

УДК 004.056.53

**РАЗРАБОТКА АЛГОРИТМА МНОГОФАКТОРНОЙ
БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ
МАШИННОГО ОБУЧЕНИЯ**

Деревцов Д.И. (Университет ИТМО)

Научный руководитель – к.т.н., Кузнецов А.Ю. (Университет ИТМО)

Рассмотрены наиболее распространенные подходы, используемые при разработке алгоритмов многофакторной биометрической аутентификации. Предложен подход для создания алгоритма на основе распознавания лица и радужной оболочки глаза с применением машинного обучения.

Введение. На сегодняшний день биометрическая аутентификация для доступа пользователей к информационным ресурсам используется во многих сферах жизни. Целью работы является рассмотрение подходов, используемых при разработке алгоритмов многофакторной биометрической аутентификации, а также разработка модели, позволяющей с достаточно высокой точностью производить аутентификацию пользователя на основе распознавания лица и радужной оболочки глаза.

Основная часть. Распознавание, основанное на одной модальности, может быть недостаточно надежным или может быть неприемлемым для конкретной группы пользователей или в конкретной ситуации. В связи с чем возникает необходимость в надежной аутентификации пользователей на основе нескольких взаимодополняющих биометрических признаков. В данной работе будет рассматриваться 2D-распознавание лица, которое из-за относительно плохих статистических показателей обычно применяется в мультимодальных системах, и радужная оболочка глаза, которая является уникальной характеристикой человека и практически не изменяется в течение всей жизни. Машинное обучение за счет специфичных особенностей и большого количества датасетов, находящихся в публичном доступе, способно свести к минимуму негативные стороны использования упомянутых выше признаков. В связи с чем они образуют достаточно сильную пару, чье использование при построении алгоритма с высоким уровнем достоверности оправдано. После извлечения векторов, содержащих соответствующие характеристики выбранных биометрических признаков, их необходимо объединить. Когда биометрические модальности не являются независимыми, то их удачное объединение на уровне признаков позволяет использовать зависимости более полно, чем объединение на уровне результатов сравнения.

Для оценивания качества работы разработанного алгоритма были выбраны следующие метрики: FAR, FRR, EER, min DCF. Использование дополнительной метрики для точного определения различных распределений ошибок обусловлено тем, что слепая оптимизация среднего EER иногда может привести к снижению безопасности.

Выводы. Разработанный алгоритм многофакторной биометрической аутентификации и его программная реализация могут быть применены в сфере защиты от несанкционированного доступа к информации.

Деревцов Д.И. (автор)

Кузнецов А.Ю. (научный руководитель)
