Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

На правах рукописи

Батенко Валерия Евгеньевна

Математические методы сравнения отпечатков пальцев для систем идентификации личности

Направление подготовки
01.04.02 «Прикладная математика и информатика»

АВТОРЕФЕРАТ
МАГИСТЕРСКОЙ ДИССЕРТАЦИИ

2019

Работа выполнена в ФГБОУ ВО
«Комсомольский-на-Амуре государственный университет»

Научный руководитель:	кандидат физико-математических наук, доцент, Козлова Ольга Викторовна
Рецензент:	И.О. заведующего кафедрой информационной безопасности, информационных систем и физики ФГБОУ ВО « Амурский гуманитарно-педагогический государственный университет» кандидат физико-математических наук Анисимов Антон Николаевич

Защита состоится 25 июня 2019 года в 9 часов 50 мин на заседании государственной экзаменационной комиссии по направлению подготовки 01.04.02 «Прикладная математика и информатика» в Комсомольском-на-Амуре государственном университете по адресу: 681013, г. Комсомольск-на-Амуре, пр. Ленина, 27, ауд. 312/3.

Автореферат разослан 17 июня 2019 г.

Секретарь ГЭК Ю.Г. Егорова

ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЕРТАЦИОННОЙ РАБОТЫ

Актуальность темы. Необходимость разграничения доступа к постоянно возрастающим объёмам информации в современном мире остро ставит проблему проверки подлинности пользователя. Рост компьютерных сетей и интенсивности их использования также упрощает задачу злоумышленника по получению несанкционированного доступа к данным или определённым сервисам, предоставляемым компьютерными системами.

Помимо обеспечения разграничения прав доступа к конфиденциальной информации современные автоматизированные комплексы решают ряд смежных задач. Двумя основными процедурами, выполняемыми подобными комплексами, являются идентификация и аутентификация субъекта доступа. В общем случае таким субъектом для компьютерной системы может являться не только человек, но и любой процесс, выполняемый удалено или локально.

В большинстве современных компьютерных систем проверка личности пользователя осуществляется с помощью ввода логина и пароля. В настоящее время существуют и другие методы, которые, хотя и не получили такого широкого распространения, потенциально являются намного более надёжными. В частности, существует целый класс перспективных биометрических подходов.

Целью данной работы является нахождение способа надёжной защиты от несанкционированного доступа к информации путём применения современных биометрических технологий.

Для достижения данной цели необходимо:

1. Проанализировать существующие подходы к идентификации и аутентификации личности.
2. Рассмотреть современные биометрические технологии, их сильные и слабые стороны.

3. На основе полученной информации разработать компьютерную программу, позволяющую идентифицировать личность по отпечатку пальца.

Публикации :

– Батенко, В. Е. Методы компьютерной идентификации личности / В. Е. Батенко, О. В. Козлова // Научно-техническое творчество аспирантов и студентов : материалы всерос. науч.-техн. конф. студентов и аспир., Комсомольск-на-Амуре, 9-20 апр. 2019 г. Комсомольск-на-Амуре : ФГБОУ ВО «КнАГУ», 2019. Ч. 2. – С. 237-249.

– Батенко, В. Е. Математические методы сравнения отпечатков пальцев для систем идентификации личности/ В. Е. Батенко, О. В. Козлова // Научно-техническое творчество аспирантов и студентов : материалы всерос. науч.-техн. конф. студентов и аспир., Комсомольск-на-Амуре, 9-20 апр. 2019 г. Комсомольск-на-Амуре : ФГБОУ ВО «КнАГУ», 2018. Ч. 2. – С. 257-259.

Структура и объем.

Магистерская диссертация состоит из введения, трёх глав, заключения и списка литературы. Объем работы 53 страниц, в том числе 10 рисунков, таблиц и приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение раскрывает актуальность темы, определяются цели и задачи исследования, объект, предмет, указываются научная новизна, практическая значимость, достоверность и обоснованность результатов исследования.

В первой главе рассказывается про современные биометрические методы идентификации.

В 95% случаев биометрия по своей сути — это математическая статистика. А математическая статистика это точная наука, алгоритмы из которой используются везде: и в радарах, и в байесовских системах. В качестве двух основных характеристик любой биометрической системы

можно принять ошибки первого и второго рода. В теории радиолокации их обычно называют «ложная тревога» или «пропуск цели», а в биометрии наиболее устоявшиеся понятия — FAR (False Acceptance Rate) и FRR (False Rejection Rate). Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей. Второе – вероятность отказа доступа человеку, имеющего допуск. Система тем лучше, чем меньше значение FRR при одинаковых значениях FAR. Иногда используется и сравнительная характеристика EER, определяющая точку, в которой графики FRR и FAR пересекаются. Но она далеко не всегда репрезентативна.

Можно отметить следующее: если в характеристиках системы не даны FAR и FRR по открытым биометрическим базам - то что бы производители не заявляли о её характеристиках, эта система скорее всего недееспособна или сильно слабее конкурентов. Но не только FAR и FRR определяют качество биометрической системы. Если бы это было только так, то лидирующей технологией было бы распознавание людей по ДНК, для которой FAR и FRR стремятся к нулю. Но ведь очевидно, что эта технология не применима на сегодняшнем этапе развития человечества!

Основными методами, использующими статические биометрические характеристики человека, являются идентификация по папиллярному рисунку на пальцах, радужной оболочке, геометрии лица, сетчатке глаза, рисунку вен руки, геометрии рук. Также существует семейство методов, использующих динамические характеристики: идентификация по голосу, динамике рукописного подчерка, сердечному ритму, походке. Ниже представлено распределение биометрического рынка пару лет назад. В каждом втором источнике эти данные колеблются на 15-20 процентов, так что это всего лишь оценочное представление. Так же тут под понятием «геометрия руки» скрываются два разных метода о которых будет рассказано ниже.

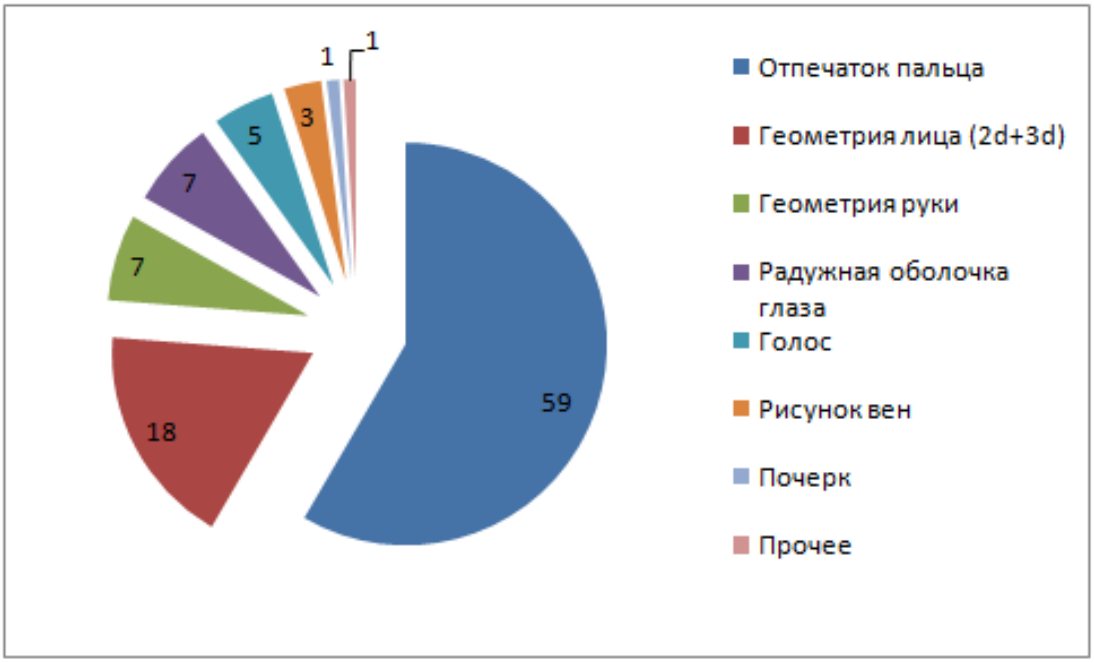


Рисунок 1 - Распределение биометрического рынка

В работе мы будем рассматривать только те характеристики, которые применимы в системах контроля и управления доступом (СКУД) или в близких им задачах. В силу своего превосходства это в первую очередь именно статические характеристики. Из динамических характеристик на сегодняшний момент только распознавание по голосу имеет хоть какую-то статистическую значимость (сравнимую с худшими статическими алгоритмами FAR~0.1%, FRR~6%), но лишь в идеальных условиях. Чтобы ощутить вероятности FAR и FRR, можно оценить, как часто будут возникать ложные совпадения, если установить систему идентификации на проходной организации с численностью персонала N человек. Вероятность ложного совпадения полученного сканером отпечатка пальца для базы данных из N отпечатков равна FAR·N. И каждый день через пункт контроля доступа проходит тоже порядка N человек. Тогда вероятность ошибки за рабочий день FAR·(N·N). Конечно, в зависимости от целей системы идентификации вероятность ошибки за единицу времени может сильно варьироваться, но если принять допустимым одну ошибку в течение рабочего дня, то:

$$FAR * N^2 \approx 1 => N \approx \sqrt{\frac{1}{FAR}}$$

Тогда получим, что стабильная работа системы идентификации при FAR=0.1% =0.001 возможна при численности персонала N≈30. Верификацией называется подтверждение личности человека через биометрический признак, где первичная аутентификация прошла по одному из первых двух методов, указанных выше. Простейшим верификатором можно назвать пограничника, производящего верификацию вашего лица с вашим паспортом.

Во второй главе говорится о методах идентификации отпечатка пальца. Это по одному или нескольким изображениям отпечатков пальцев со сканера формируется шаблон (карта), представляющий собой двухмерную поверхность, на которой выделены конечные точки и точки ветвления. Рассмотрим этапы сравнения двух отпечатков по локальным признакам:

- Улучшение качества исходного изображения отпечатка. Увеличивается резкость границ папиллярных линий;
- Вычисление поля ориентации папиллярных линий отпечатка. Изображение разбивается на квадратные блоки, со стороной больше 4 пикселей и по градиентам яркости вычисляется угол ориентации линий для фрагмента отпечатка;
- Бинаризация изображения отпечатка. Приведение к чёрно-белому изображению (1 bit) пороговой обработкой;
- Утончение линий изображения отпечатка. Утончение производится до тех пор, пока линии не будут шириной 1 пиксель;
- Извлечение деталей. Изображение разбивается на блоки 9x9 пикселей. После этого подсчитывается число чёрных (ненулевых) пикселей, находящихся вокруг центра. Пиксель в центре считается деталью, если он сам ненулевой, и соседних ненулевых пикселей: один (деталь - «окончание») или два (деталь - «раздвоение»).

При регистрации пользователей этот вектор считается эталоном и записывается в базу данных. При распознавании вектор определяет текущий отпечаток.

Сопоставление деталей. Два отпечатка одного пальца будут отличаться друг от друга поворотом, смещением, изменением масштаба и площадью соприкосновения в зависимости от того, как пользователь прикладывает палец к сканеру. Поэтому нельзя сказать, принадлежит ли отпечаток человеку или нет на основании простого их сравнения (векторы эталона и текущего отпечатка могут отличаться по длине, содержать несоответствующие детали и т.д.). Из-за этого процесс сопоставления должен быть реализован для каждой детали отдельно. Этапы сравнения:

- Регистрация данных. Определяются параметры аффинных преобразований (угол поворота, масштаб и сдвиг), при которых некоторая деталь из одного вектора соответствует некоторой детали из другого;
- Поиск пар соответствующих деталей. При поиске для каждой детали нужно перебрать до 30 значений поворота (от -15 градусов до +15), 500 значений сдвига (от -250 пикселей до +250 пикселей - хотя, конечно, границы выбирают и поменьше) и 10 значений масштаба (от 0,5 до 1,5 с шагом 0,1). Итого до 150 000 шагов для каждой из 70 возможных деталей. На практике, все возможные варианты не перебираются - после подбора нужных значений для одной детали их же пытаются подставить и к другим деталям, иначе было бы возможно сопоставить практически любые отпечатки друг другу;
- Оценка соответствия отпечатков. Оценка соответствия отпечатков выполняется по формуле K=(D*D*100%)/(p*q), где D - количество совпавших деталей, p - количество деталей эталона, q - количество деталей идентифицируемого отпечатка). В случае если результат превышает 65%, отпечатки считаются идентичными (порог может быть понижен выставлением другого уровня бдительности).

Пример сопоставления деталей между введенным и шаблонным изображениями отпечатков пальцев представлен на рисунке 10:

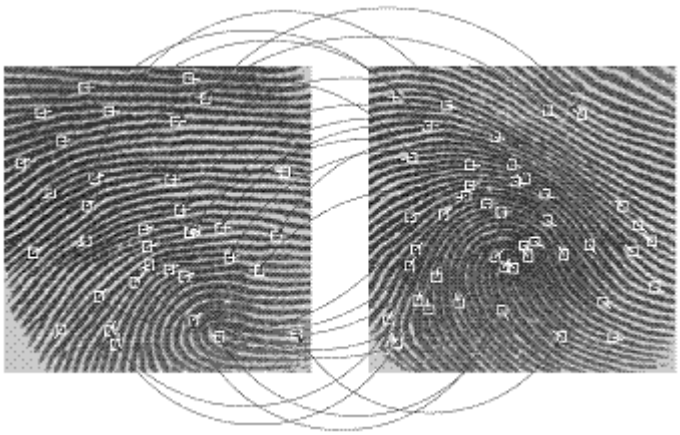


Рисунок 2 – Сопоставление деталей

Введем матрицу 3*3:

$$\begin{pmatrix} p9 & p2 & p3 \\ p8 & p1 & p4 \\ p7 & p6 & p5 \end{pmatrix}$$

Накладываем матрицу на изображение, совмещая интересующий нас пиксел с P1.

Каждая итерация состоит из 2-х подытераций:

Подытерация 1:

1) пиксел P1 удаляется из изображения , если выполняются следующие условия:

a) 2 <= B(P1) <= 6

b) A(P1)=1

c) P2*P4*P6=0

d) P4*P6*P8=0

где, A(P1)-число конфигураций 01 в последовательности P2,P3,P4,P5,P6,P7,P8,P9 , замыкая эту цепочку на P2 ,т.е. вокруг этого пиксела существует только один переход от 0 к 1.

Подытерация 2:

Выполняется аналогично, только

c) P2*P4*P8=0

d) P2*P6*P8=0

Таким образом:

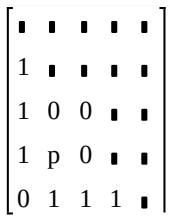
Подытерация 1. Удаление точек на юго-восточной границе и северо-западных угловых точек

Подытерация 2. Удаление точек на северо-западной границе и юго-восточных угловых точек

Такие алгоритмы называются **параллельными,** т.к. все изменения пикселов заносятся в отдельный массив, т.е. мы не заносим новое значение в массив, который обрабатываем в данный момент.

Эти итерации мы выполняем до тех пор, пока не будет удален ни один символ.

Но этими условиями мы не охватываем некоторых случаев.



Пиксел P, если он был единицей, этими условиями не удаляется. Поэтому проводится еще одна итерация, которая устраняет подобные недочеты.

На этой итерации ищутся два единичных пиксела по вертикали или горизонтали, которые окружены нулями.

Итак, точка P удаляется, если выполняется одно из условий:

1) !P9*P4*P6=1

2) !P5*P8*P2=1

3) !P3*P6*P8=1

4) !P7*P2*P4=1

где, !P9- отрицание P9

1. Запускаем цикл по всем точкам изображение. Отбираем только черные точки.

2. Если у черной точки ровно одна соседняя – черная, остальные – белые, то эта точка является минуцией.

3. Если у черной точки ровно три соседних – черные, остальные – белые, то эта точка является минуцией.

4. Завершаем цикл.

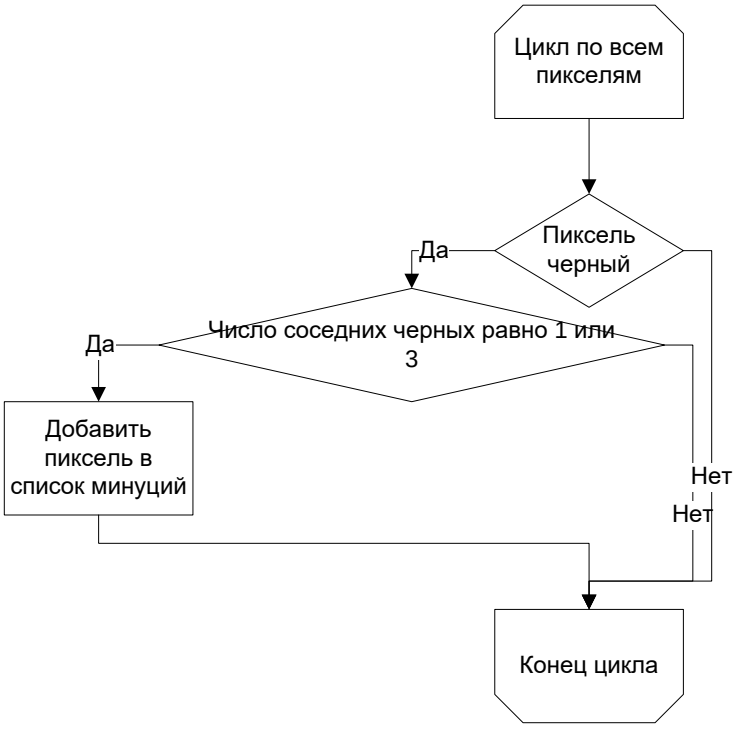


Рисунок 4 – Блок схема поиска минуций

В *заключении* подводятся основные итоги исследований, проводится анализ полученных результатов.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ИССЛЕДОВАНИЯ

– Батенко, В. Е. Методы компьютерной идентификации личности / В. Е. Батенко, О. В. Козлова // Научно-техническое творчество аспирантов и студентов : материалы всерос. науч.-техн. конф. студентов и аспир., Комсомольск-на-Амуре, 9-20 апр. 2019 г. Комсомольск-на-Амуре : ФГБОУ ВО «КнАГУ», 2019. Ч. 2. – С. 237-249.

– Батенко, В. Е. Математические методы сравнения отпечатков пальцев для систем идентификации личности/ В. Е. Батенко, О. В. Козлова // Научно-техническое творчество аспирантов и студентов : материалы всерос. науч.-техн. конф. студентов и аспир., Комсомольск-на-Амуре, 9-20 апр. 2019 г. Комсомольск-на-Амуре : ФГБОУ ВО «КнАГУ», 2018. Ч. 2. – С. 257-259.