УДК 004.023

Д.В. Дмитриев, Р.С. Чернышев, Д.Н. Антонов, Б.С. Секачев, Д.А. Кобляков

АНАЛИЗ РАБОТЫ КЛИЕНТСКИХ ПРИЛОЖЕНИЙ В СИСТЕМЕ БИОМЕТРИЧЕСКОЙ ВЕРИФИКАЦИИ КОНТРОЛЯ ДОСТУПА

Нижегородский государственный технический университет им. Р.Е. Алексеева

Разработка методов и алгоритмов распознавания по изображению лица для целей биометрической верификации. В процессе работы исследовались существующие сегодня модели методы и алгоритмы биометрической верификации, проводились сравнительные экспериментальные исследования рабочих характеристик найденных методик.

Ключевые слова: детектирование лица, предобработка изображений, нейронные сети, выравнивание гистограммы, OpenCV, биометрическая верификация.

Введение

В настоящее время всё более широкое распространение получают биометрические системы идентификации человека. Традиционные системы идентификации требуют знания пароля, наличия ключа, идентификационной карточки либо иного идентифицирующего документа, который можно забыть, потерять или подделать. В отличие от них биометрические системы основываются на уникальных биологических характеристиках человека, которые трудно подделать и которые однозначно определяют конкретного человека. К таким характеристикам относятся отпечатки пальцев, форма ладони, узор радужной оболочки, изображение сетчатки глаза. Лицо, голос и запах каждого человека также индивидуальны.

Распознавание человека по изображению лица выделяется среди биометрических систем тем, что:

- во-первых, не требует специального дорогостоящего оборудования;
- во-вторых, отсутствует физический контакт человека с устройствами.

В биометрии существует два аутентификационных метода:

- *верификация.* Данная процедура аутентификации основывается на биометрическом параметре и соответствующем ему уникальном идентификаторе, которые принадлежат конкретному человеку;
- *идентификация*, в отличие от верификации, основана только на биометрическом параметре. Он сравнивается со всеми записями из базы зарегистрированных пользователей, а не с одной из них, выбранной на основании введенного идентификатора. Доступ осуществляется в случае совпадения предъявленного параметра с любым параметром из хранящихся в базе.

Целью данного проекта является разработка гибридной системы биометрической верификации, основанной на совместном применение методов статистического анализа изображений и нейросетевых методов для решения задачи биометрической верификации.

Архитектура системы

Гибридная система биометрической верификации состоит из нескольких функциональных многоуровневых компонентов (клиент-сервер), связанных между собой.

Многоуровневая архитектура системы обусловлена не только необходимостью распределения нагрузки между частями приложения, но и сутью задачи, а также удобством использования.

Очевидно, что вопрос о балансировке нагрузки между клиентом и сервером следует

решать на ранней стадии развития данного проекта. Предусмотрено наличие инструментов перераспределения нагрузки решаемых задач с клиента на сервер и обратно.

Например, для снятия биометрических данных, таких как изображения лица, подходит камера смартфона, совершенно нет необходимости в приобретении отдельной камеры для данных целей, но при этом полная обработка биометрических данных – задача достаточно тяжелая для мощностей современного телефона, что, в свою очередь, рождает необходимость перенесения этой задачи на отдельный мощный сервер, а, возможно, и на несколько серверов, параллельно обрабатывающих данные либо выполняющих каждый свою задачу. Но и переносить всю обработку изображения с мобильного устройства тоже не стоит, иначе серверу придется обрабатывать очень большой объем информации, что может привести к нестабильной работе при достаточно большом количестве клиентов. Как правило, итоговая настройка распределения мощностей производится на основе результатов экспериментального моделирования или опытной эксплуатации на более поздних этапах разработки, однако уже на этапе проектирования следует учесть подобную возможность.

В качестве основных клиентов системы можно выделить 4:

1. Мобильный клиент на платформе *iOS*.
2. Мобильный клиент на платформе *Windows Phone*.
3. Мобильный клиент на платформе *Android*.
4. Десктопный клиент на *Windows 7* с подключенной к нему камерой.

Архитектура гибридной биометрической системы верификации для задач контроля доступа представлена на рис. 1.

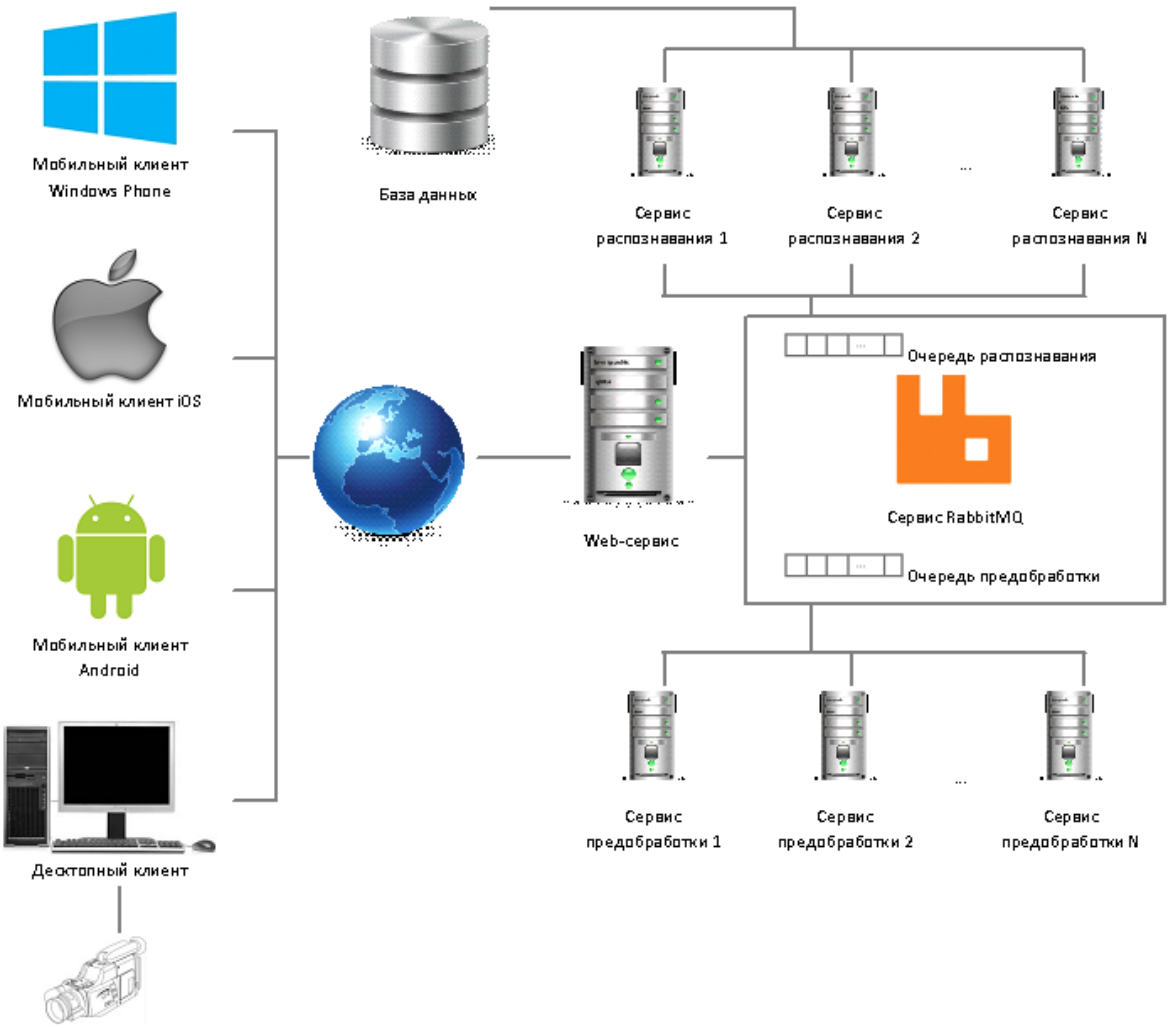

Рис. 1. Архитектура гибридной биометрической системы верификации

Web-сервис – сервис, принимающий пакеты от мобильных устройств или десктопного приложения. Все пакеты должны поддерживать проприетарный протокол взаимодействия, что является не только удобным механизмом для обмена данными, но и механизмом защиты, так как протокол не является общедоступным.

Web-сервис определяет входящему пакету дальнейшее направление: если пакет содержит в себе уже обработанное изображение, то он направляется в сервис *RabbitMQ* в очередь «распознавания», если же пакет содержит исходное необработанное изображение, то данные сначала поступят через *RabbitMQ* на сервис предобработки, а уже после обработанное изображение попадет в сервис распознавания.

Такой механизм позволяет сократить время ответа клиенту, потому что система масштабируема, а обработка изображения и распознавание могут быть разнесены на разные машины.

Функции клиента

Определение лица. Для определения лица человека на изображении используется алгоритм Виолы и Джонса в реализации библиотеки OpenCV.

Защита от фотоподлога. Основное отличие реального лица от фотографии или видео заключается в трёхмерности. Чтобы определить, что объект трёхмерен, его необходимо снять с разных ракурсов. В простейшем случае можно провести камерой перед лицом.

После успешного нахождения лица на кадре инициализируются три контрольных точки: правый глаз и кончик носа левый глаз (находятся их координаты в пределах кадра). Так как кончик носа расположен ближе к камере, во время поворота камеры смещение точки кончика носа будет большим, нежели смещение точек глаз. Примерная динамика движения контрольных точек изображена на рис. 2.

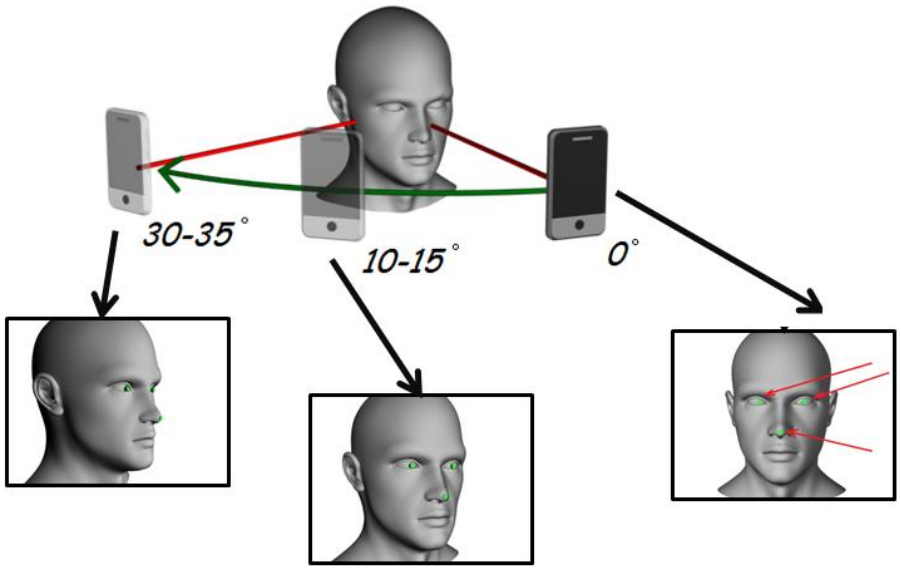

Рис. 2. Динамика движения контрольных точек

Такого эффекта невозможно добиться с помощью фотографии, так как на ней все контрольные точки расположены в одной плоскости. И при движении камеры вокруг фотографии положение точки носа относительно серединного перпендикуляра, опущенного из отрезка, соединяющего точки глаз, меняться не будет.

После проверки происходит расчёт угла, на который повёрнута голова человека. Для этого необходимо получить длину носа и расстояние между серединой отрезка, соединяющего точки глаз и проекцией точки носа на данный отрезок.

Минимальным углом, на который нужно повернуть камеру для прохождения фото-подлога, является угол 25^{o}.

Защита от видеоподлога. Для защиты от видеоподлога необходимо сравнить азимут и угол, рассчитанный при защите от фото-подлога. Для получения азимута используются датчики мобильного устройства, позволяющие определить географическую локацию устройства (например по данным акселерометра или гироскопа).

Если углы совпадают – это реальное лицо, и полученные биометрические данные (фронтальный снимок) можно использовать для авторизации. В противном случае это означает, что систему пытались обмануть с помощью видеофайла при неподвижном телефоне.

Частичная предобработка изображения. Проприетарный протоколю Клиенты системы поддерживают проприетарный протокол для обмена сообщениями. Структура пакета в соответствии с протоколом содержит следующие части:

- *version* - версия Web-сервиса;
- *client id* - идентификатор клиента, формирующийся по правилу md5(идентификатор, выданный после подключения клиента к системе + пароль пользователя);
- *action code* - код действия, определенное действие, которое нужно совершить, например, подключение клиента в web-сервису, авторизация, получение ответа и тому подобное.

Предобработка изображения на клиентских приложениях

Предобработка изображения осуществляется в несколько этапов.

GrayScale и изменение размера изображения. На первом этапе на каждой фотографии детектируется лицо, которое затем преобразуется в *grayscale*, и разрешение полученного изображения лица уменьшается с нескольких тысяч пикселей до небольшого числа (соответствующего количеству входов персептрона).

Масштабирование и центрирование. У используемого алгоритма детектирования лица Виолы Джонса имеется погрешность, в связи с которой на результирующем изображении лицо занимает разную площадь. Чтобы привести изображения к одному виду, производится масштабирование и центрирование относительно центра глаз.

Выравнивание яркости. Для повышения контраста применяется метод выравнивания гистограммы. В процессе выравнивания происходит изменение значений яркости пикселов таким образом, чтобы для каждого уровня яркости было примерно одинаковое количество пикселов.

Для компенсации неравномерности освещения применяется фильтр retina. Он осветляет спектр изображения и корректирует яркость благодаря адаптации к местным условиям. Другим важным свойством является его способность фильтровать пространственно-временной шум, увеличивая детализацию.

Удаление фона и поворот реализованы с целью сокращения влияния на процент сходства и уменьшения числа вариантов изображений в обучающей выборке. Эти функции реализованы с помощью библиотеки Stasm, так как OpenCV не обеспечивает достаточную точность.

Сжатие изображения. Производится с целью уменьшения объема трафика и увеличения скорости передачи и обработки изображения.

Проведенный анализ предварительных обработок показал, что характеристики работы биометрической системы существенно зависят от того, какие именно предобработки производятся над изображением, но несущественно меняются от последовательности их проведения, что актуально при разделении выполнения предобработок по клиентской и серверной сторонам.

Апробация результатов

Влияние выравнивания яркости. По рис. 3 видно, что комбинация методов выравнивания гистограммы и retina (график 50x50) показывает лучший результат, чем по отдельности или оригинальное изображение в grayscale.

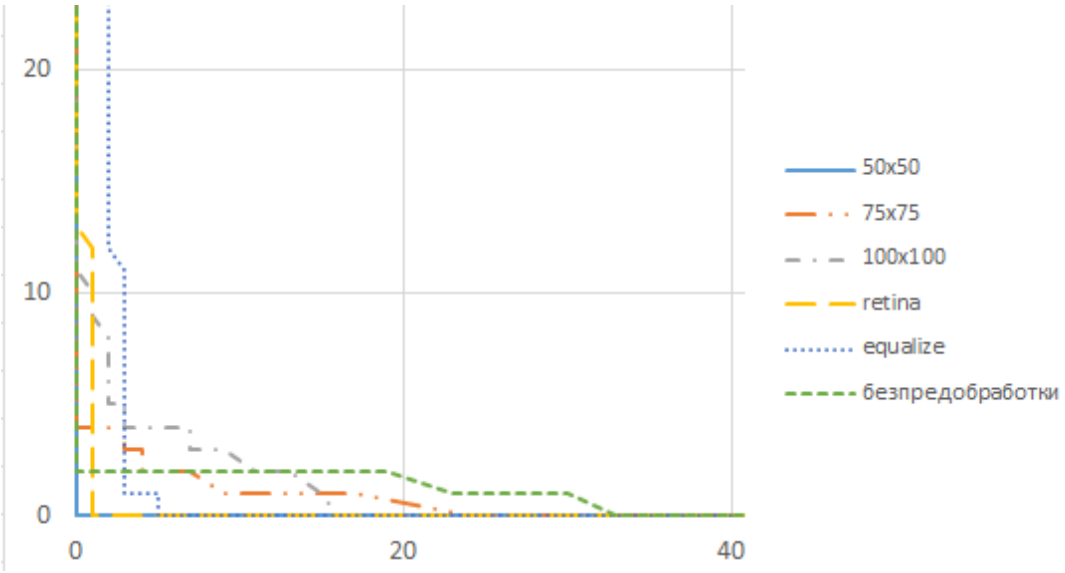

Рис. 3. ROC-кривая для разрешений и предобработок

Влияние угла поворота головы на результаты.

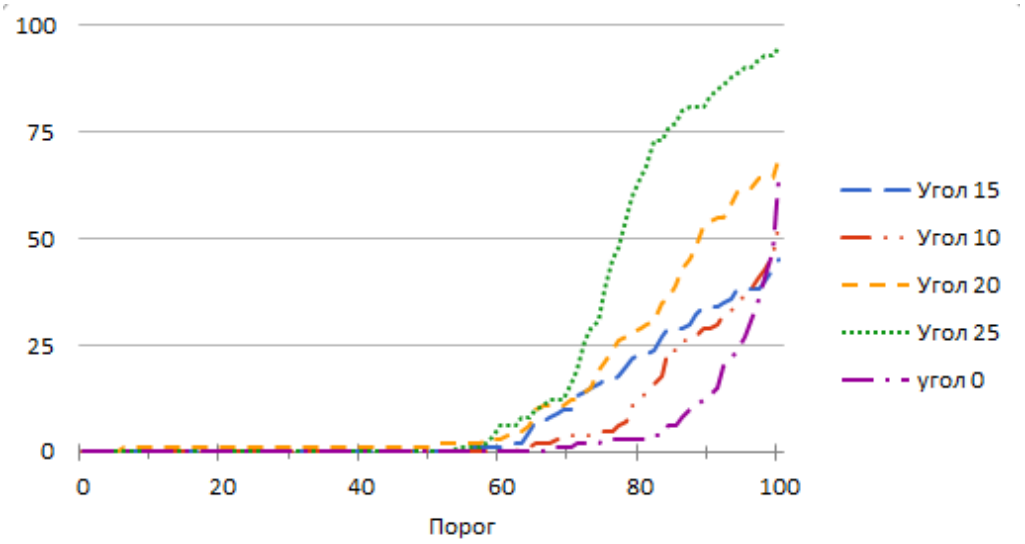

Рис. 4. График зависимости ошибки первого рода в зависимости от угла поворота головы

Рост ошибки становится заметен по сравнению с оптимальными условиями съемки при угле поворота головы выше 10^{o}.

Время верификации изображения. Также проведено исследование быстродействия проведения верификации с использованием AMD Phenom(tm) II X6 1075T Processor. Результаты исследования представлены на рис. 5.

В среднем на одну операцию верификации тратится около 300 мс. Так как сервер был настроен на одну очередь обработки сообщений, то, как видно на графике, зависимость линейна. Время верификации для большого числа одновременных подключений можно улучшить, используя горизонтальное масштабирование системы.

Оптимальными были выбраны размер изображения 50x50 и следующие предобработки: эквализация гистограммы и алгоритм Retina из библиотеки OpenCV.

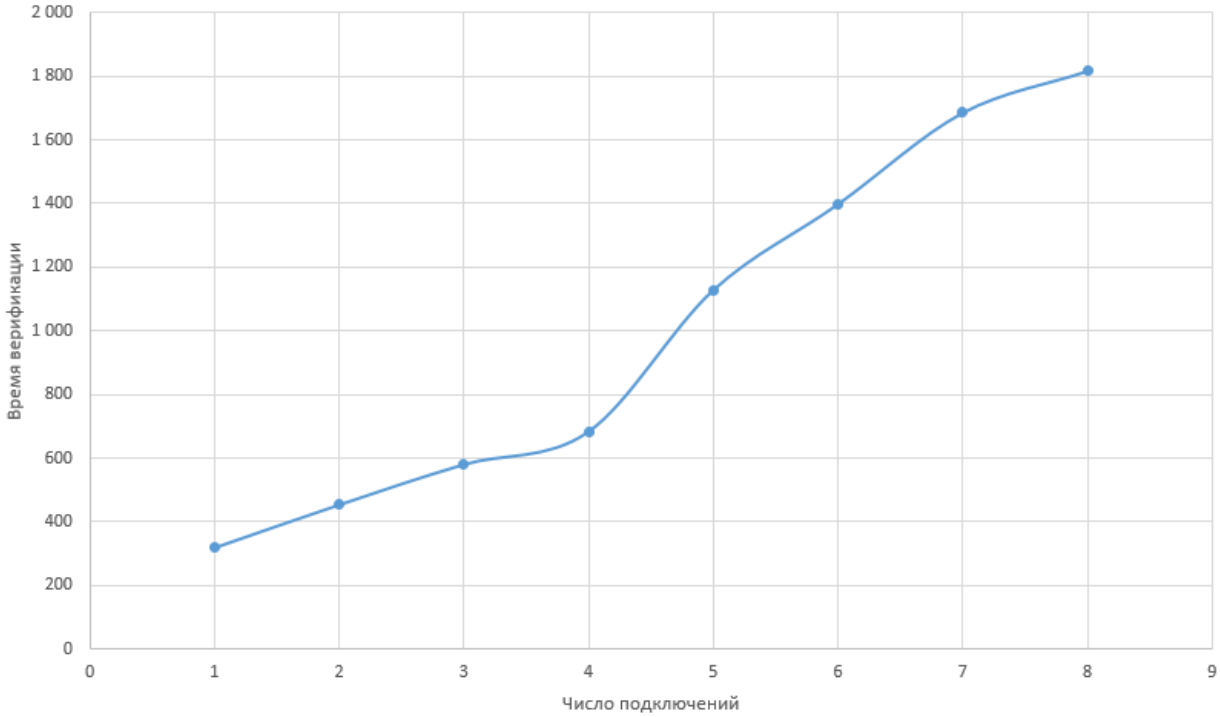

Рис. 5. График зависимости времени верификации от числа одновременных подключений

Дальнейшие шаги

Существенным недостатком библиотеки FANN является продолжительное время обучения аккаунта. При использовании системы со следующими параметрами: AMD Phenom(tm) II X6 1075T Processor и запуске обучения на 450 итерации в одном потоке с нагрузкой 100% Cpu – обучение занимало три-четыре часа.

Решено попробовать другую реализацию нейронных сетей – фреймворк от google - DeepDream: обучение новой сети занимает около 10 мин, а также допустимо использование GPU для обучения.

Выводы

В ходе исследования установлено, что к основным проблемам, возникающим при использовании лица в качестве биометрического параметра, относятся изменение освещенности, мимики, волосяного покрова, наличие или отсутствие макияжа. Все они препятствуют распознаванию и требуют особого внимания при разработке методов верификации. С помощью нейронных сетей данная проблема решена путем предоставления обучающей выборки, включающей максимально возможное число вариантов изображений лиц с различным освещением и мимикой.

Были апробированы методы нормализации изображения. Их комбинирование вне зависимости от условий освещения результирующие изображения приведены к одной контрастности, что является важным фактором при обучении нейронной сети.

В ходе проделанной работы разработаны приложения для различных платформ, осуществляющее распознавание лица человека по фотографии с помощью клиентских приложений (мобильных устройств и десктопных приложений). Разработаны метод защиты от подлога и метод защиты от недостоверных данных, который собирает качественные биометрические данные (фронтальный снимок лица) для системы авторизации.

Библиографический список

1. **Viola, P.** Robust real-time face detection / P. Viola, M. J. Jones. // International Journal of Computer Vision, 2004. – V. 57, issue 2. – P. 137–154.
2. **Вакуленко, А.** Биометрические методы идентификации личности: обоснованный выбор и внедрение / А. Вакуленко, А. Юхин. – М.: Наука, 2007. – 224 с.

3. **Viola, P.** Rapid object detection using a boosted cascade of simple features / P. Viola, P. Jones // IEEE Conf. on Computer Vision and Pattern Recognition. – 2001.
4. **Cootes, T. F.** Active shape models − their training and application / T. F. Cootes, C. J. Taylor, D. H. Cooper, J. Graham // Computer vision and image understanding. − 1995. − V. 61. − № 1. − P. 38–59.
5. Fast artificial neural network library [электронный ресурс] Режим доступа: http://leenissen.dk/ свободный. – Загл. с экрана (дата обращения: 19.02.2017)
6. The MIT-CBCL face recognition database [Электронный ресурс] Режим доступа: http://cbcl.mit.edu/software-datasets/heisele/facerecignition-database.html .– Загл. с экрана (дата обращения: 19.02.2017) Указать свою!
7. **Гонсалес, Р.** Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.
8. **Гудков, В. Ю.** Математические модели и методы обработки цифровых дактилоскопических изображений: дисс. … докт. физ.-мат. наук. – Челябинск, 2011. – 322 с.

Дата поступления
в редакцию 13.04.2017

D.V. Dmitriev, R.S.Chernyshev, D.N. Antonov, B.S. Sekachev, D.A. Koblyakov

ANALYSIS OF THE WORK OF CLIENT APPLICATIONS IN THE BIOMETRIC VERIFICATION SYSTEM OF ACCESS CONTROL

Nizhny Novgorod state technical university n.a. R.E. Alexeyev

Purpose: This article is devoted for the analysis of methods and algorithms of face recognition for the purposes of biometric verification.
Design/methodology/approach: This article observes the methods of face recognition on the image, methods of image preprocessing.
Originality/value: In the scope of this study, we described the existing models, methods and algorithms of biometric verification, make a comparative analysis of the operating characteristics of found methods.

Key words: face detection, image preprocessing, neural networks, histogram alignment, OpenCV, biometric verification.