незначительный срок. Чего-то определенного о планировке поселения и расположении зданий сейчас сказать практически нельзя, поскольку выявленные источники эту информацию не содержат, а применение археологических методов видится невозможным по причине плотной современной застройки. Тем не менее, имеющиеся данные позволяют провести общую реконструкцию укреплений поселения и расположения их на местности.

УДК 004.93

РАЗРАБОТКА АЛГОРИТМА ОБНАРУЖЕНИЯ СПУФИНГА В БИОМЕТРИЧЕСКИХ СИСТЕМАХ АУТЕНТИФИКАЦИИ

А. Т. Буриев[1]

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация

Научный руководитель: А. Ю. Денисова, к.т.н., доцент

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация

Ключевые слова: презентационная атака, антиспуфинг, аутентификация по лицу, тепловые изображения, классификация

Спуфинг-атака – это попытка обмана системы идентификации путем предъявления ей поддельного биометрического параметра (например, лица).

Целью работы является реализация алгоритма защиты от спуфинга при биометрической аутентификации по лицу на основе алгоритмов машинного обучения.

Для проведения исследования был собран набор данных, который состоит из пар изображений в видимом спектре (режим RGB) и полутоновых тепловых изображений (режим GrayScale). Размер собранного набора данных составляет 611 пар изображений, из которых 257 пар – примеры истинных лиц и 354 пары – примеры спуфинг-атак (бумажная маска, бумажная маска по контуру лица, фотография на планшете и латексная маска).

Изображения, снятые на RGB и тепловизионные камеры, имеют разные разрешения. Для того, чтобы координаты области лица на тепловом изображении соответствовали координатам области лица на RGB-изображении был использован один из видов проективного преобразования плоскостей – гомография [1]. Для получения координат области лица использовался каскад Хаара [2].

[1] Буриев Артур Тохирович, студент группы 6512-100503D,
email: arturbuiriev@yandex.ru

В ходе выполнения работы были реализованы и проанализированы 3 алгоритма для обнаружения спуфинга. Для решения задачи бинарной классификации в алгоритмах использовался классификатор SVM с линейным ядром. Все признаки рассчитывались только по области лица.

Первый алгоритм Custom Features + SVM заключается в извлечении заданного набора признаков из изображения лица в тепловом спектре и последующем обучении SVM. Были эвристически подобраны следующие признаки: дисперсия, медиана, среднее, разброс значений яркости, гистограмма градиента яркости, доля пикселей со значением яркости в заданном интервале, отношение средних яркостей в верхней и нижней половинах изображения. Значение ROC-AUC для данного алгоритма получилось равным 0.98.

Второй реализованный алгоритм – алгоритм RDWT-Haralick + SVM [3]. Признаки рассчитывались по всем каналам RGB-изображения и по тепловому. Значение метрики ROC-AUC для данного алгоритма составило 1.0.

Третий реализованный алгоритм – ULBP + SVM [4]. Значение метрики ROC-AUC для данного алгоритма составило 1.0 для тепловых изображений и 0.99 для RGB.

Выполненная работа показала, что совместное использование RGB и тепловых данных обладает высоким потенциалом для обнаружения спуфинг-атак на биометрическое предъявление.

Библиографический список

1. Homography [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Homography (08.04.2022).

2. Face Detection using Haar Cascades [Электронный ресурс]. – Режим доступа: https://docs.opencv.org/4.x/d2/d99/tutorial_js_face_detection.html (08.04.2022).

3. Akshay Agarwal, Richa Singh, and Mayank Vatsa. Face Anti-Spoofing using Haralick Features. 2016 IEEE 8th International Conference on Biometrics Theory.

4. T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolutiongray-scale and rotation invariant texture classification withlocal binary patterns. IEEE Transactions on Pattern Analysisand Machine Intelligence, July 2002, Vol. 24, pp. 971-987.