GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 22 | 2022

ISSN: 2545-0573

ТЕХНОЛОГИЯ РАСПОЗНАВАНИЯ ЛИЦ И СФЕРЫ ЕЕ ПРИМЕНЕНИЯ

Ражабов Фархат Фарманович

Ташкентский университет информационных технологий имени Муҳаммада ал-Хоразмий, PhD, доцент кафедры "Компьютерные системы"

Каримов Алишер Баходир ўғли

Ташкентский университет информационных технологий имени Муҳаммада ал-Хоразмий, Магистр

A R T I C L E I N F O.

Ключевые слова:
Информационные технологии, распознавание лиц, общество, программное обеспечение, сервера.

Аннотация

Актуальность выбранной темы обуславливается тем, что современное общество находится на пороге развития информационных технологий. Система «smarthome», беспилотные автомобили, 5g интернет и многое другое, все это уже давно вошло в жизнь каждого человека и не является чем-то новым. Однако, в данной научной работе речь пойдет про «FaceRecognition» - технология распознавания лиц.

Технология распознавание лиц (FaceRecognition - англ.) - это относительно новая информационная технология, базирующаяся на биометрической идентификации человека по его лицу [1, 25 с.]. История возникновения данной технологии начинается ещё в 1960-ом году с созданием информационной линии сетки ученным Вудро Уилсоном. Но система имела множество недостатков таких, как малый объём памяти записывающего устройства, постоянные ошибки с распознаванием лиц, а самое главное такая технология требовала участие человека в ее постоянном обслуживании [2, 128 с.].

В современном мире такие технологии внедрены практически во все смартфоны, компьютеры, системы видеонаблюдения и так далее. Даже в 2017 году Массачусетский технологический институт включил в свой международный журнал технологию распознавания лиц в список самых прорывных инноваций человечества в сфере информационной индустрии [3, 463 с.].

Для того, чтобы детальнее разобраться в данной тематике, разберем блок вопросов, которые позволят раскрыть всю сущность информационной сферы распознавания лиц.

Как же работает система распознавания лиц?

В общем весь принцип работы такой системы можно описать, как процесс распознавания лиц людей, которые ранее попадали в объективы камер (либо специально сохранялись в устройстве смартфона или компьютера). Однако, на данный момент существует всего 3 информационно-программные схемы, закладывающие базовые настройки работы системы распознавания лиц [4,

692 с.].

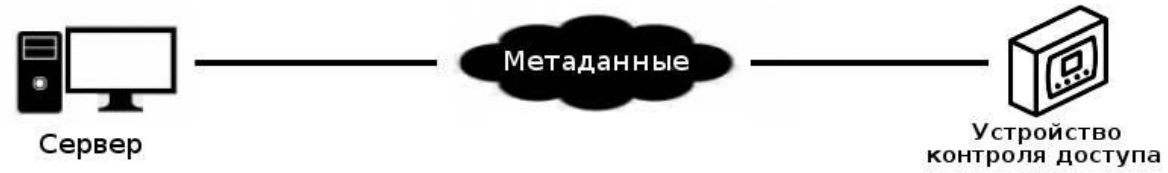
Первая - это анализ видеопотока на сервере. Пожалуй, самая простая и распространенная схема, так как специальная IP-камера передает видеопоток на облачные сервера, где находится база данных всех загруженных изображений лиц. После чего идет сопоставление полученной информации (то есть лица) с имеющейся на сервере. Однако, несмотря на распространенность схемы, все же она имеет недостатки. Например, идет очень высокая нагрузка на сеть, что тормозит ее, замедляет скорость поиска. Также остро стоит вопрос обслуживания такой схемы с точки зрения материальных затрат. Но, а самым главным и единственным положительным моментом пользования представленной схемы - это ее доступность, так как она полностью готова для эксплуатации.

Изображение 1.

Вторая - анализ видеопотока на IP-камере. Во втором случае изображение производится на самой камере, а сервер выступает своего рода принимающим источником, на который присылаются метаданные. Недостатки такой схемы - это дефицит и стоимость специальных камер, которые могут обрабатывать изображения. Важен момент с разными производителями таких камер, так как у всех свой подход к хранению, обработки и передачи изображений на сервера. Преимущество - неограниченное количество камер к одному серверу. Иными словами, в такой схеме невозможны перегрузки, сбои в работе и так далее.

Изображение 2.

Третья - анализ видеопотока на устройстве контроля доступа. Отличительной чертой заключительной схемы является то, что здесь не используется IP-камера. Однако, не обошлось без ее участия, так как модуль камеры встроен в устройство контроля доступа, выполняющий помимо функции распознавание лиц, функции управления доступом через турникеты и электрозамки. Недостатки схемы - это ограниченный круг использования, то есть используются в большинстве случаев в малогабаритных помещениях. Например, на военных КПП, на входе в государственные учреждения, сейфах банка и так далее. Преимущества - это средняя или даже низкая стоимость программного обеспечения схемы.



Изображение 3.

Какие же существуют виды технологий в системе распознавания лиц и какие проблемы они решают?

Вся система на первый взгляд типична и состоит из камеры видеонаблюдения, программного

обеспечения, а также сервера, которые хранит изображения лиц.

Однако, самую ключевую роль играет именно программное обеспечение, которое может быть «написано» под разные технологии распознавания лиц. Рассмотрим некоторые, которые обеспечиваются с помощью компьютерного зрения [5, 320с.]:

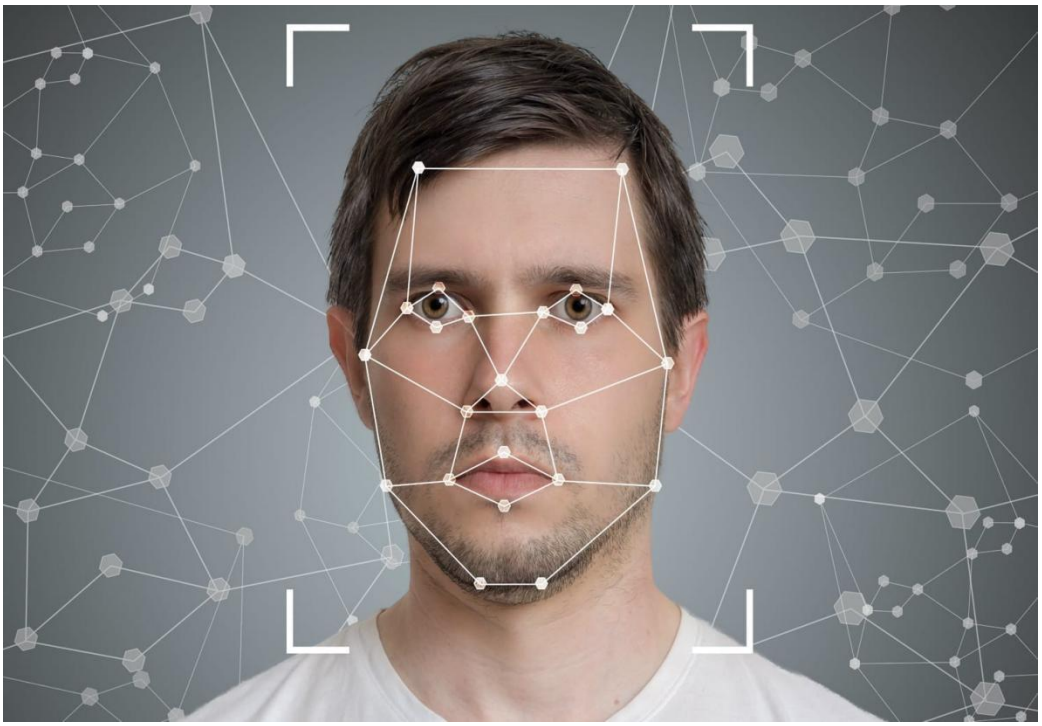
1) 2D-распознавание лиц.

С помощью распознавание лиц обеспечивается двумерная плоскость изображения, которая ложится в основу любых картинок на наших цифровых устройствах. В основу 2D двумерного распознавания лиц заложены технологии двухплоских изображений. Алгоритмы строятся на антропометрических параметрах и цифровой модели человеческого лица.

Такая технология довольно востребована на современном компьютерном рынке. Объясняется это тем, что двумерная база данных человеческих лиц является самой большой в мире. Те же самые камеры видеонаблюдения, которые можно встретить на каждом шагу в любом городе, работают на двухмерном софте. Соответственно всем производителям таких технологий распознавания лиц выгодно производить, совершенствовать и продавать двумерную базу.

Преимуществом такой технологии является в первую очередь готовность данных цифровых лица человека. Далее идет высокий спрос и недорогая установка всей системы.

Недостатки системы кроются в частоте ошибок типа FAR и FRR. Ошибка FAR - это «ложное одобрение» или «ложный пропуск», то есть устройство распознает другого человека, как авторизованного (законного) пользователя. Ошибка FRR - это «ложное отклонение», которое не дает владельцу устройства войти в систему, разблокировать смартфон и тому подобное. Например, у 3D-распознавание лиц такая ошибка в принципе возможна, однако, она возникает крайне редко по сравнению с 2D модель.



Изображение 4. 2D модель распознавание лица.

2) 3D-распознание лиц.

3D модель также поддерживается технологией распознавания лиц, которая позволяет детализировать изображение, посмотреть на него в разных плоскостях. Аналогично с 2D системой 3D технология также использует информационные изображения лиц человека, но уже

в трехмерном объеме. Такой формат намного качественнее и мобильнее функционирует в современной информационной индустрии.

В отличие от 2D системы 3D модель бывает нескольких видов. Например, существуют лазерные сканеры, которые могут на расстоянии считать нужную плоскость, изгибы предмета, его поверхность и тому подобное. Пожалуй, самой распространенной 3D системой распознавание лиц является всем известный FaceID от компании Apple. По своей сути это единственная технология трехмерного распознавания в мире, которая успешно и практично функционирует в смартфонах. В основу FaceID заложены вертикально-излучающие лазеры, которые на данный период времени невозможно каким-либо образом взломать или обмануть. Безусловно первые модели смартфонов от компании Apple с системой FaceID имели некоторые ошибки: разблокировка смартфона по фотографии владельца устройства, близкими родственниками (в силу идентичности черт лица), но все это быстро исправили и усовершенствовали.

Преимущества 3D системы заключается в высокой точности, отсутствие ошибок, а как следствие высокая безопасность. Недостатки: дороговизна технологий, слабая информационная база информационных моделей лиц.

Изображение 5. 3D модель распознавание лица.

3) Распознавание лиц по тепловизионному изображению.

Тепловизорные установки – это достаточно перспективная область, которую можно внедрить в системы распознавания лиц. Но пока что каких-либо массовых (серийных) разработок не существует. Однако, технология распознавание лиц на данный момент решает эту проблему, так как благодаря ей удается обнаружить в человеческом лице некоторые тепловые полости, с помощью которых можно идентифицировать человека.

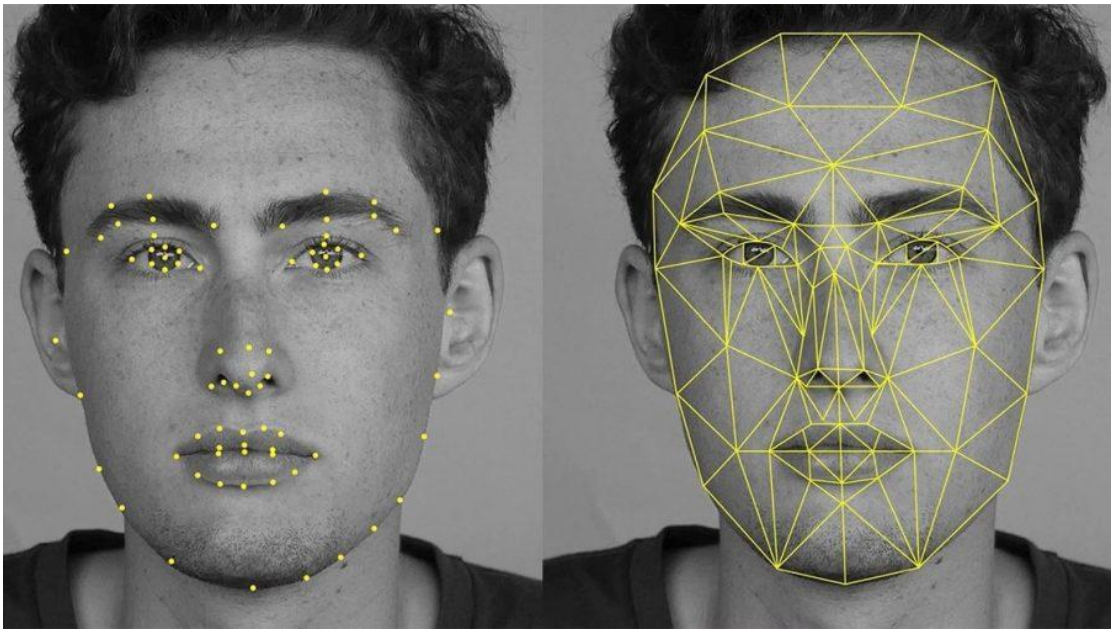
За основу берется 2D-распознавание, что позволяет открыть новые направления устаревшей технологии. С помощью тепловизора на базе 2D модели можно распознать лицо человека в полной темноте, исключить второстепенные предметы (очки, шляпу, бороду и прочее), и даже идентифицировать близнецов. Однако, все это находится в разработке и реализуется только с научной точки зрения.

Изображение 6. Тепловизионное изображение.

4) Распознавание лица по текстуре кожи лица.

Еще одно перспективное и разрабатываемое направление в сфере распознавания лиц. Благодаря распознаванию лиц можно выделить на человеческом лице особенности кожного покрова, линию волосного покрытия, индивидуальные микро кожные трещины и так далее, что позволит идентифицировать каждого человека. Технология в теории должна работать следующим образом: камерой захватывается конкретная область кожного покрова на лице (например, щека, лоб или нос), после чего данный участок с помощью программы разбивается на множество частиц и сопоставляется с информационной базой данных. Такое решение позволит существенно увеличить точность распознания, решить проблему с идентификацией близнецов и обеспечить высокую безопасность всей системы.

Опять же все это работает пока что только в научных лабораториях. Нельзя забывать о высокой стоимости, дефиците нужных запчастей, сложности программного обеспечения и многое другое [6, 254 с.].



Изображение 7. Распознавание лица по текстуре кожи лица

Что такое база данных распознанных лиц?

Выше неоднократно было сказано про базу данных, в которой хранятся информационные изображения человеческих лиц. Так вот, база данных это своего рода хранилище, откуда программа берет изображение и сопоставляет его с требуемым объектом.

На данный момент существует несколько видов баз данных [7, 240 с.]:

Первая – это государственные базы данных. Как правило, в таких базах хранятся данные о самих гражданах, которые проживают в конкретном государстве, а также лица, пересекающие границу той или иной страны.

У каждого государства свой банк базы данных, все они отличаются по-своему функционалу, системе проверки и идентификации. Например, в Индии база данных называется «Aadhaar», которая насчитывает порядка 1,19 млрд. изображений своих граждан. Безусловно база данных постоянно расширяется, фильтруется и применяется.

Самым большим риском существования государственных баз данных является их незащищенность, а именно, в случае утечки информации может пострадать огромное количество граждан. Также безопасность таких систем ослабевает, когда само государство предоставляет свой банк изображений лиц коммерческим организациям. Например, Microsoft имеет доступ к «Aadhaar», так как с помощью последнего авторизует своих пользователей в Skype и ряд других социальных сетей, которые популярны в Индии.

Возникает вопрос: зачем государству передавать такую информацию коммерческим компаниям? Ответ заключается в том, что как таковой доступ к базе данных не предоставляется, а лишь результаты идентификации, то есть уже готовые цифровые изображения лиц. Также государство за предоставление банка данных требует определенную плату от коммерческих компаний, что в свою очередь способствует пополнению бюджета в стране.

Вторая – это коммерческие базы данных. Всем нам известны частные банки данных, так как мы каждый день ими пользуемся. Социальные сети: Вконтакте, Facebook и другие, все они имеют свои облачные информационные хранилища с изображениями лиц пользователей. Все коммерческие базы данных созданы, во-первых, для быстрой аутентификации и авторизации пользователя (идет процесс отторжения длинных буквенных и цифровых паролей), а во-вторых, для предоставления своего банка изображений другим мелким коммерческим компаниям на платной основе.

Где же сейчас применяется система распознавания лиц?

1) Система контроля доступа [8, 724 с.].

Цифровой контроль доступа применяется сейчас практически в любой сфере человеческой деятельности, так как обеспечивает безопасность и автоматическую систему пропуска на тот или иной объект, хранилище и так далее.

Распознавание лиц в системе контроля доступа может функционировать в двух режимах.

Первый – это режим идентификации, то есть система допуска работает только по заранее загруженным цифровым изображениям лиц. Иными словами, на предприятие работает 100 сотрудников, которых нужно каждый день идентифицировать на входе в здание. Соответственно, изображение лиц всех сотрудников должно быть загружено в базу данных, которая не пропустит других людей. Такой режим распознавания лиц эффективнее всего использовать в особо охраняемых территориях, где ограничен круг лиц для посещения.

Второй – это режим верификации. Совсем иная технология, где применяются считывающие

устройства: карты, ключи, отпечатки пальцев и тому подобное. Система работает следующим образом: человек подносит свой пропуск к считывающему устройству, которое распознает, что это Иванов. В системе распознание лиц в свою очередь отражается фотография Иванова, а далее она сравнивается с уже загруженным изображением в базу данных. Если все совпадает, то система пропускает человека. Такая система работает быстро, без каких-либо ошибок и сбоев. Но в случае потери материального пропуска, человек не сможет попасть на охраняемую зону, а в худшем случае кто-то другой сможет воспользоваться найденным ключом доступа. Поэтому ко всем таким пропускным точкам, где применятся верификационная система, прикрепляются охранники, контролеры или вахтеры, которые сопоставляют изображение на мониторе с реальным человеком.

2) Распознавание лиц в толпе [9, 512 с.].

Распознавание лиц в толпе, как правило, применяется для розыска преступного лица, что существенно облегчает работу правоохранительных органов. В каждом городе любой страны имеется целая система камер видеонаблюдения, цель которой является охрана конкретных объектов, профилактики преступности, отображения в реальном времени ситуации в том или ином месте. Однако, как и у любой системы, здесь имеется ряд недостатков: погодные условия, влияющие на качество картинки, что порой затрудняет процесс идентификации, а также большое количество людей в кадре, что сильно нагружает систему и замедляет поиск нужного объекта.

3) Распознавание лиц для определения пола и возраста [10, 376 с.].

Цель такого распознавания – определение маркетингового плана. Речь идет о кинотеатрах, развлекательных центрах, выставках, концертах и тому подобное. Например, сеть кинотеатров «Cinemapark» уже давно запустило целую сеть определения пола и возраста своих посетителей по их лицу. Сделано это для того, чтобы понять какие маркетинговые инструменты нужно использовать для привлечения клиентов, повышения спроса, а также рекламную политику стоит выбрать.

Такой подход использования цифровых технологий распознавание лиц в маркетинговой сфере также имеет место быть в контексте данного исследования, так как позволяет не понять всю разносторонность и мобильность данной системы.

4) Авторизация и платежные системы.

Система авторизация человека по его изображению лица уже давно используется на всех платформах. Начиная от доступа к своему смартфону, заканчивая платежной системой, которая требует ваше изображение лица в качестве пароля. Самые известные платежные системы такие, как ApplePay и GooglePay используют для подтверждения транзакции FaceID.

Безусловно существует огромное количество перспективных сфер, в которые следует внедрить систему распознавания лиц, что позволит обеспечить безопасность, удобство пользования и цифровизацию.

В заключительной части исследования стоит сказать, что информационные технологии в XXI веке являются ведущим направлением, которое позволяет обществу перейти на новый этап развития. Технологии распознавания лиц безусловно являются частью всего технологического прогресса, так как они обеспечивают большинство потребностей людей в таких сферах, как предпринимательство, образование, культура, контроль на пропускных пунктах, банковский сектор и тому подобное.

Список литературы

1) Визильтер Ю. В., Желтов С. Ю., Князь В. А., Ходарев А. Н., Моржин А. В. Обработка и анализ цифровых изображений с примерами на LabVIEWIMAQVision. - М.: ДМК Пресс, 2017. - 25 с.
2) Земцов, Андрей Алгоритмы распознавания лиц / Андрей Земцов. - М.: LAPLambertAcademicPublishing, 2018. - 128 с.
3) Кухарев, Георгий Александрович Методы обработки и распознавания изображений лиц в задачах биометрии / Кухарев Георгий Александрович. - М.: Политехника, 2018. - 463 с.
4) Рожков, М. М. Использование текстурных карт Лавса и дискретного косинусного преобразования в задаче распознавания лиц / М.М. Рожков. - М.: Синергия, 2017. - 692 с.
5) Рейнгольд, Э. Комбинаторные алгоритмы: теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део. - М.:, 2018. - 320 с.
6) Афанасьев, Алексей Алексеевич Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Гриф УМО МО РФ / Афанасьев Алексей Алексеевич. - М.: Горячая линия - Телеком, 2019. - 254 с.
7) Кухарев, Г. А. Биометрические системы. Методы и средства идентификации личности человека / Г.А. Кухарев. - М.: Политехника, 2018. - 240 с.
8) Мовчан, Анатолий Компьютерные системы биометрической идентификации / Анатолий Мовчан. - М.: LAPLambertAcademicPublishing, 2015. - 724 с.
9) Русай, А.Н. Биометрическая аутентификация диктора в MATLAB. Учебное пособие / А.Н. Русай. - М.: Русайнс, 2017. - 512 с.
10) Яковлев, В.Б. Биометрическая обработка экспериментальных данных: моногр. / В.Б. Яковлев. - М.: Нобель Пресс, 2018. - 376 с.