4. Кваша Е.П. Управление ИТ-инфраструктурой как сервис // Материалы Международной мультидисциплинарной научно-практической конференции студентов, магистрантов и аспирантов "ЭМПИ - экономика, менеджмент, прикладная информатика и новые яркие идеи и решения". Брянск, БГТУ, 2016, 349-353 с.

5. Измалкова С. А., Внедрение высоких технологий в деятельность промышленно-экономических систем: интегрированный подход. Орел: ФГБОУ ВПО «Госуниверситет-УНПК», 2017

УДК 004.93.1

С.А. Кульмамиров, и. о. доцента
(Казахский национальный университет им.аль-Фараби);
Г.К. Ордабаева, ст. преп.; А.С. Кыдырбекова, ст. преп.
(Казахский национальный аграрный университет Алматы, Казахстан)

ИССЛЕДОВАНИЕ БИОМЕТРИЧЕСКОГО СПОСОБА РАСПОЗНАВАНИЯ ЛИЧНОСТИ

Аннотация: *В статье рассмотрены результаты авторских исследований по биометрической аутентификации и идентификации личности. Исследованный способ аутентификации используется для удостоверения личности людей в их биометрических данных (по овалу лица человека). Описан процесс доказательства и проверки подлинности личности через предъявление пользовательского биометрического образа. Аппаратное средство состоит из биометрических сканеров и терминалов. Оно фиксирует биометрический параметр (отпечаток пальца, радужную оболочку глаз, рисунок вен на ладони или пальце). Их полученных изображений составляется цифровая модель. Специальная программа обрабатывает данные, сортирует и сравнивает с изображениями из базы данных. Результаты аутентификации и идентификации личности выдает решение, кто представился перед сканером.*

Ключевые слова: БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ЛИЧНОСТИ, АУТЕНТИФИКАЦИЯ ПО ЛИЦУ, ИДЕНТИФИКАЦИЯ, БИОМЕТРИЧЕСКАЯ СИСТЕМА, ТЕРМИНАЛ, ЦИФРОВАЯ ОБРАБОТКА, ИДЕНТИФИКАТОР.

В настоящее время биометрическая аутентификация и идентификация личности являются способом аутентификации, использующим для удостоверения личности людей в их биометрических данных [1].

В статье излагается результаты исследований одного из биометрического способа распознавания личности по овалу лица. В этом способе процесс доказательства и проверки подлинности личности может осуществляться через предъявление пользователем своего биометрического образа. Далее путем преобразования этого образа в соответствии с заранее определенным протоколом биометрической системы аутентификации.

Рассматриваемая биометрическая система состоит из двух частей: аппаратных средств и специально написанной программы. Аппаратные средства включают в себя биометрические сканеры и терминалы. Они фиксируют тот или иной биометрический параметр (отпечаток пальца, радужную оболочку глаз, рисунок вен на ладони или пальце) и преобразуют полученную информацию в цифровую модель, доступную компьютеру для проведения соответствующей обработки. Специальной программой эти данные подлежат цифровой обработке, результаты обработки сортируют и сравнивают с типовыми изображениями базы данных. В случае положительного решения программа выдает решение, кто предстал перед сканером[2].

Для того, чтобы специальная программа биометрической системы смогла в дальнейшем идентифицировать личность, в ней необходимо учитывать исходные сведения с ненулевыми начальными условиями о его идентификаторах [3].

Биометрическая система как прототип типовой информационной системы (ИС) хранит не изображения реальных идентификаторов, а их цифровые модели. Когда специальная программа повторно обращается к системе, вновь формируется модель его идентификатора, и она сравнивается с моделями, уже занесенными ранее в базу данных (рисунок 1).

Приведем самый простой пример функционирования биометрической системы аутентификации и идентификации личности: человек поднимаетесь по лестнице, и заходит в лифт, он знает, на какой этаж ему нужно. Далее двери в квартиру перед человеком сами открываются. Компьютер и телефон «узнают» личность и не требуют ввода пароля.

Вот таким образом сейчас входят в общественную жизнь цифровые биометрические системы [4]. Автомобили, социальные сети, магазины - все приветствуют человека после биометрического сканирования, обращаются к нему по имени и предугадывают каждый его шаг.

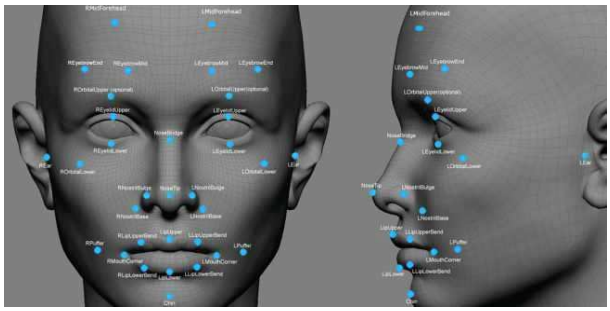

Рисунок 1 - Цифровая модель биометрической системы распознавания личности по лицу

Так работает алгоритм распознавания личности человека в биометрической системе. На первый взгляд может показаться, что любая организация или общественность, которая может себе позволить иметь биометрическую систему, следит за каждым шагом человека. Но в наше время сложено представить, как широко технологии распознавания личности распространились по всему миру и какие мощные перспективы обещают такие методы и технологии.

Помимо выше приведенного примера, биометрические системы распознавания лиц, например в образовании и обществе, позволяют делать такие простые или сложные вещи:

- подтверждение личности обучающегося во время онлайн-экзаменов;
- определение личности из «черного списка» на входе на стадионы и ночные клубы;
- оплата товаров по желанию конкретно известного человека;
- сохранение места личности в очереди при посещении парка аттракционов;
- разблокировка телефона или компьютера личности.

Также общеизвестно, что в одной только Москве уже работает сеть из более 150 000 камер наружного видеонаблюдения. От них никуда не скрыться, и это заставляет людей задумываться, но масштабы «слежки» не настолько велики. Сеть использует мощную систему распознавания лиц, но для ее работы необходимо много энергии, поэтому в режиме реального времени работают всего 2-4 тысячи камер. Массовым слежением за населением пока только пугают, поэтому стоит сосредоточиться на реальных плюсах работы биометрической технологии.

Авторы статьи проводят ряд исследований по изучению свойств биометрической системы распознавания лиц. Исследование началось после постановки актуальной задачи по распознаванию типового лица сознанием человека, т.е. его мозгом. После познания этих свойств биометрии ставилась вторая задача: как это делает компьютер?

Конечно, у человеческих лиц есть определенные свойства, которые легко описать[5]. Расстояние между глазами, положение и ширина носа, форма надбровных дуг и подбородка - все эти детали мозг человека подмечает бессознательно, когда он смотрит на другого человека. Компьютер же делает все это с определенной последовательностью и идентифицирующей точностью. Далее совмещая все эти метрики, получается математическая формула человеческого лица[6].

Также в исследованиях были попытки анализа существующих биометрических систем, чтобы выяснить насколько хорошо работает

система распознавания лиц в настоящее время. Разбор аналитических ситуации и цифровых данных показали, что созданные биометрические системы работают вполне неплохо, но они иногда ошибаются.

Если рассмотреть известную программу распознавания лица на Facebook или на другой социальной сетевой платформе, то в авторских исследованиях были заметны забавныеи положительные и отрицательные результаты И все же, хотя известные биометрические технологиине работает со 100-процентной точностью, они достаточно хороши и эффективны, чтобы найти широкое их применение в промышленных и экономических целях.

Пол Хоуи из NEC говорит [4], что их система распознавания лиц сканирует лица на предмет индивидуальных идентификаторов (рисунок 2).

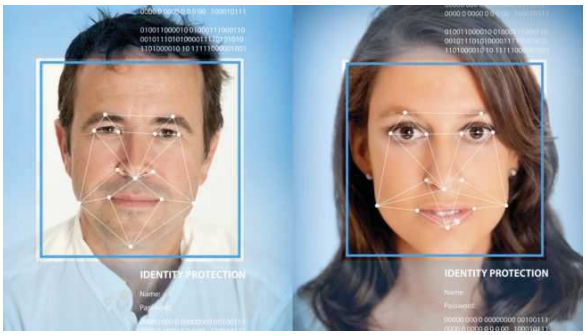

Рисунок 2 – Функционирование системы распознавания лиц человека

В статье лучше привести результаты его исследований, чем лишний раз их комментировать: «… к примеру, многие считают расстояние между глазами уникальной характеристикой. Или же это может быть расстояние от подбородка до лба и другие компоненты. Мы, в частности, учитываем 15-20 факторов, которые считаются важными, а также другие факторы, уже не настолько значимые. Создается трехмерное изображение головы человека, поэтому даже если она частично будет закрыта, мы все равно сможем получить точное соответствие. Затем система берет сигнатуру лица и пропускает ее через базу данных». Вот эти 5 предложений Пол Хоуи сущность работы специальной программы. Это один из первых в мире алгоритмов распознавания лица.

Теперь можно продолжить наши исследования, через совершенствование существующих алгоритмов или программ по аутентификации или идентификации личности. Прежде всего, распознавание лиц - это данные в цифровом формате удобные для формирования базы данных (БД). Данные можно собирать и хранить, зачастую без разрешения. Как только информация собрана и сохранена, она открыта и

для взлома. Это наталкивает на мысль обязательно предусмотреть в таких специальных программах и систему информационной безопасности данных (СИБ). Платформы со специальными программами, распознающим лица, пока не подвергались серьезным взломам, но по мере распространения технологий такие биометрические данные оказываются в руках все большего числа взламывающих людей (рисунок 3).

Рисунок 3 – Обоснование наличия СИБ по мере распространения технологий опознавания личности особенно среди взламывающих лиц

Существуют также вопросы владения описанными БД. Большинство людей не знают, что когда они регистрируются в социальных медиаплатформах, вроде Facebook, их данные с этого момента принадлежат этой самой Facebook. Поскольку число организации, использующих распознавание лиц, постоянно растет, очень скоро даже не придется загружать собственные фотографии в Интернет, чтобы оказаться скомпрометированным. Они уже там хранятся, и хранятся давно [5].

Специальные программы работают по-разным алгоритмам, но в основе своей используют похожие методы и нейронные сети. У каждого лица человека есть множество отличительных признаков (в мире невозможно найти два идентичных лица).

К примеру, программное обеспечение FaceIt определяет эти признаки как узловые точки [3]. Каждое лицо содержит примерно до 80 узловых точек, схожих с теми, что указаны на рисунках 1 и 2: расстояние между глазами, ширина носа, глубина глазных впадин, форма подбородка, длина челюсти. Эти точки измеряются и создают числовой код –так называемый «отпечаток лица», который затем попадает в состав БД.

В прошлое столетие распознавание лиц опиралось на двумерные снимки для сравнения или идентификации других двумерных снимков из хранилища данных. Для достаточной эффективности и точности изображение должно было быть лицом, прямо смотрящим в камеру, с небольшой дисперсией света и без особого выражения лица.

Такие алгоритмы и способы были не эффективными и не всегда срабатывали положительно. В большинстве случаев снимки не создавались в подходящей среде. Даже небольшое изменение света на изображении могла снизить эффективность системы, что приводило к высоким показателям отказа.

В нашем столетии на смену 2D пришло 3D-распознавание. Эта недавно появившаяся тенденция в программном обеспечении использует 3D-модель, обеспечивающую высокую точность распознавания лица [6]. Запечатлевая трехмерное изображение поверхности лица человека в реальном времени, теперь специальная программа выделяет отличительные черты для идентификации субъекта, где больше всего выдаются жесткие ткани и кость, например, кривые глазного гнезда, носа и подбородка. Эти области отличительных черт уникальны и не меняются со временем (рисунок 4).

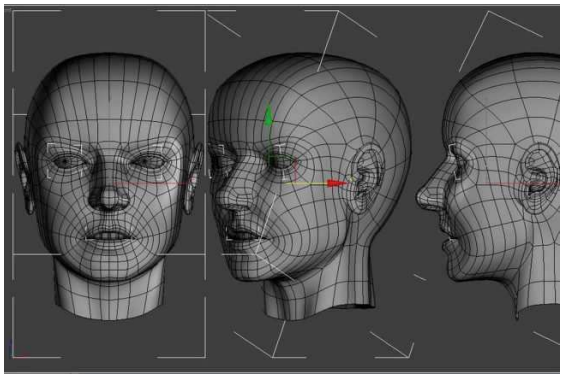

Рисунок 4 - Отличительные черты для идентификации субъекта

Используя глубину и ось измерения, на которые не влияет освещение, система трехмерного распознавания лиц может даже использоваться в темноте и распознавать объекты под разными углами (даже в профиль). Такая специальная программа реализуется выполнением нескольких этапов, идентифицируя человека:

- обнаружение - получение снимка при помощи цифрового сканирования существующей фотографии (2D) или видео для получения живой картинки субъекта (3D);

- центровка - определив лицо, программафиксируетположение головы, размер и позу;

- измерение- программа измеряет кривые на лице и биометрическая система с точностью до миллиметра и создает шаблон;

- репрезентация - система переводит шаблон в уникальный код. Этот код задает каждому шаблону набор чисел, представляющих особенности и черты лица;

- сопоставление - если снимок в 3D и БД содержит трехмерные

изображения, сопоставление пройдет без изменений снимка. Но если БД состоит из двумерных снимков, трехмерное изображение раскладывается на разные составляющие (словно сделанные под разными углами двумерные снимки одних и тех же черт лица), и они конвертируются в 2D-изображения. И затем находится соответствие в базе данных;

- аутентификация или идентификация - в процессе верификации снимок сравнивается только с одним из снимков в БД (в масштабе 1:1). Если целью обработки изображения является идентификация, то снимок сравнивается со всеми снимками в БД. Это приводит к ряду возможных совпадений снимков в масштабе 1:N.По необходимости применяются тот или иной другой метод биометрической идентификации.

Столетие назад биометрические системы распознавания лиц находили применение в основном в сфере правоохранения, поскольку государственные органы использовали их для поиска случайных лиц в толпе. Некоторые правительственные органы также использовали подобные системы для безопасности и для устранения мошенничества на выборах.

Однако есть много других ситуаций, в которых такая специальная программа становится популярным и востребованным. Биометрические системы становятся все дешевле, их распространение растет. Теперь они совместимы с камерами и компьютерами, которые используются банками, гостиницами и аэропортами. Туристические агентства работают над программой «бывалого путешественника»: с ее помощью они проводят быстрый скрининг безопасности для пассажиров, которые добровольно предоставляют информацию. Очереди в аэропортах будут продвигаться быстрее, если люди будут проходить через биометрическую систему распознавания лиц, сопоставляющую лица с внутренней БД.

Рисунок 5 - Сопоставление лиц в биометрической системе

Другие широкие применения включают банкоматы и терминалы выдачи наличных денег. Специальная программа может быстро проверить лицо клиента. После разрешения клиента банкомат или терминал делает снимок лица. Программа создает отпечаток лица, защищающий клиента от кражи личных данных и мошеннических тран-

закций. Далее банкомат просто не выдаст деньги человеку с другим лицом. Все так просто, даже ПИН-код не потребуется.

Особенно важным и интересным может быть развитие биометрической технологии распознавания лиц в сфере банковских переводов. Из публикации СМИ известно, что недавно российский банк «Открытие» представил собственное уникальное решение, разработанное под технологическим брендом «OpenGarage». Алгоритм бренда состоит: перевод денег по фотографии в мобильном приложении «Открытие.Переводы». Вместо того чтобы вбивать номер карты или телефона, достаточно просто сфотографировать человека, которому нужно сделать перевод. Биометрическая система распознавания лиц банка сравнивает фото с эталонным снимком из БД. Эталонный снимок был сделан банком, когда банк выдавал пластиковую карту. Специальная программа теперь подсказывает клиенту имя и фамилию. Останется только изъять карту с банкомата и ввести требуемую сумму.

Это особенно важно, когда клиенты сторонних банков также могут использовать эту функцию для переводов клиентам «Открытия». Отправитель переводов может пользоваться картой любого российского банка (рисунок 6).

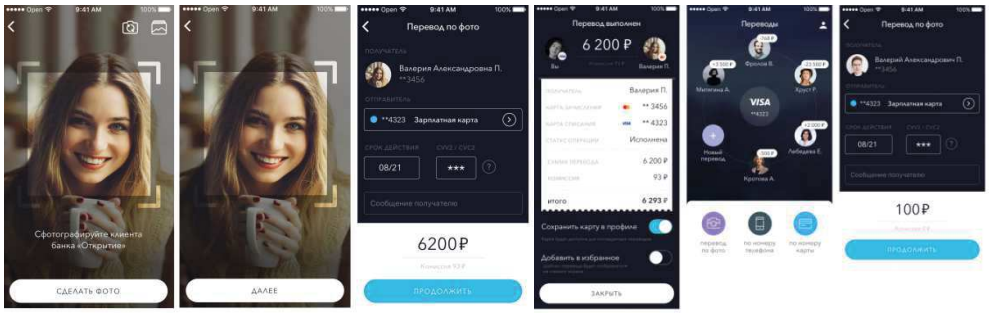

Рисунок 6 - Уникальное решение российского банка «Открытие», представленное под технологическим брендом «OpenGarage»

Здесь уникальностью является использование фотографии клиента вместо номера банковской карты. Это является принципиально новым подходом к онлайн-переводам. Технология основана на использовании нейронной сетевой системы распознавания лиц. Алгоритм биометрической системы банка позволяет с высокой степенью точности идентифицировать клиента по его биометрическим данным. Выгодный для клиентов банка сервис открывает для них совершенно новые жизненные сценарии для выполнения денежных переводов. В настоящее время ни один из участников финансового рынка в мире не предлагает подобного сервиса своим клиентам.

Таким образом, результаты проведенных исследований по био-

метрической аутентификации и идентификации личности показывают, что рассмотренный способ аутентификации используется для удостоверения личности людей в их биометрических данных (по овалу лица человека). Здесь процесс доказательства и проверки подлинности личности осуществляется через предъявление пользователем своего биометрического образа. Исследованная биометрическая система состоит из аппаратных средств и специальной программы. Аппаратные средства включают в себя биометрические сканеры и терминалы, фиксирующие биометрический параметр (отпечаток пальца, радужную оболочку глаз, рисунок вен на ладони или пальце). Эти цифровые устройства преобразуют полученную информацию в цифровую модель, доступную компьютеру для проведения соответствующей обработки. Специальная программа выполняет цифровую обработку данных. Результаты обработки сортируются и сравниваются с типовыми изображениями из базы данных. Своим положительным решением специальная программа выдает результаты аутентификации и идентификации личности, представившейся перед цифровым сканером.

ЛИТЕРАТУРА

1 Milborrow S. Locating facial features with active shape models: Master's thesis. – S. l.: Faculty of Engineering, University of Cape Town, 2007. – 103 p.

2 Броневич А. Г., Каркищенко А. Н. Вероятностные и возможностные модели классификации случайных последовательностей. – Таганрог: ТРТУ, 1996. – 196 с.

3 Кульмамиров С. А., Бейбиткызы Ф. Идентификация ориентира лица человека по ключевым точкам. Сборник трудов ICITE-218 - V-ойМеждународнойконференции «Промышленные технологии и инжиниринг», посвященная 75-летию Южно-Казахстанского государственного университета имени М. Ауэзова и 90-летию академика Сулейменова С.Т. 2018.

4 Броневич А. Г., Гречухин И. А., Каркищенко А. Н. Нечеткая классификация вероятностных распределений в задаче распознавания лиц // Обозрение прикладной и про- мышленной математики. – 2011. – Т. 18, вып. 6. – С. 530–531.

5 Cootes T. F., Taylor C. J. Technical Report: Statistical Models of Appearance for Computer Vision // The University of Manchester School of Medicine, 2004. – 125 p.

6 Kirby M., Sirovich L. Application of the Karhunen-Loeve procedure for characterization of human faces // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1990. – Vol. 12. – P. 103–108.