**BC/NW 2022 № 1 (39):11.1**

**КОМПЛЕКСНАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

Абросимов Л.И., Сорокин А.Ю.

**Введение**

При работе с конфиденциальными данными, необходимо уделять особое внимание защите от несанкционированного доступа.

Защита от внешних угроз всегда стоит на первом месте, но зачастую недобросовестность сотрудников организации наносит не меньший вред. Поэтому важно использовать такие системы защиты, при которых несанкционированный доступ к пользовательскому компьютеру сводится к минимуму.

Предлагается комплексно использовать две биометрические системы защиты.

В начале работы с пользовательским компьютером используется первая система защиты, использующая сканеры отпечатков пальцев.

В процессе работы с пользовательским компьютером осуществляется непрерывный контроль с использованием web-камеры, что обеспечивает работу второй системы защиты даже при кратковременных паузах отсутствия пользователя.

Использование комбинированных биометрических систем должно существенно повысить эффективность защиты. Однако, пользовательский компьютер должен предоставлять свои вычислительные ресурсы алгоритмам двух биометрических систем защиты, что может замедлить время выполнения штатных заданий.

Цель исследований состоит в выборе состава комбинированной биометрической системы и оценке эффективности биометрической системы защиты по набору следующих параметров: время распознавания, вероятность распознавания, объем занимаемой оперативной памяти и загрузка центрального процессора.

Актуальность темы данной работы обусловлена необходимостью уделять особое внимание защите от несанкционированного доступа, при работе с конфиденциальными данными.

Защита от внешних угроз всегда стоит на первом месте, но зачастую недобросовестность сотрудников организации наносит не меньший вред. Таким образом, объект исследования – организация, у которой может быть несанкционированный доступ к информации, поэтому важно использовать такие системы, при которых несанкционированный доступ к пользовательскому компьютеру сводится к минимуму. Предмет исследования - биометрические системы защиты информации персонального компьютера.

Предлагается комплексно использовать две биометрические системы защиты.

В начале работы с пользовательским компьютером включается первая система защиты, использующая сканеры отпечатков пальцев. В процессе работы с пользовательским компьютером осуществляется непрерывный контроль с использованием web-камеры, что обеспечивает работу второй системы защиты даже при кратковременных паузах отсутствия пользователя.

Использование комбинированных биометрических систем должно существенно повысить эффективность защиты. Однако, пользовательский компьютер должен предоставлять свои вычислительные ресурсы алгоритмам двух биометрических систем защиты, что может замедлить время выполнения штатных заданий.

Цель исследований состоит в выборе состава комбинированной биометрической системы и оценке эффективности биометрической системы защиты по набору следующих параметров: время распознавания, вероятность распознавания, объем занимаемой оперативной памяти и загрузка центрального процессора.

Для достижения поставленных целей необходимо решить следующие задач:

а) исследовать методы и способы распознавания личности по отпечаткам пальцев;

б) исследовать методы и способы распознавания личности по видеоизображению;

в) разработать программное обеспечение по распознаванию личности по отпечаткам пальцев;

г) разработать программное обеспечение по распознаванию личности по видеоизображению;

д) оценить работу программного обеспечения по критериям:

- время распознавания;

- вероятность распознавания;

- объем занимаемой оперативной памяти;

- по загрузке центрального процессора.

е) оценить эффективность комплексной защиты двух биометрических систем.

1. **Анализ биометрических систем защиты информации от несанкционированного доступа**

**1.1** Анализ оценки качества функционирования систем защиты информации от несанкционированного доступа.

На сегодняшний день сложилась наиболее распространенная практика для сравнения результатов работы систем защиты с помощью FRR (False Rejection Rate) и FAR (False Acceptance Rate).

FRR - вероятность отказа доступа человеку, имеющего допуск. Её ещё называют Ошибкой первого рода (type I error, misdetection).

FAR - вероятность ложного обнаружения ( совпадения биометрических характеристик двух людей). Её ещё называют Ошибкой второго рода (type II error, false alarm) [3].

При сравнении систем пользуются следующим принципом: cистема тем лучше, чем меньше значение FRR при одинаковых значениях FAR.

Проблема заключается в том, что не все разработчики алгоритмов и систем распознавания публикуют эти характеристики. Вызывают также сомнения и некоторые опубликованные данные. В любом случае, при выборе алгоритмов или систем распознавания, нужно использовать те системы, где эти характеристики заявлены. Это дает некоторую гарантию на достоверный результат.

1.2 Анализ методов распознавания по отпечаткам пальцев

Дактилоскопия, как способ идентификации [человека](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D0%BA) по [следам пальцев](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BB%D0%B5%D1%86) рук, предполагает пусть и очень маленькую, но вероятность совпадения отпечатков пальцев у двух разных людей. Однако, в ограниченном сообществе людей, таком как сотрудники предприятия, или группа лиц имеющая доступ к ПК, такую вероятность легко исключить с помощью соответствующих программ и простым визуальным сравнением. Таким образом, все дальнейшие рассуждения будут основываться на положении, что отпечатки пальцев, поступающие для идентификации, у разных людей будут отличаться.

Кожа человека на ладонях и пальцах имеет объемную структуру, которая образована как из отдельных бугорков, так и из сросшихся между собой бугорков. Между бугорками остаются пустые бороздки. После сканирования, на снимке, бугорки видны как темные пятна или линии разной конфигурации, а пустые бороздки между ними как светлые (рисунок 1.1).



Рисунок 1.1 - Отпечаток пальца человека

Рисунок, который они собой представляют уникален. На сегодняшний день существуют несколько методов распознавания отпечатков [4,5,6,7,8].

*1.2.1 Корреляционное сравнение*

Полученное изображение отпечатка накладывают на эталонное изображение отпечатка и подсчитывается корреляция (по уровню интенсивности) между соответствующими пикселями. По значению коэффициента корреляции принимается решение об идентичности отпечатков.

Недостатки:

* необходимо осуществлять поэтапные сдвиги изображения отпечатка относительно эталонного в различных направлениях, в том числе вращать вокруг центра, чтобы максимально совместить изображения;
* при поиске совпадений со многими эталонными изображениями количество операций возрастает многократно.

Из-за сложности и длительности работы данного алгоритма он практически не используется.

*1.2.2 Сравнение по узору*

Полученное со сканера изображение отпечатка пальца, разбивается на ячейки (размер ячеек зависит от требуемой точности), рисунок 1.2.

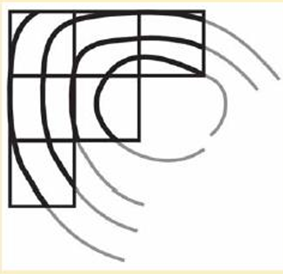


Рисунок 1.2 - Изображение отпечатка разбитого на ячейки

Расположение линий в каждой ячейке описывается параметрами некоторой синусоидальной волны. Данные волн (длина волны, направление волны) используются для идентификации. Сравнение отпечатков осуществляется по содержимому ячеек.

Достоинства: для данного метода подходят отпечатки с относительно низким качеством сканирования.

Недостатки: сложная реализация и сложный, объемный математический аппарат.

Вследствие указанных недостатков данный метод применяется редко.

*1.2.3 Сравнение по особым точкам*

Отпечаток каждого человека уникален. Однако, при более близком рассмотрении, становится видно, что рисунок состоит из повторяющихся по структуре фрагментов (рисунок 1.3), которые могут присутствовать на отпечатках других людей. Это окончания папиллярных линий и места, где эти линии разветвляются.

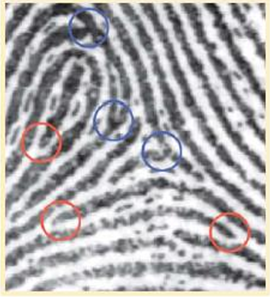


Рисунок 1.3 - Разветвления и окончания папиллярных линий

По изображению отпечатка пальца формируется шаблон (рисунок 1.4), на котором выделены конечные точки и точки ветвления. При сравнении, карта этих точек сравнивается с шаблоном эталона и по количеству совпавших точек принимается решение по идентичности отпечатков.



Рисунок 1.4 - Шаблон отпечатка пальца

Сравнение точек осуществляется корреляционными методами, из предположения, что положение точек соответствуют друг другу.

Достоинства: простая (относительно) реализации и высокая скорость работы.

Недостатки: для реализации необходимо, чтобы снимок отпечатка содержал не менее 500 пикселей. Большинство современных сканеров обеспечивают такое разрешение и больше.

Благодаря своим достоинствам и возможностям технической реализации, данный метод чаще всего применяют на практике. Применим в данной работе метод сравнения по особым точкам для распознавания по отпечаткам пальцев.

*1.2.4.* *Сравнение отпечатков по особым точкам*

Отсканированный отпечаток пользователя проходит все те же этапы обработки, что и эталонный отпечаток:

* фильтрация;
* бинаризация полученного изображения;
* скелетизация изображения;
* выделение особых точек.

После чего можно приступать к сравнению отпечатков. Отсканированный отпечаток будет отличаться от эталонного поворотом, смещением, изменением масштаба и площадью соприкосновения в зависимости от того, как пользователь прикладывает палец к сканеру.

Определяются параметры аффинных преобразований (угол поворота, масштаб и сдвиг), при которых некоторая деталь из одного вектора соответствует некоторой детали из другого. Эти параметры пытаются применить к другим деталям вектора рисунок 1.11.

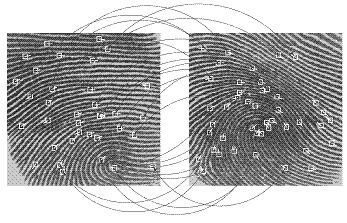


Рисунок 1.11 - Сопоставление деталей отпечатков

Оценка соответствия отпечатков с помощью коэффициента соответствия. Коэффициента соответствия рассчитывается как процент совпавших точек по отношению к числу особых точек отпечатка и выполняется по формуле:

P=(D\*100%)/(k), (4)

где D - количество совпавших особых точек;

k - количество особых точек отпечатка.

Поскольку количество особых точек у эталона и отпечатка разное, расчет производится для эталона по формуле:

Pэт=(D\*100%)/(kэт), (5)

где D - количество совпавших особых точек,

kэт - количество особых точек эталона.

Расчет производится для отпечатка по формуле:

Pот=(D\*100%)/(kот), (6)

где D - количество совпавших особых точек,

kот - количество особых точек отпечатка.

Из двух значений Pэт и Pот  берут меньшее значение.

Если результат превышает порог, отпечатки считаются идентичными (порог может быть понижен выставлением другого уровня бдительности).

*Выводы*:

Таким образом, для идентификация отпечатков пальцев выбран метод сравнения по особым точкам. На каждом этапе реализации метода были выбраны следующие способы:

- глобальная бинаризация (этап бинаризации);

- метод Зонго-Суня (этап скелетизации);

- поиск точек окончания и разветвления (этап выделение особых

точек);

- расчет коэффициента соответствия (этап оценки соответствия отпечатков пальцев).

1.3 Анализ методов распознавания по лицу

*1.3.1 Этапы распознавания лиц*

Технология распознавания лиц работает путем сопоставления лиц людей, попадающих в область видимости специальных камер, с изображениями людей в списке наблюдения. Списки наблюдения могут содержать фотографии людей которым разрешен допуск в организации, которые подозреваются в каких-либо правонарушениях или любые другие группы лиц подлежащих наблюдению на законных основаниях.

Существуют различные технологии распознавания лиц, но их работу можно разбить на следующие этапы:

1. Обнаружение лица.

В область видимости камеры могут попадать различные объекты реального мира (мебель, картины, цветы, животные, автомобили и т.д.). Алгоритм распознавания, на полученном изображении, должен уметь обнаруживать и фиксировать положение изображения лица, как одного, так и в толпе. При этом, это может быть человек смотрящий в анфас или под каким-то углом в камеру (величина этого угла различается у разных алгоритмов).

б) Анализ лица.

Выделенное, с изображения фотография, лицо подлежит сравнению с данными из списка сравнения. Возможны технологии сравнения с плоским изображением (технология 2D), т.е. фотографией, возможна технология сравнения с объемным изображением (технология 3D). Технология 2D проще в реализации по нескольким причинам:

- для нее проще получить фотографию человека;

- нужно хранить меньший объем исходных изображений человека;

- алгоритмы сравнения и распознавания проще в реализации.

Однако, надежность распознавания, на современном этапе, уступает технологии 3D.

в) Преобразование изображения в данные.

Для сравнения лиц людей необходимо сформулировать набор формальных признаков, которые, присутствуют у всех людей, и по которым будет происходить сравнение. У разных алгоритмов этот набор разный и является главным секретом разработчиков. Например, можно сравнивать расстояние между глазами, глубину глазниц, расстояние ото лба до подбородка, форму скул и контуры губ, ушей и подбородка. По мере эволюции алгоритмов стали учитывать минимум 68 точек на лице

Можно с помощью сверточных нейросетей обработать изображение и получить некий набор чисел присущий этому человеку. У другого человека этот набор чисел будет другим.

г) Поиск совпадения.

Поиск совпадения между изображением из списка наблюдений и изображением, полученным с камеры, происходит по набору формальных признаков, который используется конкретным алгоритмом распознавания (классификатором). Какое количество формальных признаков, и каких должно совпасть, чтобы сказать, что человек обнаружен, зависит от конкретного алгоритма распознавания.

*Выводы:*

Из рассмотренных классов решаемых задач в распознавании по изображению лица и методов их реализации для защиты информации на ПК от несанкционированного доступа лучше всего подходят нейронные сети по ряду причин:

- не требуется качественная предварительная обработка изображений, подлежащих распознаванию;

- работают в реальном масштабе времени с видеопотоком;

- распознают людей при различных условиях освещенности, измененияx ракурса, разных прическах, различных мимиках лица, наличии очков и бороды.

- демонстрируют высокую вероятность распознавания.

1.4 Особенности аппаратной реализации методов распознавания для ПК

Для реализации методов распознавания используются аппаратные средства: видеокамера, сканер отпечатка пальца, персональный компьютер. Характеристики этих устройств влияют на результаты распознавания.

*1.4.1 Характеристики и особенности применения сканеров отпечатков пальцев.*

Для сканирования отпечатков пальцев был выбран оптический сканер ZK6500 фирмы ZKTeco, который использует отражение светового излучения (Приложение Б). Критериями отбора были:

* разрешение изображения (не менее 500 dpi (пикселей на дюйм));
* возможность подключения к ПК;
* совместимость с операционной системой (Windows 7-10);
* цена.

*1.4.2 Характеристики и особенности применения видеокамер*

Для распознавания человека по его изображению необходимо к персональному компьютеру подключать видеокамеру, либо пользоваться встроенной камерой.

Для получения потока видеоизображения была выбрана видеокамера для потокового видео Canyon CNS-CWC5

Критериями отбора были:

* разрешение (видео) - 1920x1080, 1280x720, 640x480;
* частота кадров 30 Гц;
* возможность подключения к ПК;
* совместимость с операционной системой (Windows 7-10);
* цена.

*1.4.3 Характеристики и особенности применения ПК*

Для эффективной работы важен такой параметр компьютера как производительность. Производительность показывает сколько операций в секунду выполняет компьютер (измеряется в флопсах, 1 флопс означает одну операцию (например, сложение) над вещественными числами за 1 секунду). Современные компьютеры способны выполнять миллиарды операций в секунду, поэтому к размерности добавляются приставки системы СИ: TFLOPS (терафлопс), GFLOPS (гигафлопс) и т.д.

По возможности, компьютеры предприятия, с системой защиты персональных данных, должны быть оснащены достаточно современным оборудованием.

В частности, разработка экспериментального стенда, в данной работе, проводилась на компьютере со следующими техническими характеристиками:

* процессор – Intel(R) Core(TM) i5-2500 @ 3.30GHz;
* оперативная память – 8 Гб;
* тип системы – 64 разрядная операционная система Windows 10.

**2. Разработка экспериментального стенда**

2.1 Техническое описание стенда

Разработка экспериментального стенда проводилась на компьютере со следующими техническими характеристиками:

* процессор – Intel(R) Core(TM) i5-2500 @ 3.30GHz;
* оперативная память – 8 Гб;
* тип системы – 64 разрядная операционная система Windows 10.

Для получения персональных данных пользователя к ПК подключаются видеокамера и сканер отпечатков пальцев.

В качестве устройств для идентификации личности были отобраны видеокамера и сканер отпечатка пальца для ПК.

Для получения видеоизображения пользователя была выбрана видеокамера Canyon CNS-CWC5 (Приложение А), которая поддерживает три режима работы:

* 640x480 (30 Гц);
* 1280x720 (30 Гц);
* 1920x1080 (30 Гц).

Для сканирования отпечатков пальцев применен оптический сканер ZK6500 (Приложение Б) с разрешением изображения 500 dpi (точек на дюйм).

2.2 Создание модели системы защиты информации от несанкционированного доступа

*2.2.1 Реализация метода сравнения отпечатков по особым точкам*

Опишем практическую реализацию всех этапов этого метода.

а) Фильтрация изображения.

Фильтрацию изображения производят с помощью цифровых фильтров. На современном этапе нет необходимости заниматься их разработкой. Большинство из них реализовано в виде публичных программных библиотек.

При выборе фильтра необходимо стремиться к максимальному устранению шумов, и в то же время, к максимальному сохранению структуры папиллярных линий отпечатка. На рисунке 2.1 представлены два отпечатка пальца одного человека.

а) б)

Рисунок 2.1 - Отпечатки пальца одного человека

На рисунке 2.2 представлены те же отпечатки после обработки фильтром Гаусса с параметрами (7х7) ( функция GaussianBlur(img, img, Size(7, 7), 0), библиотека OpenCV)

а) б)

Рисунок 2.2 - Отпечатки пальца одного человека после обработки фильтром Гаусса

На рисунке 2.3 представлены отпечатки после обработки фильтром Гаусса с параметрами (7х7) и фильтрации адаптивным фильтром Гаусса (функция adaptiveThreshold(img, img, 255, ADAPTIVE\_THRESH\_GAUSSIAN\_C, CV\_THRESH\_BINARY, 15, 4 , Библиотека OpenCV). Адаптивный фильтр Гаусса осуществляет также бинаризацию изображения.

а) б)

Рисунок 2.3 - Отпечатки пальца одного человека после обработки фильтром Гаусса и адаптивным фильтром Гаусса

Как видно из рисунка 2.3, шумы между папиллярными линиями удалось убрать, но сами папиллярные линии порваны на множество мелких частей. При последующей скелетизации методом Зонго-Суня,

это приведет к образованию множества ложных точек окончания.

На рисунке 2.4 представлены отпечатки после обработки фильтром Габора ( библиотека fingerprint\_enhancer, функция fingerprint\_enhancer.enhance\_Fingerprint(img). Изображение инвертировано.

а) б)

Рисунок 2.4 - Отпечатки пальца одного человека после обработки фильтром Габора

Из рисунка 2.4 видно, что после обработки фильтром Габора удалось не только убрать шумы, но и сохранить целыми большинство папиллярных линий. Структура отпечатка отчетливо видна.

В данной работе, для фильтрации, применялся фильтр Габора.

б) Бинаризация изображения глобальным методом.

Для реализации бинаризации изображения глобальным методом необходимо задать порог преобразования. Поскольку фон изображения может варьироваться в широких пределах, то выбор порога становится непростой задачей. Неправильно выбранный порог может приводить к существенным потерям изображений папиллярных линий или полной потере изображения. Для того, чтобы не потерять изображение совсем, нужно найти значение яркости самого светлого пикселя и самого темного. Порог нужно выбирать в диапазоне между ними.

Бинаризация изображений реализуется с помощью функции threshold(img, img, 127, 255, cv::THRESH\_BINARY), где 127 порог бинаризации, библиотека OpenCV.

в) Скелетизация изображения (Метод Зонго-Суня).

Метод Зонго-Суня не требует входных параметров и является одним из самых простых. Алгоритм является многопроходовым (обрабатывает изображение пока не исключит пиксели подлежащие изменению). Вследствие этого, время обработки достаточно велико.

Опишем алгоритм Зонго-Суня.

1) Cоздадим матрицу байтов такого же размера как изображение отпечатка. Проинициализируем нулями. В ней будем фиксировать пиксели, которые уже изменяли, устанавливая 1;

2) Выставим флаг окончания алгоритма finish=true;

3) Введем следующую матрицу;

|  |  |  |
| --- | --- | --- |
| P9 | P2 | P3 |
| P8 | P1 | P4 |
| P7 | P6 | P5 |

Данная матрица попиксельно накладывается на изображение таким образом, чтобы P1 поочередно совмещался со всеми пикселями изображения.

Белый пиксель на изображения при этом имеет значение 0, а черный 1;

4) Пиксель меняет свой цвет с белого на черный, если выполняется ряд условий:

а) 2 <= P2+P3+...+P8+P9 <=6

б) S(P1) = 1,

где S(P1) - количество найденных последовательностей 01 в последовательности P2, P3, P4, P5, P6, P7, P8, P9, P2.

Т.е. для удаления пикселя, вокруг него должен существовать только один переход от нуля к единице.

в) P2\*P4\*P6 = 0

г) P4\*P6\*P8 = 0

Для работы с крайними левыми пикселями в) и г) пункты необходимо заменить на:

д) P2\*P4\*P8 = 0

е) P2\*P6\*P8 = 0

Алгоритм скелетизации отображен на рисунке 2.5

Конец

Да

Начало

Инициализация матрицы rempic

Флаг окончания алгоритма finish=true

Пока finish=true

2 <= P2+P3+...+P8+P9 <=6

S(P1) = 1

X=0

P2\*P4\*P6 = 0 P4\*P6\*P8 = 0

P2\*P4\*P8 = 0 P2\*P6\*P8 = 0

Да

Да

Да

Нет

Нет

Нет

Нет

Пиксель P1 окрасим в белый цвет

Пиксе

Пока X<imageI.Width

Пока Y<imageI.Height

Да

Нет

Да

Finish=false

Нет

rempic(x,y)=1

Нет

Да

imageI(x,y)=0

P1…P9=1

P1…P9=0

Да

Нет

Рисунок 2.5 - Алгоритм скелетизации (Метод Зонго-Суня)

На рисунке 2.6 представлены результаты скелетизации отпечатков пальцев после обработки фильтром Габора

Рисунок 2.6 - Результаты скелетизации отпечатков

В результате обработки изображения алгоритмом Зонго-Суня папиллярные линии стали толщиной в 1 пиксель, при этом не порваны и структура отпечатков сохранена.

г) Обнаружения особых точек.

Алгоритм обнаружения особых точек ищет на изображении отпечатка после скелетизации особые точки разветвления и окончания папиллярных линий [33,34] , (рисунок 2.7).

Рисунок 2.7 - Скелет отпечатка с фрагментами

На рисунке 2.7 зеленым цветом обозначены точки разветвления и сиреневым цветом точки окончания.

Опишем алгоритм обнаружения особых точек.

1) Устанавливаем счетчик особых точек count=0, счетчик суммы sum=0.

2) Введем следующую матрицу.

|  |  |  |
| --- | --- | --- |
| P9 | P2 | P3 |
| P8 | P1 | P4 |
| P7 | P6 | P5 |

Данная матрица попиксельно накладывается на изображение таким образом, чтобы P1 поочередно совмещался со всеми пикселями изображения. Белый пиксель на изображения при этом имеет значение 1, а черный 0;

3) Особая точка считается найденной если:

а) Центральный пиксель P1=1 (т.е. он белый);

б) sum = (P9 + P2 + P3 + P8 + P4 + P7 + P6 + P5)=3 (разветвление), если sum=1 (окончание);

4) Если особая точка найдена, увеличим счетчик count на 1.

Конец

Да

Начало

P1=1

sum = (P9 + P2 + P3 + P8 + P4 + P7 + P6 + P5)

count=count+1

Да

Да

Sum=3

Нет

Sum=0, count=0

Пиксель P1 окрасим в зеленый цвет

Пиксе

Пока X<imageI.Width

Пока Y<imageI.Height

Да

Да

Нет

imageI(x,y)=1

P1…P9=1

P1…P9=0

Да

Нет

Пиксе

Нет

Рисунок 2.8 - Алгоритм выделения особых точек

д) Сравнение отпечатков по особым точкам.

Для сравнения двух отпечатков по особым точкам нужно попытаться найти для каждой точки эталонного отпечатка соответствующую точку отсканированного отпечатка. Если осуществлять непосредственное последовательное сравнение, то время обработки будет очень большим. Процесс сравнения можно ускорить применяя следующий алгоритм:

1) Обозначим набор особых точек эталона как двумерный массив А(x,y) длиной n где, x,y координаты особых точек. Обозначим набор особых точек отсканированного отпечатка как двумерный массив B(x,y) длиной k где, x,y координаты особых точек.

Для эталонного и отсканированного отпечатка найдем геометрические центры, как среднее арифметическое координат их особых точек. Тогда, геометрический центр для эталонного отпечатка рассчитывается по формулам:

Gax= Gay=, (7)

где Gax, Gay – координаты геометрического центра,

xn, yn- координаты особой точки,

n – число особых точек.

Аналогично, геометрический центр для отсканированного отпечатка рассчитывается по формулам:

Gвx= Gвy=, (8)

где Gвx, Gвy – координаты геометрического центра,

xk,yk- координаты особой точки,

k – число особых точек.

Геометрические центры находятся в середине обоих отпечатков, но на практике, их координаты совпадают крайне редко.

2) Для обоих отпечатков находим расстояние от геометрических центров до особых точек отпечатков из массивов A и В. Ранжируем массивы А и В в порядке возрастания расстояния до геометрических центров. Тогда нулевые элементы массивов А(х0,y0) и В(х0,y0) оказываются самыми близкими к геометрическим центрам (рисунок 2.9). На рисунке 2.9 серым крестом обозначен геометрический центр, а белым крестом помечена ближайшая особая точка.



Рисунок 2.9 - Геометрический центр с ближайшей особой точкой

3) Рассчитываем разницу между координатами элементы массивов А(х0,y0) и В(х0,y0). Изменяем координаты всего массива В на полученную разницу, таким образом совместив изображения эталона и отпечатка в т. А.

4) Поскольку эталонное изображение и отпечаток могут быть повернуты относительно друг друга, то необходимо осуществлять поворот всех точек массива В с помощью формул аффинного преобразования на угол α (рисунок 2.10) .

Рисунок 2.10 - Необходимый угол поворота для совмещения отпечатков

Формулы аффинного преобразования:

X’ =  X cosα — Y sinα, Y’ = X sinα — Y cosα (9 )

где X’, Y’ – новые координаты точек после поворота.

Углы поворота обычно выбирают не более ± 13 градусов (окно сканера ограничивает повороты) с минимальным шагом Δ.

Минимальный шаг поворота рассчитывают из соображений, чтобы точки на краю кадра смещались не меньше чем на 1 пиксель.

После поворота всех точек массива В на минимальный шаг Δ производится подсчет совпавших точек и если процент совпадения превысил порог, отпечатки считаются совпавшими (т.е. принадлежат одному человеку).

При этом алгоритм останавливает работу и выводит соответствующее сообщение. Если нет, то осуществляется очередной поворот всех точек массива В на минимальный шаг Δ и производится подсчет совпавших точек.

Так будет происходить до тех пор, пока угол поворота не достигнет 13 градусов. Поскольку неизвестно, куда повернут отпечаток, все выше описанные операции необходимо выполнить и в другую сторону.

Если в пределах ±13 градусов порог не был превышен, выполняются действия из п. в), только теперь нужно совмещать нулевой элемент массива А(х0,y0) с первым элементом массива В(х1,y1).

На практике, для совмещения обычно используют не более 5-7 элементов массива В. Если и после этого порог не был превышен, берут первый элемент массива А(х1,y1) (и т.д.) и совмещают последовательно с элементами массива В.

Число элементов массива A также ограничиваются 5-7 шт. Если в результате всех выполненных действий, порог так и не был превышен, считают отпечатки НЕ совпавшими (т.е. принадлежащими разным людям).

На рисунке 2.11 отображены совмещенные эталонные отпечатки (белые линии) с отпечатками полученными при сканировании (зеленые линии). Процент совпавших точек при сравнении для этих пар отпечатков превысил порог сравнения. Пара отпечатков 2.11 а) принадлежат одному человеку, а пара отпечатков 2.11 б) принадлежат другому человеку.

а) б)

Рисунок 2.11 - Пары отпечатков пальцев у которых процент совпавших точек превысил порог сравнения

Координаты совмещаемых точек проверяют в пределах некоторого δ. Все этапы обработки отпечатка (фильтрация, бинаризация, скелетизация) вносят некоторую погрешность в значение координат особых точек. Кроме того, люди прикладывают палец к сканеру с разным усилием (даже в пределах одного отпечатка), что также вносит погрешность (рисунок 2.12).



Рисунок 2.12 - Фрагмент отпечатка из рисунка 2.11 а) левый нижний угол

На практике, чтобы учесть все погрешности, берут 10-15 полноценных, с хорошо прорисованным рисунком папиллярных линий, отпечатков пальца одного человека и постепенно увеличивают δ, до тех пор, пока процент совпавших точек большинства из отпечатков превысит порог сравнения. Эти действия выполняют для отпечатков нескольких людей.

* + 1. *Реализации методов распознавания по лицу*

Реализацию программ по распознаванию лиц можно осуществлять на разных языках программирования, таких как Python, C++, C#.

В данной работе для реализации программ для распознавания по лицу был выбран язык Python по следующим причинам:

* Python — это активно развивающийся скриптовый язык, который используют для решения большого объема самых разноплановых проблем и задач;
* на Python разрабатываются компьютерные приложения при работе с большим объемом информации, при разработке web-сайтов и других разнообразных проектов, используют в машинном обучении, в том числе для задач по распознаванию объектов;
* данный язык программирования используют крупные известные корпорации, такие как Spotify и Амазон (например, для анализа данных и создания алгоритма рекомендаций);
* существует большой набор бесплатных библиотек для обработки видеоизображений.

Распознавание лиц было реализовано двумя разными способами: с использованием библиотеки OpenCV и библиотеки Face recognition на языке Python.

Распознавание с использованием библиотеки OpenCV

[OpenCV](https://opencv.org/) — это библиотека с открытым программным кодом. Ее поддерживают различные языки программирования, например C++ и Python [35]. Библиотека может работать на многих операционных системах, например на Windows, Linux и MacOS.

Преимущества OpenCV:

* имеет открытый программный код и абсолютно бесплатна;
* написана на C/C++, что обеспечивает ей более высокое быстродействие в сравнении с другими библиотеками;
* хорошо работает при небольшом объеме оперативной памяти.

Библиотека OpenCV была разработана для эффектного вычисления и работы в реальном времени. По этой причине она подходит для распознавания лиц в реальном времени с помощью камеры.

Для реализации алгоритма распознавания с помощью библиотеки OpenCV необходимо осуществить 2 подготовительных этапа:

а) Подготовить файлы с изображением людей, которых необходимо распознать. Для одного человека делают несколько фронтальных фотографий с различными выражениями лица (рисунок 2.13).



Рисунок 2.13 - Фронтальные снимки человека с различными выражениями лица

Вышеуказанные фотографии преобразуют в черно-белый формат.

С помощью существующего в библиотеке OpenCV и уже обученного классификатора, основанного на алгоритме Виолы Джонса, его еще называют фильтрами Хаара (haarcascade\_frontalface\_default.xml), на изображении обнаруживают только лицо человека. Принцип работы фильтров Хаара заключается в том, что на изображении ищут паттерны характерные для человеческого лица. Есть некоторые общие черты, которые мы находим на самых обычных человеческих лицах (рисунок 2.14):

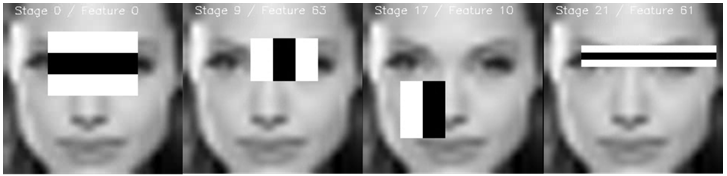


Рисунок 2.14 - Типичные паттерны для фильтров Хаара

У фильтров Хаара есть один существенный недостаток.

Они хорошо работают только с фронтальным изображением лиц. Любые повороты лица приводят к снижению вероятности распознавания.

Полученные изображения сохраняют в виде графического файла (рисунок 2.15) с наименованием User\_0.0.jpg, User\_1.0.jpg, Где цифра между точками идентификатор распознаваемого лица.



Рисунок 2.15 - Выделенное изображение лица

б) Для распознавания лиц в библиотеке OpenCV существует распознаватель LBPH (Гистограмма локальных двойных шаблонов, функция LBPHFaceRecognizer\_create). Распознаватель обучается с помощью выделенных изображений лица (функция train). Обученный распознаватель LBPH используется для распознавания людей в режиме реального времени по видео, которое поступает с видеокамеры. Распознавание идет в несколько этапов:

* кадры с видеопотока, так же как и фотографии, преобразуются в черно-белое изображение;
* с помощью классификатора основанного на фильтрах Хаара обнаруживают и выделяют на изображении лица;
* с помощью обученного распознавателя LBPH определяется, есть ли на видеоизображении лица людей присутствующие в списке для распознавания с некоторой степенью вероятности.

На рисунке 2.16 показан результат работы программы по распознаванию лиц.

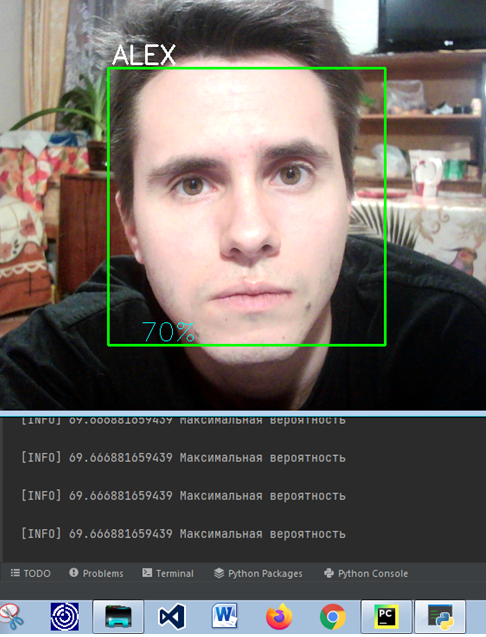


Рисунок 2.16 - Результат распознавания лица с видеопотока

Для распознавания использовалась видеокамера Canyon CNS-CWC5 Необходимо сказать, что результаты распознавания сильно зависят от положения человека перед камерой. Если лицо расположено строго напротив камеры, с минимальными отклонениями влево, вправо, вверх или вниз, то достигаются максимальные результаты по вероятности распознавания. Кроме того, результаты зависят от освещенности, и того, с какой стороны падает свет. Эксперимент производились при двух источниках освещения, сверху и навстречу распознаваемому человеку бытовыми осветительными приборами (рисунок 2.17).

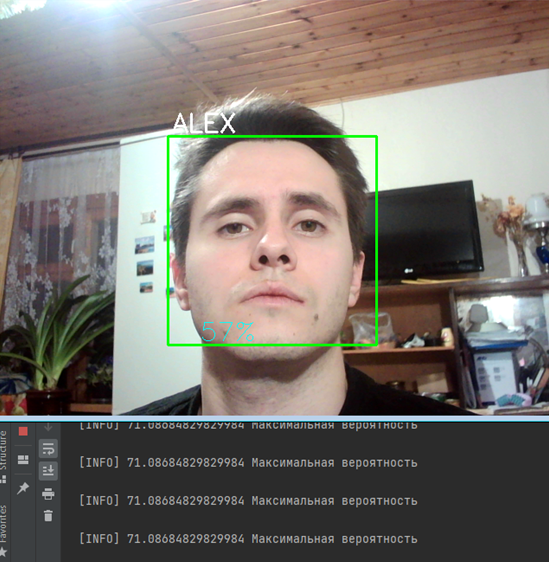


Рисунок 2.17 - Результат распознавания

Распознавание с использованием библиотеки Face recognition

Для реализации программы используем библиотеку [dlib](http://dlib.net/), которую поддерживает Дэвис Кинг. Она содержит реализацию глубокого метрического обучения. Библиотека [face\_recognition](https://github.com/ageitgey/face_recognition), созданная Адамом Гейтгеем, включает в себя функции распознавания лиц dlib и является по сути надстройкой над ней.

Распознавание с использованием библиотеки Face recognition, также начинается с выделения лица с любого изображения c помощью функции face\_locations(). После выделения изображения лица необходимо извлечь из него характерные черты. Для этого применяют процедуру под названием эмбеддинг. Библиотека [dlib](http://dlib.net/) содержит процедуры, которые можно использовать для конструирования векторов (эмбеддингов) изображений, функция face\_encodings(). Нейронная сеть осуществляет свертку изображения, а на выходе возвращает числовой вектор, характеризующий основные признаки данного лица (эмбеддинг). Пример такого преобразования показан на рисунке 2.18

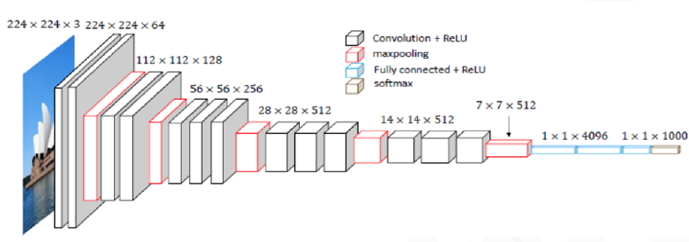


Рисунок 2.18 - Пример свертки изображения

Во время обучения нейронная сеть научилась выдавать близкие векторы для лиц, которые выглядят похожими друг на друга. Например, если у вас есть несколько изображений вашего лица в разные моменты времени, то некоторые черты лица могут меняться, но все же незначительно. Таким образом, векторы этих изображений будут очень близки в векторном пространстве (рисунок 2.19).

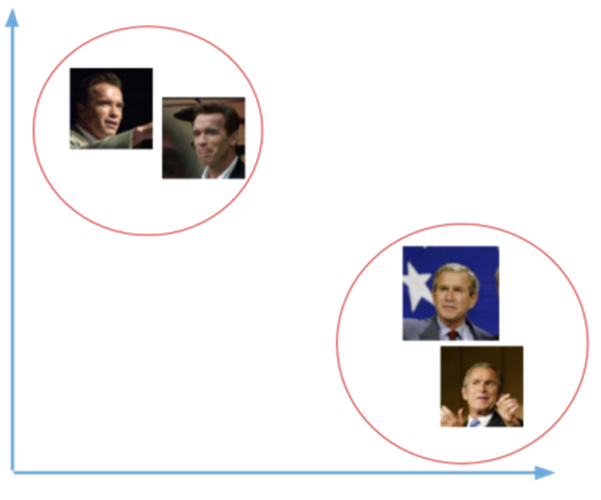


Рисунок 2.19 - Изображения лиц в соответствии с их векторами в векторном пространстве

Для распознавания человеческих лиц используется предобученная Дэвисом Кингом нейронная сеть. Она обучалась приблизительно на 3000000 изображений. Эта сеть выдает вектор длиной 128 чисел, который и определяет основные черты лица.

Процесс распознавания осуществляется путем сравнения векторов, полученных с фотографий лиц ( из списка имеющих доступ), с векторами, полученными с кадров видеопотока (функция compare\_faces)). Функция face\_distance рассчитывает вероятность совпадения фотографии и кадра из видеопотока. Необходимо заметить, что возможно использовать фотографии не только фронтальные, но и с небольшим поворотом лица, до 13-15˚. Это существенно повышает вероятность распознавания, поскольку человек перед камерой движется.

Распознавание проводилось на том же компьютере и с тем же исходным набором фотографий, которые применялись для работы с алгоритмом на основе библиотеки OpenCV. Сам эксперимент проводился в том же помещении, при тех же источниках освещения, при том же расположении распознаваемого лица. Результаты приведены на рисунке 2.20 и рисунке 2.21.

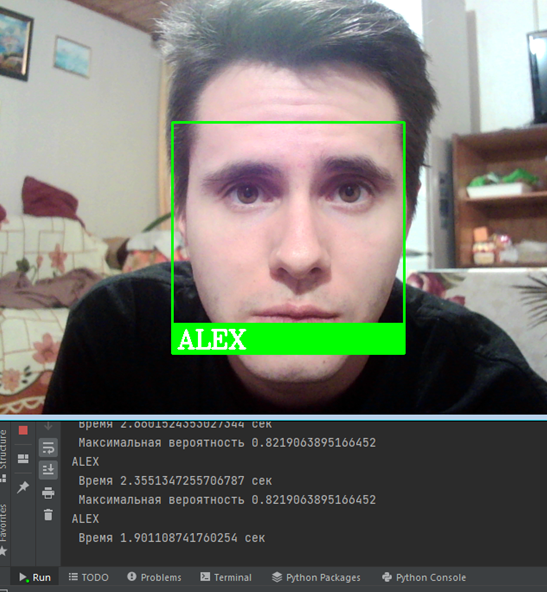


Рисунок 2.20 - Результат распознавания лица с видеопотока

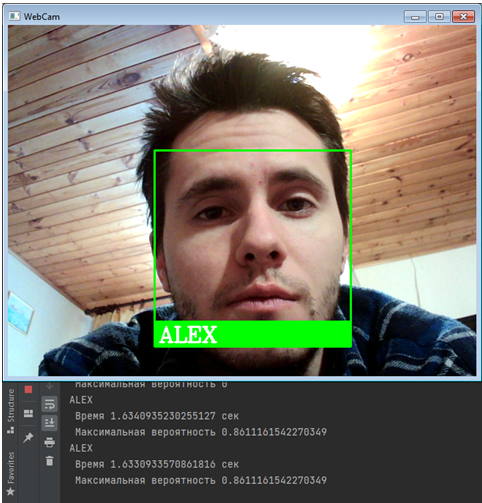


Рисунок 2.21 - Результат распознавания лица с видеопотока

**3. Исследование характеристик биометрических алгоритмов защиты от несанкционированного доступа**

3.1 Параметры реализации алгоритма распознавания по отпечаткам пальцев

Для расчета значений FAR и FRR необходимо определить число сбоев разного рода при распознавании. Для проведения этого эксперимента были сформированы 10 рядов различных отпечатков пальцев, по 10 отпечатков в ряду одного и того же пальца.

Эксперимент по получению значения FAR “свой с чужими” проводился следующим образом: из ряда брался отпечаток пальца в качестве эталона “свой” и проводилось сравнение с отпечатками из других рядов “чужие”. Далее, брался отпечаток из следующего ряда в качестве эталона “свой” и проводилось сравнение с отпечатками из других рядов “чужие”. Отпечатки, которые уже сравнивались, не использовались. Общее колличество сравнений VFAR рассчитывается по формуле:

VFAR =, (10)

где m-число отпечатков,

n- число рядов.

Расчет количества сравнений VFAR производится по формуле (10).

VFAR =

Эксперимент по получению значения FRR “свой со своим” проводился следующим образом: из ряда брался первый отпечаток пальца в качестве эталона “свой” и проводилось сравнение с отпечатками из этого же ряда. Далее выбирался следующий отпечаток и сравнивался с оставшимися в этом ряду. И так до конца ряда. Аналогично поступали с другими рядами. Общее количество сравнений VFRR рассчитывается по формуле:

VFRR =, (11)

где m-число отпечатков,

n- число рядов.

Расчет количество сравнений VFRR по формуле (11)

VFRR =

Таким образом, в ходе эксперимента были получены 3 ложных распознавания чужого отпечатка, что соответствует FAR=0,0066 (0,66%), и 15 отказов при распознавании своего отпечатка, что соответствует FRR=0,034 (3,4%).

В ходе эксперимента фиксировались и другие параметры алгоритма, которые представлены в таблице 3.1.

Таблица 3.1 - Основные параметры реализованного алгоритма

|  |  |
| --- | --- |
| Список параметров | Величина параметра |
| Максимальный коэффициент соответствия, % | 84 |
| Время распознавания, сек | 4 |
| Загрузка центрального процессора,% | 44 |
| Объем памяти ОЗУ, Мбайт | 20 |

На рисунке 3.1 представлена загрузка ЦП компьютера. Загрузка процессора разработанной программой составила 44%.

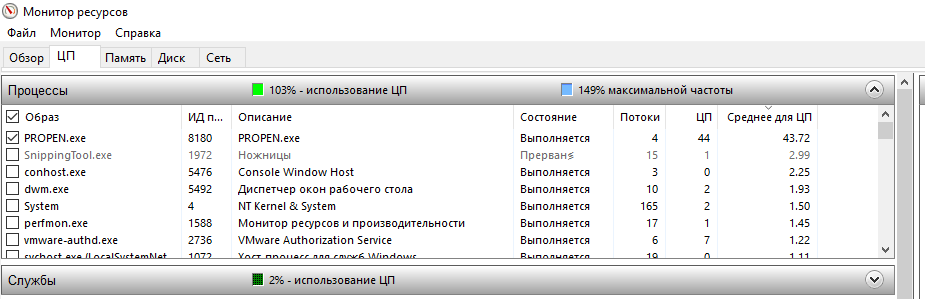


Рисунок 3.1 – Загрузка центрального процессора при распознавании отпечатка пальца

Необходимо заметить, что алгоритм распознавания отпечатков по особым точкам чувствителен к полноте отпечатка пальца. Поскольку в алгоритме происходит сравнение совпавших точек эталона и отсканированного отпечатка, частичные отпечатки или полученные под большим углом наклона, по отношению к плоскости сканера, не распознаются. Коэффициент соответствия из таблицы 3.1 получен для полных отпечатков.

3.2 Параметры реализации алгоритмов распознавания по лицу от несанкционированного доступа

В данной работе было реализовано два алгоритма распознавания по лицу: с использованием библиотек OpenCV и Face recognition. Для оценки основных параметров алгоритмов, проводились эксперименты следующим образом: изображение пользователя с видеопотока сравнивалось с эталонной фотографией, каждый алгоритм запускался в непрерывном режиме работы, в одном и том же помещении, при одном и том же освещении. При этом фиксировались основные параметры, представленные в таблице 3.2.

Таблица 3.2 - Сравнительные характеристики реализованных алгоритмов

|  |  |  |
| --- | --- | --- |
| Параметры | Библиотека  OpenCV | Библиотека  Face recognition |
| Максмальная вероятность распознавания, % | 71 | 86 |
| Время распознавания одного лица, сек | 0,15 | 1,65 |
| Загрузка центрального процессора,% | 52 | 26 |
| Объем памяти ОЗУ, Мбайт | 62 | 190 |

Вероятность распознавания показывает степень уверенности алгоритма распознавания в сравнении эталонного изображения лица и лица полученного с видеопотока. На величину вероятности распознавания влияют: разрешение видеокамеры, освещенность, положение лица перед камерой. Максимальное значение вероятности распознавания измерено на протяжении всего эксперимента. Данный параметр выше у алгоритма Face recognition, но не существенно.

Время распознавания лица у алгоритма OpenCV ниже, но при этом время распознавания алгоритма Face recognition пригодно для практического применения.

Параметры загрузки ЦП и объем памяти ОЗУ были получены с помощью монитора ресурсов операционной системы. Если учитывать, что предполагается периодическое распознавание во время работы пользователя, то загрузка процессора должна быть как можно меньше, чтобы не мешать работе других программ. Алгоритм Face recognition обеспечивает загрузку ЦП в 2 раза ниже и по этой причине имеет преимущество.

Объем занимаемой оперативной памяти для обоих алгоритмов небольшой в сравнении с полным объемом ОЗУ компьютера.

При проведении экспериментов распознавания по лицу были выявлены ряд особенностей.

Во время распознавания по лицу нейросеть на основе библиотеки OpenCV уверенно обнаруживает лицо человека на изображении только при фронтальном расположении. Даже небольшие повороты головы приводят к периодическому срыву обнаружения. Таким образом, для идентификации нужно смотреть строго в направлении камеры. В свою очередь, алгоритм на основе библиотеки Face recognition уверенно обнаруживает лицо человека, который работая за компьютером, периодически опускает взгляд на клавиатуру, при этом склоняет голову, и даже, когда закрывает глаза. Эти обстоятельства позволяют осуществлять периодический контроль присутствия человека за компьютером.

Кроме того, программа на основе библиотеки OpenCV иногда помимо лица выделяла рамкой фрагменты одежды, особенно если она имеет пятнистый окрас. Это значит, что нейросеть обнаруживает лица там, где их нет. При работе с библиотекой Face recognition случаев обнаружения лиц на посторонних предметах не было замечено.

Поскольку для системы защиты от несанкционированного доступа приоритетными являются надежность распознавания и загрузка ЦП, то для комплексной системы защиты выбран алгоритм идентификации на основе библиотеки Face recognition.

* 1. Влияние алгоритмов распознавания на работу штатных процессов ПК

Загрузка процессора при работе алгоритма по распознаванию отпечатков пальцев представляется достаточно большой (44%) в течение 4 сек. Однако, данный алгоритм запускается сразу после включения компьютера и до запуска пользователем других программ, поэтому он не влияет на их работу.

Загрузка процессора при непрерывной работе алгоритма распознаванию по лицу составляет менее 26% (рисунок 3.2).



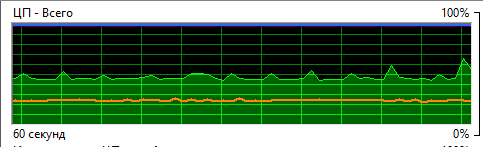


Рисунок 3.2 - Загрузка центрального процессора при непрерывной работе программы распознавания по лицу

На рисунке 3.2 зеленой линией отображается полная загрузка процессора, оранжевой линией - загрузка процессора программой по распознаванию лица при непрерывной работе. Средняя загрузка процессора при этом около 50% из них 26% используется программой по распознаванию лица.

Если осуществлять периодический контроль доступа пользователя (10 сек) в процессе его работы за компьютером, то средняя нагрузка процессора падает и составляет около 7% (рисунок 3.3).

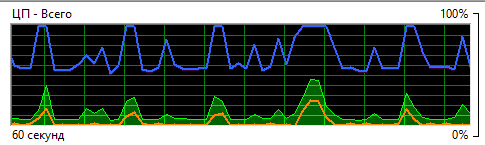


Рисунок 3.3- Загрузка центрального процессора при периодической работе (10 сек) программы распознавания по лицу

* 1. Оценка эффективности комплексной защиты двух биометрических систем

Эффективность защиты биометрических систем оценивают с помощью параметра FAR (вероятность ложного совпадения биометрических характеристик двух людей). Чем меньше этот параметр, тем меньше вероятность, что посторонний человек получит допуск к информации на ПК.

Комплексное значение FARком для двух биометрических систем рассчитывается по формуле:

FARком = FAR1\* FAR2, (12)

где FAR1- вероятность ложного совпадения биометрических характеристик двух людей для алгоритма распознавания по отпечаткам пальцев,

FAR2- вероятность ложного совпадения биометрических характеристик двух людей для алгоритма распознавания по лицу.

Для алгоритма распознавания по отпечаткам пальцев значение FAR=0,0066 (0,66%), п. 3.1.

В алгоритме распознавания по лицу на основе библиотеки Face recognition используется обученная нейронная сеть. Показатели FRR=0,1169 (11,69%), FAR=0,026 (2,6%) были получены в ходе тестирования сети разработчиком и опубликованы [36].

Расчет комплексного значения производится по формуле (12)

FARком =0,0066\*0,026=0,00017

При последовательной работе двух систем защиты степень защищенности возрастает, FARком=0,017%.

**4. Демонстрационная программа**

Для демонстрации разработанных алгоритмов была создана программа, которая является прототипом системы управления доступа к ПК. В этой программе в режиме реального времени демонстрируются:

* процесс распознавания личности по видеоизображению;
* процесс получения отпечатка пальца пользователя и его последующая идентификация.

На рисунке 4.1 отображен интерфейс программы в процессе распознавания личности пользователя по видеоизображению.

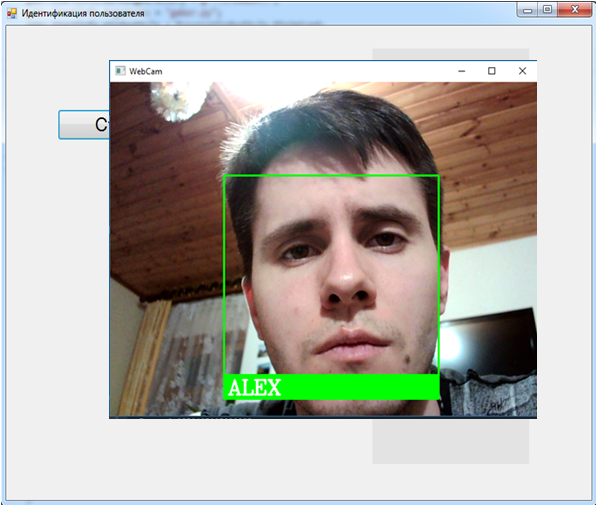


Рисунок 4.1 - Интерфейс программы для распознавания личности пользователя по видеоизображению.

После идентификации пользователя по видеоизображению, предлагается пройти идентификацию по отпечатку пальца (рисунок 4.2.).

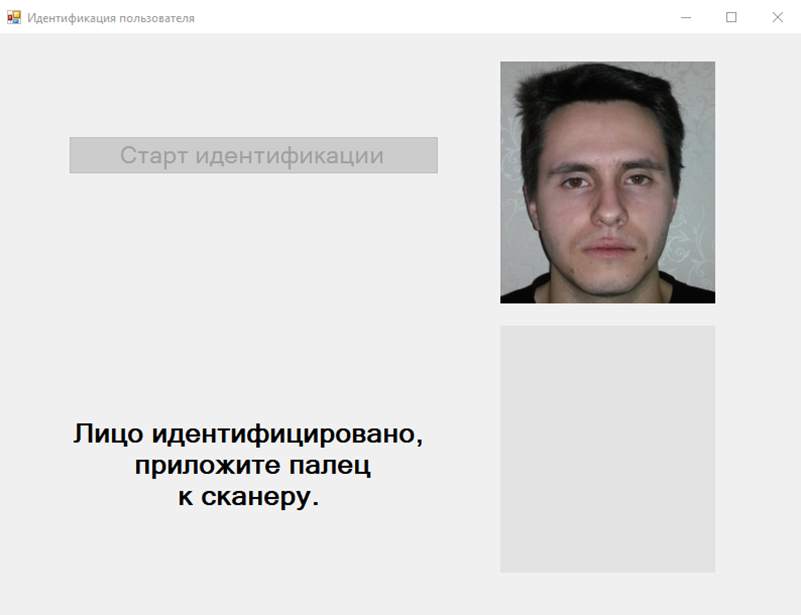


Рисунок 4.2 - Интерфейс программы для распознавания личности пользователя по отпечатку пальца.

Если идентификация по отпечатку прошла успешно, программа выводит соответствующее сообщение (рисунок 4.3). Если нет, предоставляется возможность повторно идентифицировать отпечаток пальца.

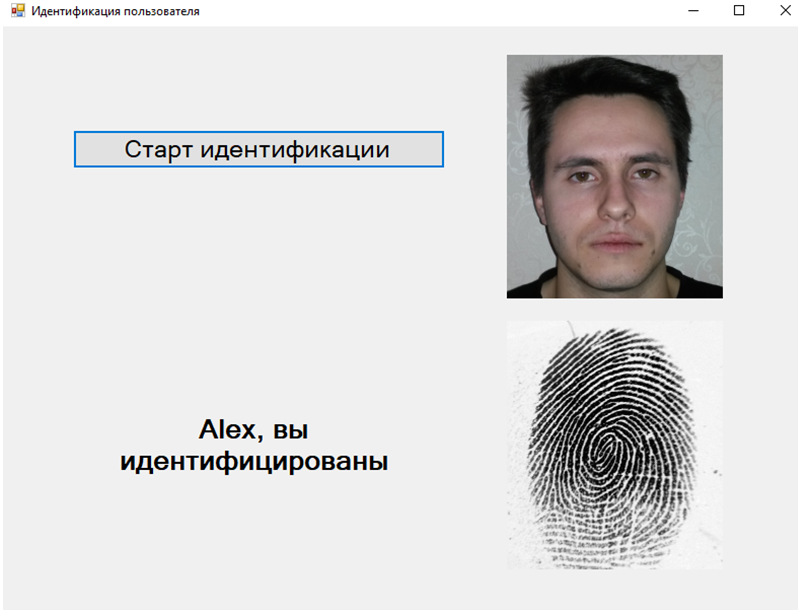


Рисунок 4.3 - Интерфейс программы с результатами идентификации личности

**Заключение**

В данной работе были исследованы биометрические системы защиты информации от несанкционированного доступа в несколько этапов:

1. Рассмотрены и проанализированы основные типы аппаратных средств для реализации биометрических систем защиты. Для исследования и практического применения была отобрана видеокамера Canyon CNS-CWC5 и сканер отпечатков пальцев ZK6500
2. Рассмотрены и проанализированы различные методы распознавания по лицу и отпечаткам пальцев. Для реализации программ по распознаванию личности были исследованы и отобраны лучшие, на текущий момент времени, методы, исходя из критериев качество и время распознавания. Приоритетным являлось качество распознавания.
3. Реализован алгоритм распознавания отпечатков пальцев по особым точкам на языке C++, с использованием бесплатных библиотек OpenCV и Fingerprint\_enhancer
4. Реализованы два алгоритма распознавания по лицу с использованием бесплатных библиотек OpenCV и Face recognition на языке Python.
5. Произведена оценка работы программного обеспечения. Анализ показал, что:

* распознавание осуществляется успешно с высокой степенью вероятности (до 84% для распознавания отпечатка пальца и до 86% для распознавания по лицу);
* время распознавания, реализованного программного обеспечения, позволяет применять его в режиме реального времени (до 4 сек для распознавания отпечатка пальца и до 1,65 сек для распознавания по лицу), например, для оперативного контроля доступа к персональному компьютеру;
* загрузка работы центрального процессора во время распознавания достаточно высокая (44% для распознавания отпечатка пальца и 26% для распознавания по лицу), но не критичная для большинства программ и процессов, работающих на ПК;
* при работе программ задействуется относительно небольшой объем оперативной памяти компьютера (20 Мбайт - распознавание по отпечатку пальца Мбайт – распознавание по лицу), что не существенно влияет на работу других программ;
* разработка самих программ реализовалась с помощью широко распространенных средств программирования и бесплатных библиотек.

1. Произведена оценка комплексной защиты двух биометрических систем. Анализ показал, что совместное применение двух биометрических систем усилило степень защищенности ПК от несанкционированного доступа (FARком=0,017%).
2. Для демонстрации комплексной работы двух биометрических систем защиты разработана программа на языке C#

В результате была разработана комплексная система защиты ПК от несанкционированного доступа. Контроль в системе осуществляется в два этапа:

* распознавание отпечатков пальцев;
* распознавание по лицу.

Основные параметры комплексной системы защиты представлены в таблице 1.

Таблица 1 - Основные параметры комплексной системы защиты

|  |  |  |
| --- | --- | --- |
| Параметры | 1 этап  Распознавание отпечатков пальцев | 2этап  Распознавание по лицу |
| Время распознавания одного лица, сек | 4 | 1,65 |
| Объем памяти ОЗУ, Мбайт | 20 | 190 |
| Загрузка центрального процессора, % | 44 | 26 |
| Загрузка центрального процессора (периодический режим работы 10 сек), % | ----- | 7 |
| Вероятность ложного обнаружения FAR, % | 0,66 | 2,6 |
| Вероятность ложного обнаружения FARком, % | 0,017 | |

Таким образом, было показано, что:

1. При наличии необходимых аппаратных средств, задействованные ресурсы алгоритмов распознавания позволяют реализовать идентификацию пользователя, не только для специализированных ПК, но и для компьютеров бытового назначения.
2. Разработанные аппаратно-программные средства могут быть применены для контроля доступа к ПК.
3. Применение комплексной работы биометрических систем защиты увеличивает степень защищенности ПК от несанкционированного доступа. Вероятность несанкционированного доступа к информации на ПК составляет сотые доли процента FARком=0,017%.

Поскольку разработки в этой области ведутся постоянно (могут измениться качественные характеристики аппаратных средств, возможно появление других методов идентификации и т.д.), то исследование биометрических систем защиты информации от несанкционированного доступа остается актуальной задачей.

**Список использованной литературы**

1. Биометрия по лицу: мировая история развития, сферы применения и способ оплаты. URL: <https://vc.ru/services/233794-biometriya-po-licu-mirovaya-istoriya-> razvitiya-sfery-primeneniya-i-sposob-oplaty (дата обращения: 01.05.2022).

2. Пентланд А.С., Чаудхари Т. Распознавание лиц для интеллектуальных сред // Открытые системы. – 2000. – №3. URL: <https://www.osp.ru/os/2000/03/177939> (дата обращения: 01.05.2022)

3. А.Г. Сабанов, С. Г. Смолина “Сравнительный анализ методов биометрической идентификации личности” Труды ИСА РАН. Том 66. 3/2016

4. Б. Яне “Цифровая обработка изображений”, Техносфера, Москва 2007г.;

5. Зуй Тхай Аспирант “Некоторые вопросы применения методов сравнения отпечатков пальцев для биометрических систем идентификации личности” Фам , кафедра МОСИТ, Московский государственный университет информационных технологий, радиотехники и электроники (МИРЭА);

6. Задорожный В., "Идентификация по отпечаткам пальцев", Часть 1, 2004;

1. [Задорожный В., "Идентификация по отпечаткам пальцев", Часть 2, 2007;](http://www.4delo.ru/inform/articles/419370.html)
2. [Давлетханов М., "Способы идентификации по отпечаткам пальцев", 2004;](http://infobez.com/article.asp?ob_no=2568)

9. В.Ю. Гудков, Д.А. Клюев “Скелетизация бинарных изображений и выделение особых точек для распознавания отпечатков пальцев” Южно-Уральский государственный университет, г. Челябинск 2015г.;

10. К. т. н. В. А. Болтенков, Д. В. Малявин, Нгуен Гуи Кионг “Сравнительный анализ алгоритмов скелетизации бинарных изображений” Одесский национальный политехнический университет Украина, г. Одесса 2014г.;

11. [Блог компании Droider.Ru](https://habr.com/ru/company/droider/blog/) “[Поисковые технологии](https://habr.com/ru/hub/search_technologies/),[Алгоритмы](https://habr.com/ru/hub/algorithms/),[Софт,](https://habr.com/ru/hub/soft/) [Фототехника”](https://habr.com/ru/hub/photo/). URL: <https://habr.com/ru/company/droider/blog/568764/?%29> (дата обращения: 01.05.2022)

12. Кузнецов Д.А., Никольский П.Г., Рачков Д.С., Кузнецов А.В., Хахамов А.П. Классификация методов обнаружения и распознавания лица на изображении // Научный результат. Информационные технологии. – Т.4, №1, 2019.

13. Jonathon Shlens A Tutorial on Principal Component Analysis Google Research April 7, 2014; Version 3.02 URL: <https://arxiv.org/pdf/1404.1100.pdf> (дата обращения: 01.05.2022).

14. Брилюк Д.В., Старовойтов В.В. Распознавание человека по изображению лица нейросетевыми методами. – Минск, 2002. – 54 с. (Препринт / Ин-т техн. кибернетики НАН Беларуси; №4.

15. Хемант Синг Миттал, Гарприт Каур Распознавание с использованием метода главных компонент и нейросети. – 2013. URL: <http://www.ijese.org/attachments/File/v1i6/F0266041613.pdf> (дата обращения: 01.05.2022).

16. H. B. Kekre , Sudeep D. Thepade , Akshay Maloo Performance Comparison for face Recognition using PCA,DCT&WallshTransform of Mean and Column Mean

URL: <https://www.researchgate.net/figure/FAR-FRR-Using-PCA-Figure-7-gives-the-percentage-of-FAR-and-FRR-for-face-recognition-using_fig5_228585933> (дата обращения: 01.05.2022).

17. Хайкин, С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1104 с.

18. Дорогой, Я.Ю. Архитектура обобщённых свёрточных нейронных сетей / Я.Ю. Дорогой // Вестник Национального технического университета Украины. - 2011. - № 49.

19. Татьяна Гайнцева. История развития сверточных нейронных сетей. Лекция (Видео). URL: <https://www.youtube.com/watch?v=Xq76hQHCkvQ> (дата обращения: 01.05.2022).

20. А. И. Бредихин Алгоритмы обучения сверточных нейронных сетей Вестник Югорского Государственного университета 2019 г. Выпуск 1 (52). С. 41–54

21. Федоренко, Ю.С. Технология распознавания образов с использованием свёрточной нейронной сети [Электронный ресурс] / Ю.С. Федоренко // Инженерный Вестник, ФГБОУ ВПО «МГТУ им. Н.Э. Баумана». - 2013. URL: <http://sntbul.bmstu.ru/file/out/641033> (дата обращения: 01.05.2022).

22. LeCun, Y. The MNIST database of handwritten digits URL:<http://yann.lecun.com/exdb/mnist/index.html> (дата обращения: 01.05.2022).

23. Солдатова, О. П. Применение свёрточной нейронной сети для распознавания рукописных цифр / О.П. Солдатова, А.А. Гаршин // Компьютерная оптика. – 2010 г.

24. Савченко А.В. Алгоритмы компьютерного зрения на основе

сверточных нейронных сетей. -2018г.

25. Стэнфордский курс: лекция 9. Архитектуры CNN <https://www.reg.ru/blog/stehnfordskij-kurs-lekciya-9-arhitektury-cnn/> (дата обращения: 01.05.2022).

26. Krizhevsky, A. ImageNet Classification with Deep Convolutional Neural Networks [Текст] / Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton // In NIPS, 2012.

27. Christian Szegedy Going Deeper with Convolutions [Текст] / Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, Andrew Rabinovich // In CVPR, 2015

28. Karen Simonyan, Very Deep Convolutional Networks for Large-Scale Image

Recognition [Текст] / Karen Simonyan, Andrew Zisserman, // In ICLR,2015

29. Kaiming He, Deep Residual Learning for Image Recognition / Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun [Текст] // In The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770-778

30. Jie Hu, Squeeze-and-Excitation Networks [Текст] / Jie Hu, Li Shen, Samuel Albanie, Gang Sun, Enhua Wu // In CVPR 2018

31. [«Алгоритмы, которые хотели как лучше»](https://www.youtube.com/watch?v=qdMp3ZwuwwA), Борислав Козловский Лекция (Видео) URL: <https://rb.ru/list/iskusstvennyj-intellekt/> (дата обращения: 01.05.2022).

32. Дубинин Н.М. Организация ЭВМ и систем Учебное пособие. — М. : МАИ, 2003. — 238 с.

33. [Вакуленко А., Юхин А., "Биометрические методы идентификации личности: обоснованный выбор и внедрение", 2007;](http://www.npo-inform.com/press/biovybor/)

34. [Зиятдинов А. И., "Принципы построения систем биометрической аутентификации"/ МФТИ, 2005, 8 с.](http://www.re.mipt.ru/infsec/2005/essay/2005_Construction_Principles_of_Biometric_Authentication_Systems__Ziyatdinov.htm)

35. Учебник по Python <URL:https://pymanual.github.io/>? (дата обращения: 01.05.2022).

36. [Harry Davis](https://quick-adviser.com/author/gxtraiurigl987utifffuf8t/) “How do you use face recognition on DLIB?” [31.12.2020](https://quick-adviser.com/how-do-you-use-face-recognition-on-dlib/) г. URL: <https://quick-adviser.com/how-do-you-use-face-recognition-on-dlib/> (дата обращения: 01.05.2022).