Методы защиты от спуфинга при биометрической аутентификации лиц

А.Ю. Денисова[1], Ю.А. Мещерская[1], В.А. Федосеев[1,2]

[1]*Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34а, Самара, Россия, 443086*
[2]*Институт систем обработки изображений РАН - филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001*

Аннотация
В работе рассматривается методика противодействия спуфинг-атакам на системы аутентификации по лицевой биометрии. В качестве модели спуфинг-атаки рассматривается демонстрация злоумышленником фотографии авторизованного пользователя вместо собственного лица. Для обнаружения подобных атак предлагается использовать дополнительные источники данных помимо изображения в видимом спектре. Так, в работе предлагается и исследуется схема аутентификации с использованием данных тепловизионной съемки. Проведённые исследования показывают эффективность такого подхода для решения поставленной задачи.

Ключевые слова
Спуфинг, биометрическая аутентификация, распознавание лиц

1. Введение

Технология лицевой биометрии является наиболее простым методом с точки зрения считывания биометрических данных [1, 2]. Во многом поэтому она широко применяется на практике в ряде систем, и рынок систем лицевой биометрии продолжает расти [3]. Однако этот фактор обусловливает и уязвимость данной технологии к атакам подмены биометрической информации, называемым также спуфинг-атаками. В сети Интернет можно найти качественные изображения лиц многих людей (чего не скажешь об изображениях отпечатков пальцев или рисунках вен), и очень часто сами они публикуют их в социальных сетях. Таким образом, злоумышленник при авторизации в системе, использующей лицевую биометрию, может предоставить фотографию другого человека вместо демонстрации собственного лица.

Одним из способов обеспечения защиты от спуфинг-атак является взаимодействие системы с пользователем, требующее обратной связи [2, 4]. Например, система может потребовать открыть рот в определенный момент, сказать определенную фразу [4]. Недостатком является усложнение логики алгоритма аутентификации и увеличение времени съёмки. Другим подходом является применение сложных методов анализа изображения, в частности, методов глубокого обучения для выявления артефактов, свойственных рассматриваемой модели спуфинг-атаки [2]. Такие методы более удобны в использовании, но требуют предварительного обучения на больших объёмах данных, а кроме того не обеспечивают абсолютной защиты. В настоящем исследовании рассматривается третий подход, который состоит в использовании дополнительного датчика помимо RGB-камеры. В этой роли может использоваться лазерный дальномер, инфракрасная камера и др. В данной работе рассматривается тепловизионная камера.

2. Краткое описание предлагаемого метода

Бытовые тепловизоры, чья цена позволяет говорить о целесообразности их использования для задачи биометрической аутентификации, характеризуются низким пространственным

разрешением и высоким уровнем шумов. По этой причине они не могут использоваться непосредственно для идентификации пользователя, однако могут применяться для решения задачи обнаружения спуфинг-атаки. Как показано на Рисунке 1, тепловой портрет человека имеет неоднородную структуру, что не свойственно фотографиям на бумажном носителе или на экране цифрового устройства.

Предлагаемая технология совместной аутентификации при помощи пары устройств включает следующие основные этапы:

1) калибровка двух датчиков, расчёт матриц преобразования координат между изображениями, получаемыми разными устройствами;
2) обнаружение лица на изображении в видимом спектре, расчёт координат лица на тепловизионном изображении;
3) расчёт признаков, характеризующих подлинность лица, и собственно проверка подлинности по тепловизионному изображению;
4) идентификация пользователя по изображению лица в видимом спектре.

Преимуществом использования тепловизора являются простота расчёта и робастность признаков, которые могут быть использованы для проверки подлинности, что в свою очередь позволяет избежать необходимости подготовки большого обучающего набора данных. Так, в ходе исследований при классификации на основе лишь пяти простых признаков (медиана, максимальная температура, дисперсия, доля температур выше порога, разброс температур) линейный классификатор на основе SVM, обученный на 10 изображениях, позволил безошибочно классифицировать 29 изображений тестовой выборки.

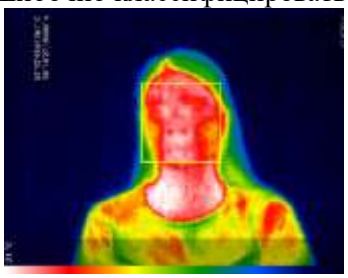
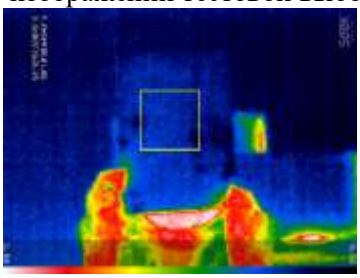
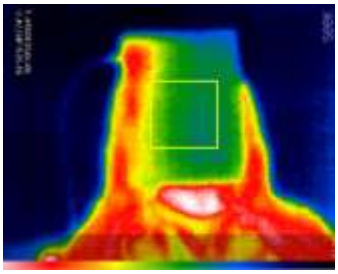
а)  б)  в) 

Рисунок 1: Примеры изображений лиц, снятые тепловизором: (а) подлинное, (б) фото, напечатанное на бумаге, (в) фото на экране планшета

3. Благодарности

Работа выполнена при поддержке РФФИ (гранты 19-29-09045, 19-07-00357).

4. Литература

[1] Mahmood, Z. A review on state-of-the-art face recognition approaches / Z. Mahmood, N. Muhammad, N. Bibi, T. Ali // Fractals. – 2017. – Vol. 25(1). – P. 1750025. DOI: 10.1142/S0218348X17500256.

[2] Калиновский, И.А. Обнаружение спуфинг-атак на систему лицевой биометрии / И.А. Калиновский, Г.М. Лаврентьева // Труды международной конференции по компьютерной графике и зрению «Графикон». – 2018. – С. 204-207.

[3] Facial recognition market to grow at 12 percent CAGR to 2024, Technavio forecasts // Biometric Update [Electronic resource]. – Access mode: https://www.biometricupdate.com/202011/facial-recognition-market-to-grow-at-12-percent-cagr-to-2024-technavio-forecasts (accessed date: 27.01.2021).

[4] Wang, T. Face liveness detection using 3D structure recovered from a single camera / T. Wang, J. Yang, Z. Lei, S. Liao, S.Z. Li // International Conference on Biometrics (ICB). – 2013. – P. 1-6. DOI: 10.1109/ICB.2013.6612957.