Идентификация по биометрии, исключение имитации живого присутствия и проверка динамики поведения способны в совокупности обеспечить высокую степень доверия такой системе принятия решений, способной повысить уровень сервиса банковских услуг.

Список литературы

[1] D. Belo, N. Bento, H. Silva, A. Fred, H. Gamboa ECG Biometrics Using Deep Learning and Relative Score Threshold Classification. Sensors 2020, 20(15), 4078, DOI: 10.3390/s20154078

[2] A. Pandey and D. Wang, "TCNN: Temporal Convolutional Neural Network for Real-time Speech Enhancement in the Time Domain," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 2019, pp. 6875-6879, DOI: 10.1109/ICASSP.2019.8683634.

[3] A.K. Jain1, A. Kumar Biometrics of Next Generation: An Overview, Second Generation Biometrics: The Ethical, Legal and Social Context, pp.49-79, DOI:10.1007/978-94-007-3892-8_3

[4] S.S. Sengar, U. Hariharan and K. Rajkumar, "Multimodal Biometric Authentication System using Deep Learning Method," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2020, pp. 309-312, doi: 10.1109/ESCI48226.2020.9167512.

[5] S. Eberz, V. Lenders, K.B. Rasmussen, I.Martinovic Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics, ASIA CCS '17: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp. 386–399, DOI: 10.1145/3052973.3053032