УДК 004.056.5:612.087.1

ЗАЩИТА ДОКУМЕНТА С ИСПОЛЬЗОВАНИЕМ ДЛЯ ЭЛЕКТРОННОЙ ПОДПИСИ QR-КОДА, СОДЕРЖАЩЕГО ЛИЦЕВУЮ БИОМЕТРИЧЕСКУЮ ИНФОРМАЦИЮ

ТЫНЫБЕКОВА У. М., ТОКТАУ Д. С., КАЗИЕВА Н. М.

Евразийский Национальный Университет имени Л.Н. Гумилева
(Казахстан, г.Астана)

E-mail: ulzhan.tynybekova@mail.ru, dinarats11@mail.ru

Аннотация. Современный этап развития общества характеризуется непрерывным процессом совершенствования информатизации и телекоммуникационных технологий. Благодаря этому расширяется сфера внедрения коммуникационных и вычислительных систем. В связи с этим важной задачей является обеспечение достаточной защиты этих систем для их эффективного функционирования в условиях проявления информационных угроз. В этой статье рассматриваются вопросы защиты информации с использованием биометрии лица и QR-кода.

Abstract. The current stage of the society's development is characterized by a continuous process of improving informatization and telecommunication technologies. Thanks to this, the scope of implementation of communication and computing systems is expanding. In this regard, an important task is to ensure sufficient protection of these systems for their effective functioning in the face of information threats. This article discusses the issues of information protection using facial biometrics and a QR code.

Введение

На сегодняшний день деятельность любой организации связана с получением и передачей информации, т.е. информация является стратегически важным товаром. Проблема защиты информации от внешнего доступа и негативных воздействий на нее является актуальной.

В настоящее время биометрическая идентификация является одним из наиболее защищенных методов информационной безопасности.

В Казахстане набирает популярность применение биометрии: ее уже активно используют банки, со следующего года планируется запуск закона об обязательной биометрической регистрации. Биометрические данные уже используются при дистанционном получении государственных услуг в приложении eGov mobile. Для подтверждения личности нужно пройти видео идентификацию: приложение предлагает включить камеру, далее детектируется лицо по изображению лица. В Казахстане также можно получить биометрический паспорт, который содержит в себе электронные носители информации, также паспорт соответствует международым требованиям и стандартам, предъявляемыми к машиночитаемым проехдеым документам [1].

Проблема безопасной и гарантированной отправки электронных документов нынче актуальна, как, когда-либо. В настоящее время всеобщая компьютеризация производства привела к тому, что документы в электронном виде распространяются в информационных системах, начиная и заканчивая свой жизненный кругооборот нередко будучи ни разу распечатанными. Это в современном мире большой плюс - экономия времени, бумаги, возможность мгновенно получить нужный документ. Такое применение документооборота требует бдительного внимания службы информационной безопасности предприятия: лёгкость обращения документов в информационной системе может быть опсаным, если защите информации в ней не обращено соответственного внимания.

Сегодня в сети пользователи интенсивно обмениваются электронными документами, особенно в том случае если работа связанно с удаленной работой. Поэтому, для того чтобы защитить документ в локальной сети по всем требованиям информационной безопасности, предлогается использование в качестве электронной подписи QR-кода, содержащего биометрическую информацию.

Работы проводимые в процессе исследования

В рамках работы были исследованы существующие научные работы в этой области. Были изучены биометрические методы индентификации личности. Из всех биометрических методов индентификации личности выбор был сделан в пользу лицевой биометрии, так как это один из методов бесконтактного получения биометричемкой информации. Так в процессе работы были изучены работы где рассматривались вопросы получения лицевой биометрической информации. В процессе изучения лицевой биометрической информации были рассмотрены различные способы получения лицевой информации. Одним из них является изучение биометрических баз данных для получения биометрической информации в ходе экспериментов. В рамках исследования были рассмотрены биометрические приметивы и параметры необходимые для индентификации изображения лица. Далее описывается одна из биометрических баз данных технологического института Джорджии.

База данных лиц технологического института Джорджии. База данных лиц технологического института Джорджии содержит изображения 50 человек, сделанные за два-три сеанса с 01.06.99 по 15.11.99 в центре обработки сигналов и изображений технологического института Джорджии [2]. Все на базе представлены 15 цветными изображениями в формате JPEG с забитым фоном, снятыми с разрешением 640x480 пикселей. Средний размер страницы на этих изображениях составляет 150x150 пикселей. Фотографии имеют переднюю и/или наклонную поверхность с различными чертами лица, условиями освещения и масштабом. Каждое изображение помечается вручную, чтобы определить положение страницы на изображении (рисунок 1).

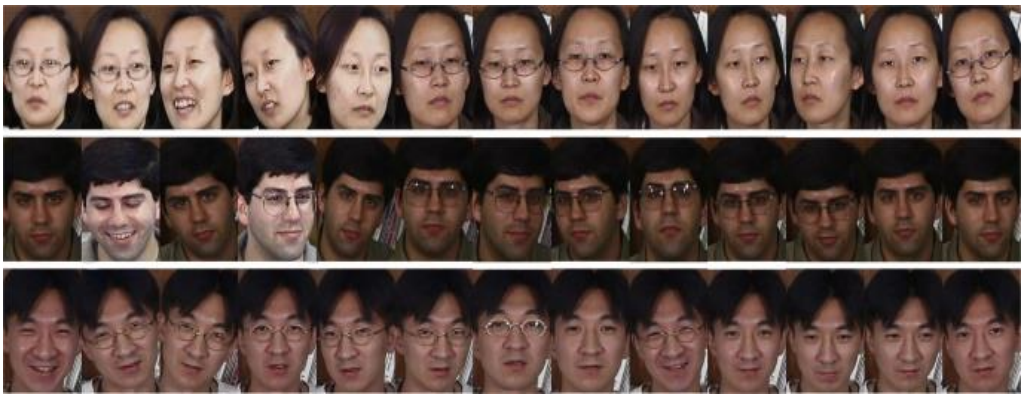

Рис. 1. Примеры изображений базы данных Georgia Tech face Database

Как видно из изображения, даже если есть перекрывающиеся объекты, такие как очки, система находит лицо этого человека. Кроме того, несмотря на некоторое сходство лиц разных людей, алгоритм определяет их как разные. При проведении экспериментов в базе данных лиц технологического института Джорджии результат на пороге 0.4 был 100%. Следует отметить, что во время экспериментов с пределом 0.5 появились ошибки первого типа (FAR). Поэтому рекомендуется снизить порог до 0.4.

А также, проводились эксперименты на основе собственных рисунков. Результаты можно увидеть на рисунке 2.

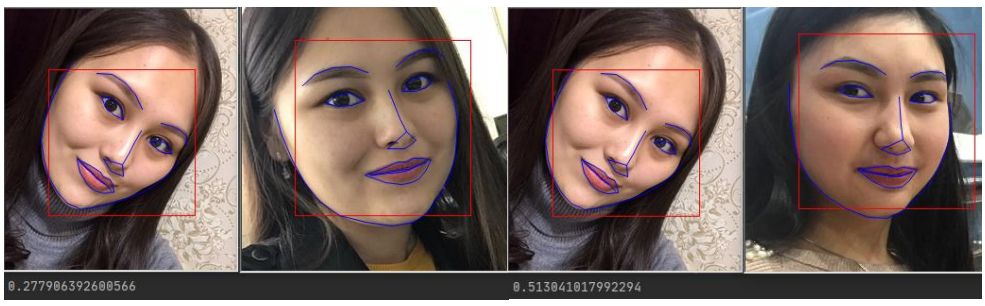

Рис. 2. Эксперименты проводимые на базе данных созданных в рамках исследования

Как видно из рисунка, расстояние между изображениями одного человека составляло 0.27, а между разными людьми - 0.51.

Для выравнивания поверхности можно использовать алгоритм, называемый «оценка антропометрических точек». Есть много способов сделать это, но это самый популярный подход, предложенный Вахидом Кэземи и Жозефиной Салливан в 2014 году [3].

Основная идея состоит в том, что 68 характерных точек (отметин), присутствующих на каждой странице, различаются-выступ подбородка, внешний край каждого глаза, внутренний край каждой брови и т. д. Затем устанавливается алгоритм обучения машины поиску этих 68 характерных точек. На каждой странице находится 68 антропометрических точек. Благодаря этому, независимо от того, как повернуто лицо, вы можете центрировать глаза и рот так, чтобы они находились примерно в одном положении на изображении. Это значительно повышает точность следующего шага.

В рамках исследования лицевой биометрической индентификации по изображению лица были использованы антропометрические точки лица. Выше представлены некоторые результаты полученные в процессе проведения экпериментов.

Описание процесса лицевой биометрической идентификации и создание QR-кода. Сначала камера делает несколько снимок. На этом этапе берется несколько кадров. Затем в блоке детекции происходит распознавание лиц, процесс обучения. Здесь читается только страница, а задний фон, объекты не берутся. Далее берутся антропометрические точки поверхности. При биометрической идентификации лица принято решение, что достаточно получить 68 антропометрических точек. Поэтому считывается 68 антропометрических точек поверхности. В следующем блоке усреднения кадров получается средний одиночный кадр из тех, которые изначально были сделаны несколько раз. Затем антропометрические точки и информация о личности в этом кадре отправляются в блок генерации QR-кода. В блоке генерации QR-кода мы получаем цифровую форму, математически кодируя антропометрические точки. Его и информацию о физическом лице подключают к QR-коду. Наконец, появится QR-код и отдельная цветная фотография. Этот процесс выполняется на стороне отправителя (рисунок 3).

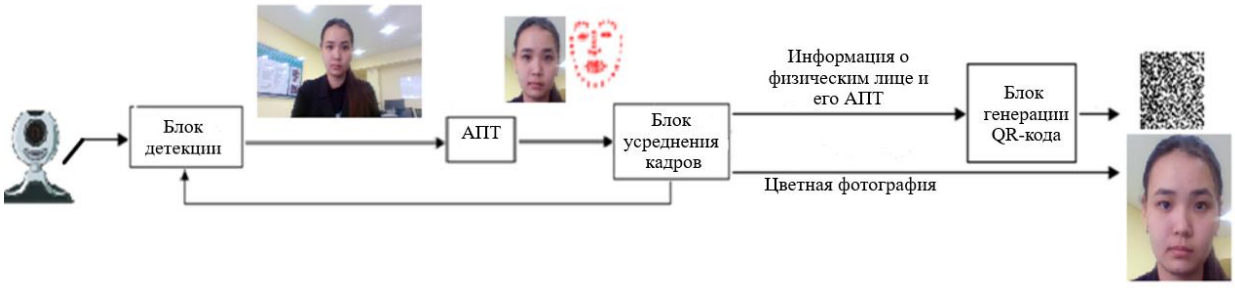

Рис. 3. Схема генерации QR-кода, содержащего биометрическую информацию

Для реализации процесса в блоке детекции необходимо разработать его модель. Разработка модели проводилась на базе изображений лиц Georgia Tech face database в свободном доступе в сети Интернет [2].

После отправки сигнала по рисунку 3 на принимающей стороне происходит обратный процесс. Сгенерированный QR-код в отправленном документе считывается. QR-код считывается путем декодирования закодированной информации внутри. Затем берутся антропометрические точки отправляющего сотрудника. На принимающей стороне фотография того же сотрудника в базе данных помещается и сравнивается с антропометрическими точками, полученными путем декодирования. Если есть совпадение, то подтверждается, что документ пришел от конкретного сотрудника-отправителя (рисунок 4).

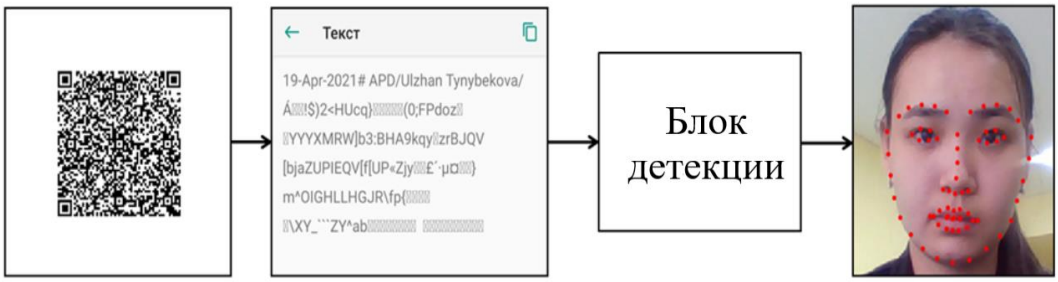

Рис. 4. Схема декодирования QR-кода, содержащая биометрическую информацию

Проектируемая система веб-камера, подключенная к компьютеру, должна сфотографировать сотрудника и сделать несколько снимков. Далее следует страницы в кадрах. При усреднении кадров получается последний фактический кадр,и его антропометрические точки. После этого QR-код генерируется. В QR-коде содержится информации о сотруднике и его биометрические данные. В результате получается QR-код и фотография сотрудника. После этого принятый QR-код должен быть прочитан. Полученные биометрические данные, ПК выставляются и сопоставляются с фотографией в базе данных фотографий размещенных сотрудников. При наличии соответствия документ принимается и подписывается.

Сведения о способах получения информации с помощью QR-кода, о процессе ее декодирования взяты из следующей статьи [5].

Заключение

Поскольку в настоящее время система информационной защиты недостаточно развита, разработка новых методов защиты по-прежнему актуальна. Поэтому, изучая методы защиты информации и информационной безопасности, мы предлагаем способ защиты информации в качестве электронной подписи с помощью QR-кода, содержащего биометрические характеристики. Этот метод используется при удаленной работе и является полезным и безопасным для обмена информацией. В этом методе в QR-код вводятся биометрические характеристики, то есть антропометрические точки поверхности лица человека. Биометрические признаки каждого человека уникальны, и достигается высокий уровень безопасности, поскольку его невозможно потерять, забыть. Этот биометрический документ можно быстро прочитать с помощью QR-кода, и QR-код отвечает за конфиденциальность данных. В обмене документами это важный критерий.

Список использованных источников

1. https://mk-kz.kz/social/2022/08/17/ugrozhaet-li-vvedenie-biometrii-chastnoy-zhizni-kazakhstancev.html?ysclid=laj5s6id5r954317221
2. https://computervisiononline.com/dataset/1105138700
3. Kazemi V., Sullivan J. One millisecond face alignment with an ensemble of regression trees // The IEEE Xplore. 2014. P. 1867–1874.
4. Brunelli R. and Poggio T.Face recognition: features versus tem- plates// IEEE Trans. on Pattern Analysis and Machine Intel.- 1993. — Vol.15. — No 10. — P. 1042-1052.
5. Казиева Н. Модуль онлайн-системы генерации QR-кода с координатами антропометрических точек изображения лица // Сборник трудов VII конгресса молодых ученых (Санкт-Петербург, 17-20апреля 2018г.) -2018. - Т. 2. - С. 28-30