Санкт-Петербургский государственный университет
Математическое обеспечение и администрирование информационных систем
Системное программирование

Захаров Роман Вадимович

Выпускная квалификационная работа

Оптимизация эффекта биометрического зверинца в мультимодальных системах

Научный руководитель:

старший преподаватель кафедры системного программирования СПбГУ
Сартасов Станислав Юрьевич

Рецензент:

к.ф.-м.н. Мельников Александр Алексеевич

Санкт-Петербург

2017

SAINT-PETERSBURG STATE UNIVERSITY
Software and Administration of Information Systems
Software Engineering

Zakharov Roman Vadimovich

Biometric menagerie optimisation in multimodal systems

Graduation Project

Scientific supervisor:

Senior Lecturer Sartasov Stanislav Yurievich

Reviewer:

Ph.D. Melnikov Alexander Alexeevich

Saint-Petersburg

2017

Оглавление

Введение

Современные электронные устройства все чаще включают в себя биометрические системы, позволяющие обеспечить безопасный доступ к чтению данных и совершению операций. Биометрическая система предполагает наличие двух вещей: сенсора для считывания определенных физических данных человека и алгоритма, обрабатывающего эти данные. Одними из самых распространенных методов получения биометрических данных являются сбор отпечатков пальцев, сканирование сетчатки глаза и фотографирование лица.

Основными и важнейшими задачами биометрии являются верификация и идентификация. Провести верификацию означает выяснить у пользователя, какой персоной в системе он хочет представиться, собрать у него биометрические данные, сравнить их с имеющимися данными для заявленной персоны и сделать вывод о возможности доступа (например, к конфиденциальным данным) или отказе доступа. Идентификация от верификации отличается тем, что пользователь не указывает какой именно персоной в биометрической системе он является, система должна выяснить это самостоятельно.

Если алгоритм работы биометрической системы недостаточно хорошо зарекомендовал себя (слишком часто отказывает в доступе тем, кто на него имеет право, и/или слишком часто дает доступ к конфиденциальным данным тем, кто к ним не должен иметь доступа), то имеется возможность увеличить количество рассматриваемых в системе биометрических признаков, применив биометрическое слияние, то есть проанализировав несколько физических признаков человека. Биометрическая система, анализирующая только один набор физических данных (например, только отпечатки пальцев человека) называется унимодальной. Биометрическая система, анализирующая сразу несколько наборов, называется мультимодальной.

Следует отметить, что сбор дополнительных признаков у пользователя хотя и увеличивает безопасность системы, уменьшает удобство использования системы из-за необходимости большее время вводить физические признаки.

В данной работе реализован алгоритм, описанный в статье авторов А. Росса, А. Раттани и М. Тистарелли [1] (далее алгоритм РРТ, англ. *RRT – A. Ross, A. Rattani, M. Tistarelli*). Этот алгоритм является основой системы, являющейся компромиссным вариантом между унимодальной и мультимодальной системами. Компромисс достигается за счет использования единственной модальности, когда это не вызывает слишком плохой работы системы, и использования двух модальностей в противном случае. Классификация пользователей биометрической системы, основанная на оценке их поведения в ней, называется биометрическим “зверинцем”. Именно в том, как предсказать насколько часто пользователь системы будет сталкиваться с ошибками системы, и состоит проблема определения модальности, по которой будет происходить верификация пользователя в системе.

1. Постановка задачи

Целью данной работы является улучшение алгоритмов биометрического слияния с учетом эффекта биометрического зверинца. Для достижения цели нужно выполнить следующие задачи.

- Сделать обзор предметной области.
- Реализовать алгоритм проведения эксперимента PPT.
- Усовершенствовать алгоритм проведения эксперимента PPT.
- Провести сравнение полученного алгоритма с оригинальным.
- Создать демонстрационное приложение, иллюстрирующее работу полученного алгоритма.

2. Обзор
2.1. Общие понятия

Для работы алгоритма биометрической системы необходимо создать некоторую базу данных, которая содержит биометрические данные пользователей системы [2]. Во время работы алгоритм сравнивает свежесобранные данные с уже имеющимися, используя метрику (расстояние), означающую насколько сильно новые данные не похожи на собранные заранее. Чем меньше это расстояние, тем больше вероятность того, что пользователь системы действительно имеет право на чтение данных. В зависимости от алгоритма биометрической системы, выставляется пороговое значение (англ. *threshold*). Если расстояние ниже порога, либо равно ему – доступ будет предоставлен, если выше, то в доступе будет отказано. В одних биометрических системах используется такой подход, в некоторых других биометрических системах применяют метрику, имеющую противоположный смысл. Такая метрика отражает насколько данные похожи друг на друга.

При работе биометрической системы возможны ошибки двух типов: ложноположительные и ложноотрицательные результаты распознавания. Вероятности возникновения этих ошибок обозначаются как КЛД (Коэффициент Ложного Доступа) или FAR (англ. *False Acceptance Rate*), и как КЛОД (Коэффициент Ложного Отказа Доступа) или FRR (англ. *False Rejection Rate* — доступ запрещен зарегистрированному в системе человеку). Увеличение порога приводит к увеличению КЛД и одновременному уменьшению КЛОД, уменьшение порога приводит к уменьшению КЛД и увеличению КЛОД. Также увеличение порога увеличивает удобство для пользователя, но уменьшает безопасность биометрической системы. Если при конкретных настройках и общей базе данных у одной биометрической системы КЛД и КЛОД меньше, чем у второй, то первая и безопаснее, и удобнее второй.

2.2. Зверинец Доддингтона

Биометрический зверинец Доддингтона – название классификации для персон, известных биометрической системе. Схема зверинца Доддингтона изображена на рисунке 1. Классы зверинца отличаются друг от друга значениями КЛД и КЛОД. Деление всех классов зверинца происходит следующим образом: есть овцы (англ. *sheep*; основная популяция биометрической системы, для которой алгоритм работает лучше, чем для оставшейся части, имеют приемлимые КЛД и КЛОД), козлы (англ. *goats*; те, кто плохо распознается, у них высокий КЛОД), ягнята и волки (англ. *lambs* и *wolfs*; те, у кого высокий КЛД) [3]. Отличие последних в том, что именно волков распознают как ягнят в асимметричных алгоритмах, а не наоборот.

Такая классификация позволяет описывать слабые стороны биометрической системы.

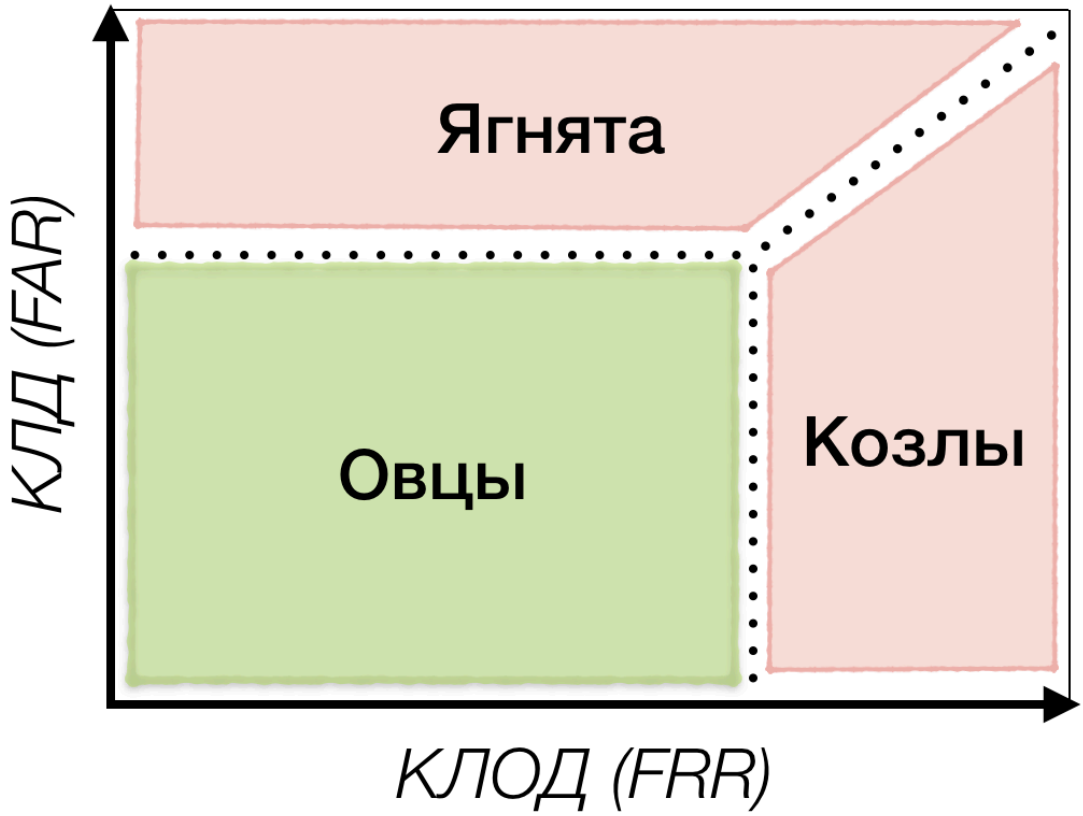

Рисунок 1. Схема зверинца Доддингтона

2.3. Эксперимент PPT

Имея мультимодальную биометрическую систему, есть возможность изменить её, приведя к компромиссному варианту между мультимодальной и унимодальной системами. Для этого необходимо провести некоторую классификацию пользователей для каждой модальности отдельно. Так поступили А. Росс, А. Раттани и М. Тистарелли, предложив новый алгоритм для создания биометрической системы [1]. В качестве классификации они использовали биометрический зверинец Доддингтона. Например, может оказаться, что для первой модальности один и тот же человек – “овца”, а по второй оказывается, что он “козёл”. Таким образом, применяя метод зверинца Доддингтона для двух типов биометрических данных мы получим 9 новых классов, описанных в таблице 1. Эта таблица сопоставляет классы двух модальностей действию, которое необходимо осуществить для нового класса.

Основная идея состоит в том, что бы для каждого нового класса использовать ту биометрическую характеристику, в которой он лучше себя показывает, или обе (используя биометрическое слияние) в худшем случае.

Мод. 1	Мод. 2	Действие
Козёл	Козёл	Использовать биометрическое слияние
Ягнёнок	Ягнёнок	Использовать биометрическое слияние
Овца	Овца	Использовать наилучшую из двух модальностей
Козёл	Ягнёнок	Использовать модальность 1 или слияние
Козёл	Овца	Использовать модальность 2
Овца	Ягнёнок	Использовать модальность 1
Овца	Козёл	Использовать модальность 1
Ягнёнок	Козёл	Использовать модальность 2 или слияние
Ягнёнок	Овца	Использовать модальность 2

Таблица 1: Схема алгоритма эксперимента PPT

2.4. Увеличение количества классов зверинца Доддингтона

Также есть возможность увеличить количество различных классов в биометрическом зверинце [4].

В схеме расширенного зверинца присутствуют дополнительные классы – хамелеоны, фантомы, голуби и черви. Таким образом, количество разных классов увечилось до восьми. Схема такого зверинца отображена на рисунке 2. Помимо количества классов зверинца есть еще одно отличие – классы отделяются друг от друга не с помощью подсчета КЛД и КЛОД для пользователей, а рассматриваются математические ожидания расстояния до подлинников (то есть среднее расстояние между образцами в базе данных для конкретного пользователя) и до злоумышленников (среднее расстояние между образцами пользователя до всех остальных пользователей). Например, голуби – пользователи, для которых биометрическая система работает лучше всего, так как они наименее отличаются от подлинников, и наиболее от злоумышленников. Худший класс – черви, так как они больше других отличаются от самих себя и меньше всех от злоумышленников.

Использование большего числа классов позволило сделать применение классической схемы зверинца более гибким и универсальным.

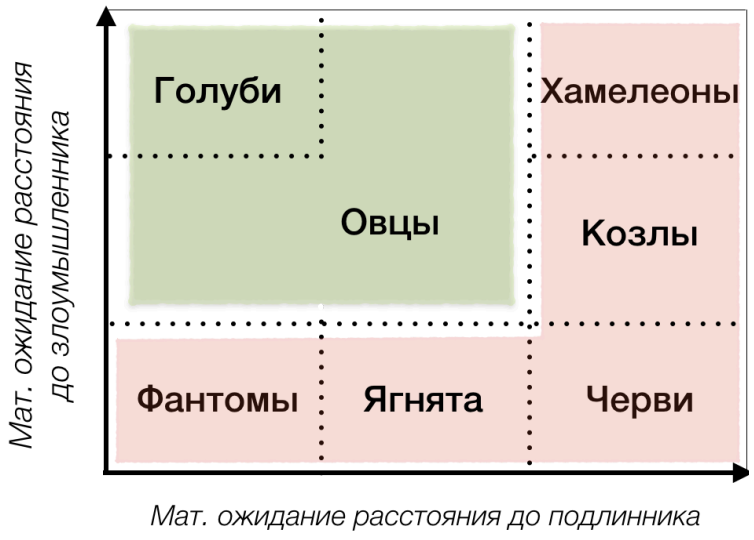

Рисунок 2. Схема расширенного зверинца

3. Реализация алгоритма PPT

Для реализации алгоритма PPT необходимо выполнить следующие шаги.

- Выбрать набор(ы) биометрических баз данных.
- Выбрать алгоритмы верификации для этих наборов и произвести настройку этих алгоритмов.
- На основе биометрических данных и алгоритмов создать две независимые модальности.
- Для каждой из модальностей построить “зверинцы Доддингтона”.
- Осуществить действия, согласно таблице 1.

В качестве набора данных был выбран сборник Put Face Database, созданный в Познаньском Технологическом Университете (Польша). Этот сборник содержит фотографии 100 человек. На каждого из них приходится по 22-е фронтальных фотографии. Эти фотографии были изменены так, чтобы оставить на них только изображения лиц. Для этого был использован инструмент FaceRect, доступный бесплатно [5]. В качестве основного алгоритма верификации был выбран алгоритм Fisherfaces [6] из распространенной библиотеки машинного зрения OpenCV. Этот алгоритм применяется дважды – для верхней половины лица человека и для нижней. Этот прием создает две различные модальности. Для того, чтобы построить “зверинцы Доддингтона”, набор из 22-ух фотографий для каждого человека был разделен следующим образом. Для обучения алгоритмов Fisherfaces были использованы 9 снимков, ещё 6 использовались для подсчета КЛД и КЛОД для каждого человека при верификации алгоритмами Fisherfaces для половин лица и, соответственно, определения классов зверинца. Оставшиеся семь использованы для подсчета КЛД и КЛОД после осуществления действий, описанных в таблице 1.

4. Усовершенствование алгоритма PPT и сравнение

В качестве усовершенствованного алгоритма PPT в данной работе был предложен алгоритм PPT с двумя изменениями.

Первое изменение предполагает вместо построения для каждой из модальностей “зверинца Доддингтона” строить другой зверинец, изображенный на рисунке 3. Этот зверинец включает 5 классов, разделенных четырьмя линиями прямой пропорциональности и различающихся друг от друга отношением математического ожидания различия до злоумышленника к математическому ожиданию различия до подлинника. Наилучший класс – муравьи, дальше следуют пчелы, затем раки, после олени, и, наконец, слоны – наихудший класс. Заметим, что данная классификация позволяет делать предположения о поведении системы для пользователей. То есть, если один пользователь был классифицирован как “рак”, а второй как “олень”, это может с определенной вероятностью означать, что первый пользователь будет сталкиваться с ошибками биометрической системы чаще, чем второй.

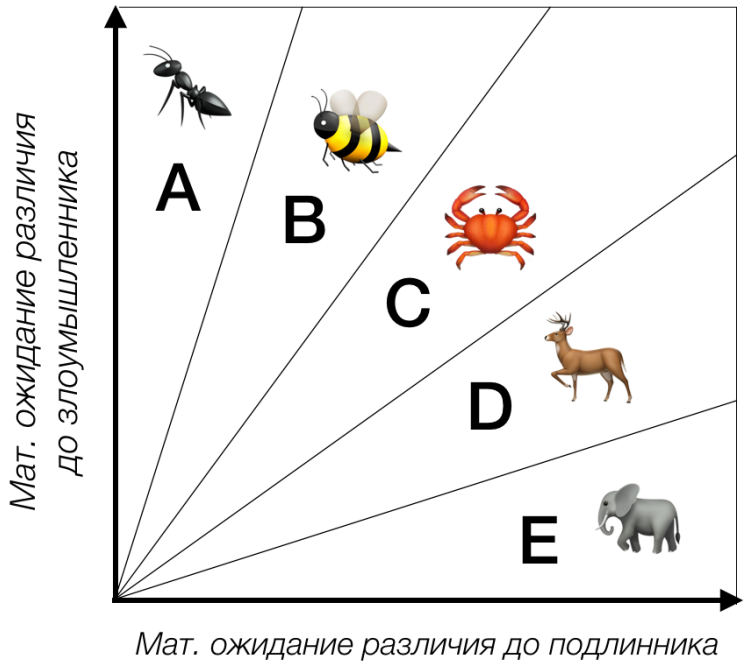

Рисунок 3. Схема предложенного зверинца
(A – муравьи, B – пчелы, C – раки, D – олени, E – слоны)

Второе изменение описывает новые действия, связанные с предложенными классами. Эти действия описаны в таблице 2.

Мод. 1	Мод. 2	Действие
Муравей	Муравей	Использовать наилучшую из двух модальностей
Пчела	Пчела	Использовать наилучшую из двух модальностей
Рак	Рак	Использовать наилучшую из двух модальностей
Муравей	Пчела/Рак/ Олень/Слон	Использовать модальность 1
Пчела/Рак/ Олень/Слон	Муравей	Использовать модальность 2
Пчела	Рак/Олень/ Слон	Использовать модальность 1
Рак/Олень/ Слон	Пчела	Использовать модальность 2
Рак	Олень/Слон	Использовать модальность 1
Олень/Слон	Рак	Использовать модальность 2
Олень	Олень	Использовать биометрическое слияние
Слон	Слон	Использовать биометрическое слияние
Олень	Слон	Использовать модальность 1
Слон	Олень	Использовать модальность 2

Таблица 2. Схема усовершенствованного алгоритма PPT

Общий принцип построения таблицы можно описать кратко. Если одна модальность лучше другой (в порядке от лучшей к худшей: муравей – пчела – рак – слон – олень), то использовать её; если по обеим модальностям человек одновременно олень или одновременно слон, то использовать биометрическое слияние; и использовать наилучшую из двух модальность в остальных трёх случаях.

Для сравнения различных биометрических систем используют кривые рабочих характеристик приемного устройства (РХПУ, англ. *ROC – Receiver Operating Characteristic*) [2]. Эти кривые иллюстрируют зависимость между КЛД и КЛОД. Таким образом, если на каком-то участке графика кривая РХПУ ниже другой кривой РХПУ, то соответствующая первой кривой биометрическая система лучше соответствующей второй кривой.

Для сравнения оригинального алгоритма PPT с полученным были построены кривые РХПУ соответствующих биометрических систем. Также кривые РХПУ были построены для систем, использующих только одну модальность и полное слияние. Результат построения изображен на рисунке 4 (рассмотрена содержательная часть графиков).

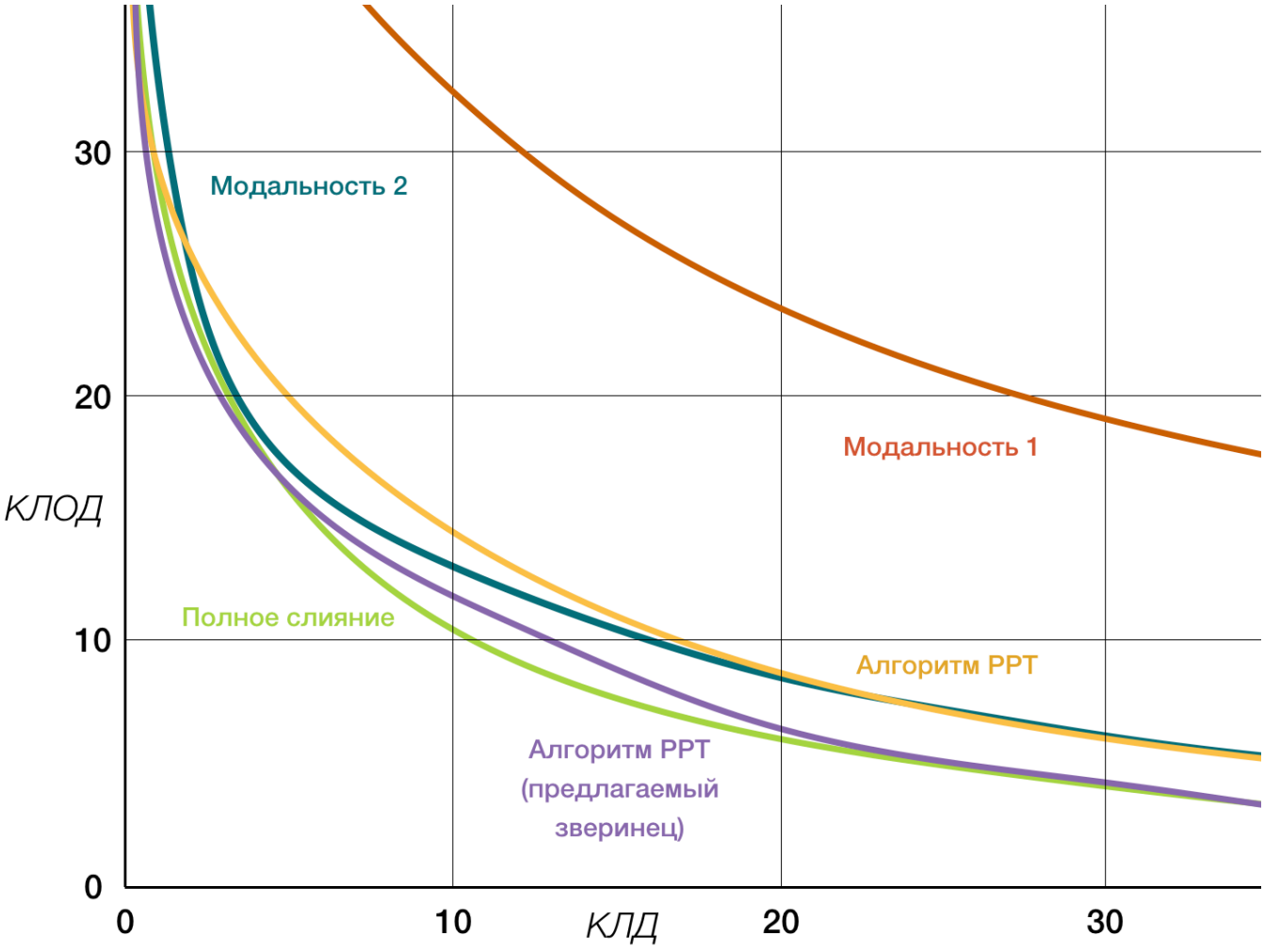

Рисунок 4. Кривые РХПУ (модальность 1 – алгоритм Fisherfaces для нижней половины лица, модальность 2 – для верхней половины лица)

Совершив анализ рисунка 4, можно сказать, что модальность 1 образует наихудшую систему верификации. Модальность 2 лучше неё, так как её кривая РХПУ располагается ближе к осям координат. Полное слияние, ожидаемо, лучше обеих модальностей. Кривая РХПУ для алгоритма PPT на части графика близка к кривой РХПУ модальности 2 на одной части графика, и немного ниже на других частях. Усовершенствованный алгоритм PPT, лучше обеих модальностей и местами его кривая РХПУ близка к кривой РХПУ для полного слияния, что и характеризует его как компромиссный вариант. Таким образом, можно утверждать, что в данной работе удалось усовершенствовать алгоритм PPT.

5. Создание демонстрационного приложения

В качестве языка программирования для создания приложения был выбран язык Python. Используемые технологии – VideoCapture из библиотеки машинного зрения OpenCV, инструмент FaceRect для определения на фотографии расположения лица человека.

Работа приложения состоит из следующих шагов.

• Пользователь с помощью веб-камеры компьютера делает серию снимков своего лица.

• Программа сохраняет снимки, изменяет их, оставляя на изображениях только лица (если таковых не смогла найти – удаляет) и разрезает снимки на верхние и нижние половины.

• Программа измеряет расстояния между снимками с помощью Fisherfaces, для обоих модальностей, подсчитывает среднее значение расстояний.

• Программа измеряет расстояния между снимками пользователя и снимками из набора данных PUT Face Database для обоих модальностей, подсчитывает среднее значение.

• Программа отображает на экране подсчитанные средние значения, их отношения, определяет классы из предложенного зверинца и отображает наилучшее для пользователя действие.

Пример результата программы изображен на рисунке 5.

```
Модальность                  | Мод. 1  | Мод. 2
Мат. ожид. до пользователя   | 951.12  | 999.57
Мат. ожид. до злоумышленника | 1332.26 | 1135.21
Отношение                    | 1.4     | 1.13
Класс                        | Олень   | Слон
─────────────────────────────────────────────────
Предлагаемое действие – использовать модальность 1
```

Рисунок 5. Результат работы программы

Заключение

В ходе данной выпускной квалификационной работы достигнуты следующие результаты:

- Сделан обзор предметной области.
- Реализован алгоритм проведения эксперимента PPT для мультимодальной системы распознавания лиц.
- Модифицирован алгоритм проведения эксперимента PPT путем замены общепринятой классификации на классификацию, созданную в рамках работы.
- Проведено сравнение полученного алгоритма с оригинальным алгоритмом, показавшее преимущество полученного.
- Создано демонстрационное приложение, иллюстрирующее работу полученного алгоритма (кроссплатформенное приложение на языке программирования Python).

Список литературы

[1] Ross A., Rattani A., Tistarelli M. Exploiting the ”Doddington zoo” effect in biometric fusion // 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems.— 2009.—Sept.— P. 1–7.

[2] Ruud M. Bolle Jonathan H. Connell Sharath Pankanti Nalini K. Ratha Andrew W. Senior. Guide to biometrics. — New York : Springer, 2004. — ISBN: 0387400893.

[3] George Doddington, Walter Liggett, Alvin Martin et al. SHEEP, GOATS, LAMBS and WOLVES A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation INTERNATIONAL CONFERENCE ON SPOKEN LANGUAGE PROCESSING. — 1998.

[4] Yager N., Dunstone T. Worms, Chameleons, Phantoms and Doves: New Additions to the Biometric Menagerie // 2007 IEEE Workshop on Automatic Identification Advanced Technologies. — 2007. — June. — P. 1–6.

[5] FaceRect– a powerful and completely free API for face detection.: FaceRect API Documentation. — URL: http://apicloud.me/apis/facerect/docs/. — 2012–2017.

[6] Belhumeur, P. N., Hespanha, J., and Kriegman, D. "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection.". IEEE Transactions on Pattern Analysis and Machine Intelligence 19. — 1997. — P. 711–720.