Секция «Дискретная математика и математическая кибернетика»

Фронтальный алгоритм защиты от атак предъявления для лицевой биометрии

Научный руководитель – Полевой Дмитрий Валерьевич

Бурыкина Алина Ильинична

Студент (бакалавр)

Национальный исследовательский технологический университет «МИСиС», Институт информационных технологий и автоматизированных систем управления, Москва, Россия

E-mail: alina4268@mail.ru

В настоящее время многие мобильные приложения сталкиваются с необходимостью идентифицировать пользователей по лицу. Задача идентификации по лицу в целом решена. Однако одной из актуальных проблем остается обеспечение достоверности такой идентификации: необходимо отличать настоящее лицо от статичных изображений, скриншотов и других видов мошенничества. Данная работа сосредоточена на разработке и оценке эффективности системы проверки подлинности лицевой биометрии, направленной на предотвращение мошеннических попыток взлома систем распознавания лиц. Основным упором создания такого алгоритма была возможность его внедрения в устройства со слабыми вычислительными мощностями, как банкоматы, мобильные телефоны, терминалы и т. д. Поэтому наравне с точностью работы алгоритма также оценивалась его легковесность и скорость работы.

Для решения этой проблемы используется подход, использующий машинное обучение. Решение представляет собой ансамбль трех слабо скоррелированных сетей, основанных на современных подходах, применяемых в компьютерном зрении. Помимо существующих архитектур была разработана собственная кастомная архитектура. Данная архитектура представляет собой двухступенчатую систему. На первом этапе используется предобученная нейронная сеть для детекции положения лица на картинке. Затем на изображение добавляется специальное поле, 60% от площади которого составляет анализируемое лицо. Такое приближение дает значительный прирост в точности. Далее используется сеть, благодаря которой были получены числовые представления особенностей лица (эмбеддинги). Это позволило избежать смещения в предсказании модели, которая, помимо лица, анализирует все изображение в целом. На втором этапе используется еще несколько слоев нейронной сети для отбора признаков изображения. Результаты двух этапов объединяются и проходят через несколько финальных слоев для получения окончательного вывода о подлинности изображения. Используемый подход позволяет достичь высокого значения точности.

Источники и литература

1) Li X. An Effective and Efficient Face Mask Recognition System for Edge Devices //2022 5th International Conference on Data Science and Information Technology (DSIT). – IEEE, 2022. – С. 1-5.
2) Rangasrinivasan S. et al. A Unified Analysis of Masked Face Recognition & Social Distancing Detection //2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT). – IEEE, 2022. – С. 520-527.
3) Xiang J., Zhu G. Joint face detection and facial expression recognition with MTCNN //2017 4th international conference on information science and control engineering (ICISCE). – IEEE, 2017. – С. 424-427.

4) Zhang N., Luo J., Gao W. Research on face detection technology based on MTCNN //2020 international conference on computer network, electronic and automation (ICCNEA). – IEEE, 2020. – С. 154-158.

5) Kaziakhmedov E. et al. Real-world attack on MTCNN face detection system //2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). – IEEE, 2019. – С. 0422-0427.

6) Szegedy C. et al. Inception-v4, inception-resnet and the impact of residual connections on learning //Proceedings of the AAAI conference on artificial intelligence. – 2017. – Т. 31. – №. 1.

7) Rangasrinivasan S. et al. A Unified Analysis of Masked Face Recognition & Social Distancing Detection //2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT). – IEEE, 2022. – С. 520-527.

8) Liu Y., Jourabloo A., Liu X. Learning deep models for face anti-spoofing: Binary or auxiliary supervision //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2018. – С. 389-398.

9) Yang J., Lei Z., Li S. Z. Learn convolutional neural network for face anti-spoofing //arXiv preprint arXiv:1408.5601. – 2014.

Иллюстрации

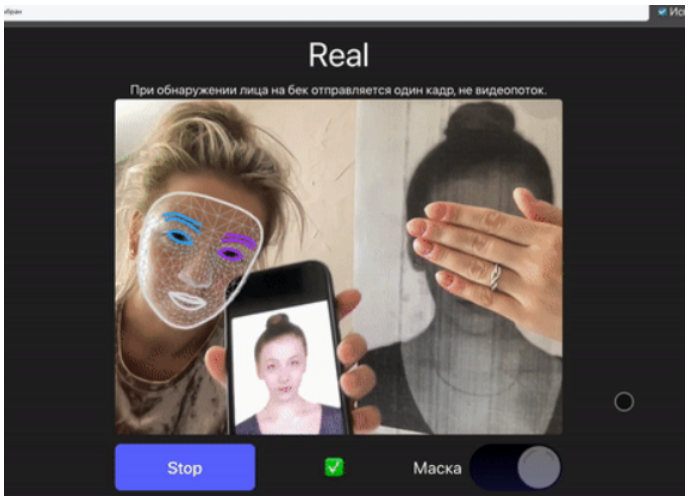

Рис. : Пример 1 работы интеллектуальной системы

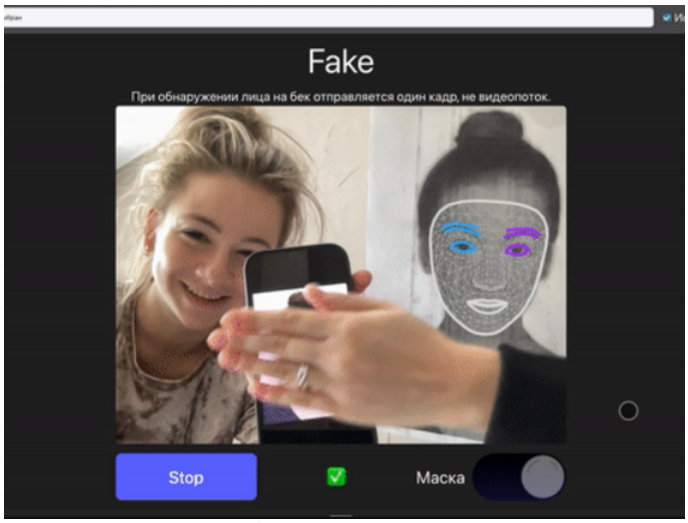

Рис. : Пример 2 работы интеллектуальной системы

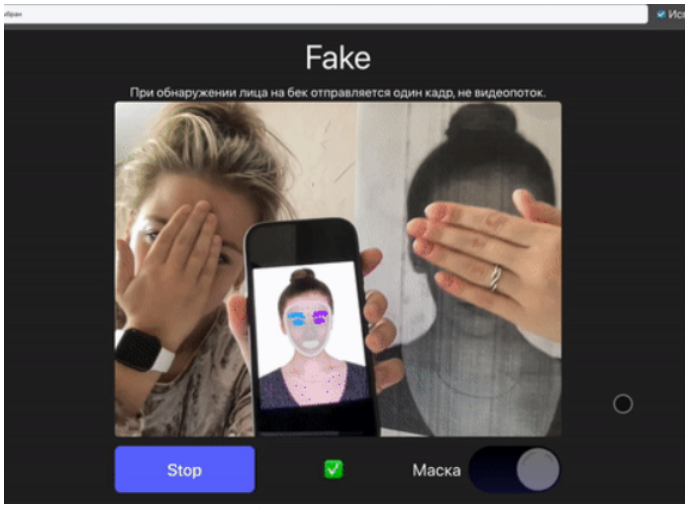

Рис. : Пример 3 работы интеллектуальной системы