



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении производственной (по получению профессиональных умений и опыта научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01ммзи
_____ Князев Д.А.
(подпись)

Отчет защищен с оценкой

(подпись) С.С. Зотов
(И.О. Фамилия)
« 31 » августа 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН

(подпись) С.С. Зотов
(И.О. Фамилия)

Регистрационный № _____
« 31 » августа 2021 г.

(подпись) Е.В. Третьяк
(И.О. Фамилия)

Практика пройдена в срок
с « 19 » августа 2021 г.
по « 31 » августа 2021 г.
на предприятии

Кафедра информационной
безопасности ШЕН ДВФУ

г. Владивосток
2021

Оглавление

| | |
|----------------------------------------------------------------------|----|
| Задание на практику | 3 |
| Исследование технологий биометрической идентификации | 4 |
| Сравнительный анализ основных методов биометрической идентификации.. | 5 |
| Геометрия руки | 5 |
| Отпечатки пальцев | 6 |
| Радужка..... | 6 |
| Лицо | 7 |
| Карта вен ладони | 7 |
| Заключение | 10 |
| Список используемых источников..... | 11 |

Задание на практику

- Исследование технологий биометрической идентификации.
- Проведение Сравнительного анализа основных методов биометрической идентификации.
- Написание научной статьи на вышеуказанную тему.

Исследование технологий биометрической идентификации

В последние годы развитие биометрических технологий достигло нового уровня, что привело к широкой популярности идентификации и верификации с использованием биометрик. Важнейшей характеристикой любой системы защиты является точность, то есть не допущение ложных допусков и отказов. При этом технологиям необходимо оставаться экономически доступными для потребителя, чтобы иметь успех на рынке. Технология распознавания отпечатков пальцев удовлетворяет обоим параметрам.

Биометрики в целом это крайне надежный и удобный способ идентификации. PIN-коды, токены могут быть забыты или похищены, пароли могут быть подобраны методом brute force, что является причиной растущих случаев нарушения конфиденциальности, целостности и доступности данных. Кроме того, затраты на поддержку баз данных с высоки и зачастую неоправданы, так как сброс потерянных или забытых паролей замедляет быстроедействие и снижает производительность системы.

Существуют две категории биометрической: физическая и поведенческая.

Технологии распознавания пользователя, основанные на физических биометриках, считывает уникальные особенности отдельных частей человеческого тела, такие как лицо человека, радужная оболочка, ДНК, отпечатки пальцев и т. д., обрабатывает полученную информацию и превращают эту её в код, понятный системой ИИ.

Технологии, работающие с поведенческими биометриками, функционируют аналогичным образом, за исключением того, что они проводят анализ уникальных поведенческих характеристик, такие как манера ввода текста с помощью клавиатуры, походка, голос и т. д.

Биометрия представляет собой набор метрик, связанных с физическими характеристиками человека. Биометрические данные – отличительные, измеряемые характеристики, используемые для идентификации людей. Они

делятся на две большие категории:

- физиологические характеристики связаны с формой тела. Это отпечатки пальцев, ладоней, голос, ДНК, радужка глаза и т.д.
- поведенческие характеристики относятся к модели поведения человека. Это ритм печати, походка, речь и т.п.

Несмотря на то, что биометрические параметры обеспечивают практически 100%-ную идентификацию, биометрическая аутентификация имеет ряд недостатков:

- биометрические параметры уникальны, но их нельзя сохранить в секрете; в случае их компрометации, их нельзя сменить, в отличие от паролей;
- некоторые биометрические параметры меняются со временем, из-за старения человека или полученных травм, а значит, база шаблонов требует постоянного сопровождения, что создает дополнительные неудобства;
- если злоумышленник получит доступ к базе шаблонов, то он сможет изменить ее, либо использовать в каких-то других целях;
- сами по себе системы распознавания по биометрическим параметрам имеют недостатки, например, устройства идентификации по ДНК могут быть использованы для выявления генетических заболеваний, причем без согласия человека.

Сравнительный анализ основных методов биометрической идентификации.

Геометрия руки

Распознавание на основе геометрии руки является одним из самых ранних, так как появилось на рынке еще в конце 1980х (рис.1).

Геометрия руки – это биометрическая характеристика, которая предполагает идентификацию человека по форме руки.

При создании шаблона, специальное устройство замеряет и запоминает длину, ширину и толщину различных частей руки, а камера делает снимок

руки, из которого получают изображение контура ладони. С помощью специально расположенного зеркала, камера снимает руку как сверху, так и сбоку .

Отпечатки пальцев

Отпечатки пальцев представляют собой карту неровностей кожи пальцев. Отпечатки пальцев детальные и уникальны, однако в качестве биометрической характеристики очень ненадежны, так как их легко подделать.

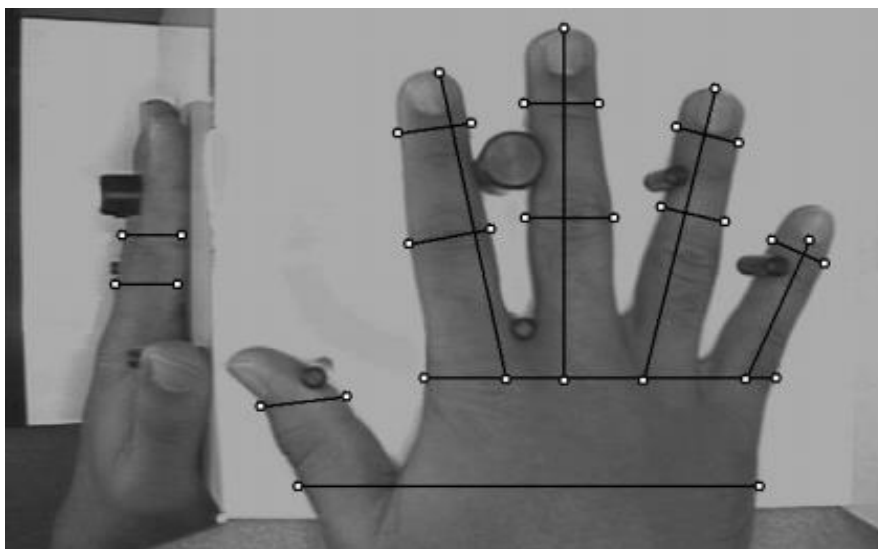


Рисунок 1 – Пример замеров для создания шаблона геометрии руки (вид из камеры)

Радужка

Процесс распознавания по радужке основан на анализе узора радужной оболочки глаза человека. Радужная оболочка – это цветная часть глаза, которая регулирует размер зрачка. Цвет и структура радужки связаны с генетикой, а детали узора – нет. Узор радужки уникален для каждого человека (рис.2).

Создание шаблона радужки требует использования высококачественной цифровой камеры. Современные коммерческие камеры, используемые для распознавания радужной оболочки, применяют инфракрасный свет.

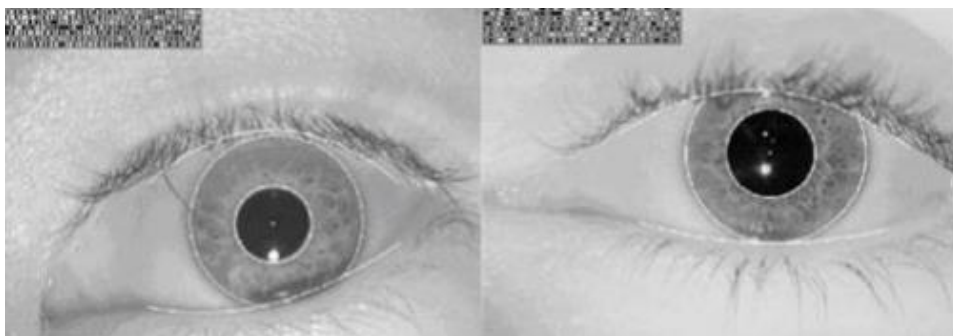


Рисунок 2 – Снимки глаз с обрисованными контурами радужки

Лицо

Распознавание лиц основывается на лицевых характеристиках индивида. Подходы к распознаванию лиц делятся на две группы:

- геометрические – базирующиеся на чертах лица;
- фотометрические – в основе которых лежит полный вид лица.

Карта вен ладони

Карта вен ладони представляет собой узор сети видимых кровеносных сосудов руки (рис.4). Камера получает изображение сети сосудов с помощью инфракрасного света, отраженного гемоглобином в крови.

Из представленной таблицы 1 видно, что карта вен ладони является оптимальной метрикой по большинству показателей.

Точность и безопасность биометрики являются основными показателями ее надежности.

Точность определяется FalseRejectionRate (FRR) –коэффициентом ошибочных отказов.

Безопасность определяется FalseAcceptanceRate(FAR) – коэффициентом ошибочных подтверждений. Из графика, представленного на рисунке 5, показывающего соотношение этих двух показателей, видно, что самым надежным биометрическим показателем является отпечаток ладони (карта вен, ладони).



Рисунок 4 – Схема получения шаблона карты вен ладони

Таблица 1 – Сравнение биометрических характеристик

| Биометрика | Цена | Лёгкость использования | FAR | FRR | Риск для безопасности |
|------------------|----------------------------|------------------------|----------|--------|-----------------------|
| Отпечаток пальца | От 3.400 до 1.5млн рублей | высокая | 0,001% | 0,6% | высокий |
| Радужка | От 37.000 до 5.5млн рублей | низкая | 0,00001% | 0,016% | низкий |
| Лицо | От 7.000 до 550.000 рублей | высокая | 0,1% | 2,5% | высокий |
| Карта вен ладони | От 9.600 до 150.000 рублей | средняя | 0,0008% | 0,01% | низкий |

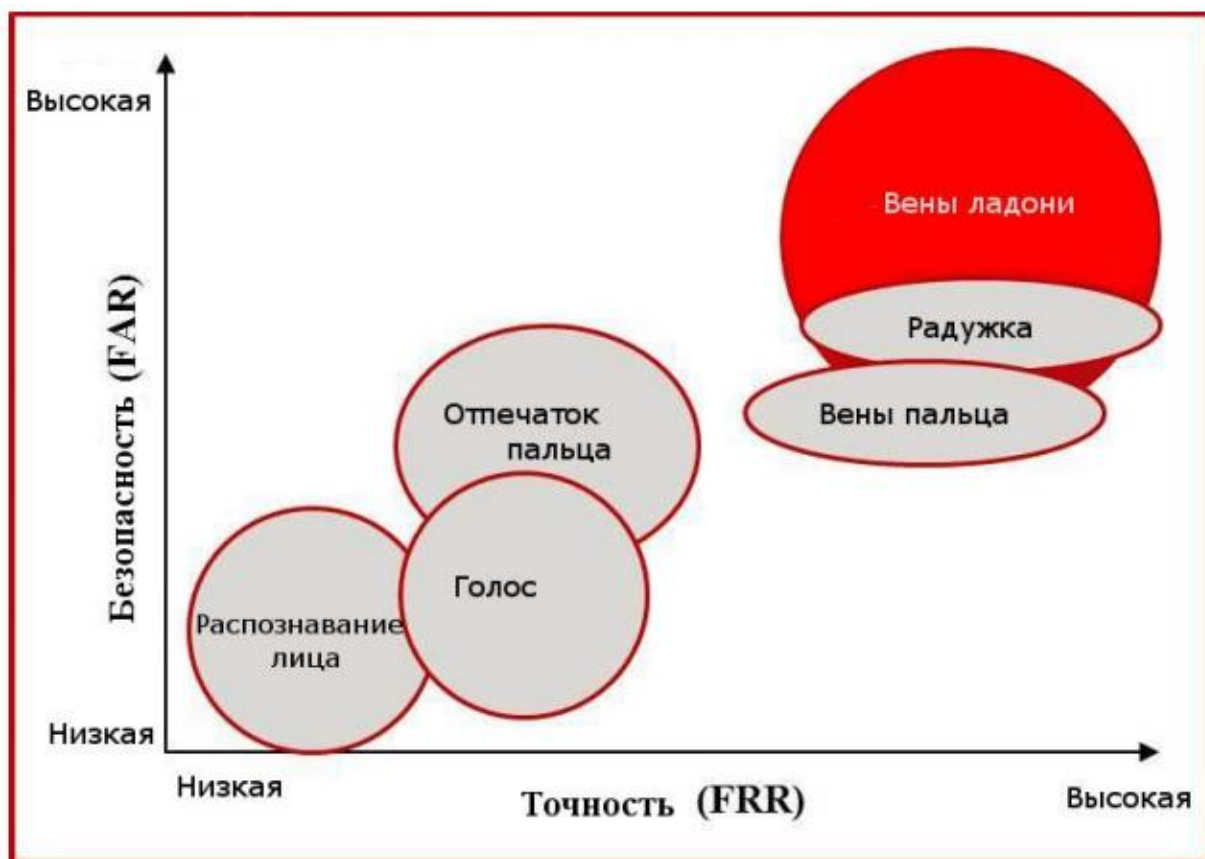


Рисунок 5 – Надежность биометрик

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики был проведен анализ биометрических характеристик, в результате которого был определен наиболее оптимальный параметр для проведения биометрической аутентификации.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1. Черноусова, Т. Г. Биометрия и аутентификация / Т. Г. Черноусова // Мир современной науки. – 2017. – № 3(43). – С. 20-24. Лукашов, И. В.
2. Состояние и перспективы биометрии / И. В. Лукашов // Мир измерений. – 2009. – № 3. – С. 27-32.
3. Антипова, Т. С. Биометрические технологии идентификации пользователя и их применение / Т. С. Антипова // Потенциал современной науки : Материалы Международной (заочной) научно-практической конференции, Прага, 30 ноября 2018 года / под общей редакцией А.И. Вострецова. – Прага: Научно-издательский центр "Мир науки" (ИП Вострецов Александр Ильич), 2018. – С. 13-15.
4. Системы контроля доступа. [Электронный ресурс]. Режим доступа: <https://securityrussia.com>