Гудонис Вадим Максимович
Gudonis Vadim Maximovich
Аншаков Никита Андреевич
Anshakov Nikita Andreevich
Студенты
Students
Астраханский государственный университет
Astrakhan State University

ОСОБЕННОСТИ СОЗДАНИЯ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ
PECULIARITIES OF FACE RECOGNITION SYSTEM CREATION

Аннотация на русском языке: Современные системы контроля доступа не лишены недостатков. Авторы предлагают создать систему, использующую распознавание лиц, для идентификации и аутентификации пользователя. Современный уровень развития вычислительных средств позволяет создать такую систему, и она будет достаточно эффективной. Для обеспечения заданной эффективности можно использовать метод гибкого сравнения на графах, метод главных компонент, скрытые Марковские модели. Также необходимо будет обеспечить уверенное отличие живого человека, от его фото- или видеосъемка. Для чего предлагается отслеживать моргание и пульс идентифицируемого объекта. Авторы предлагают проводить расчёты на GPU вместо CPU и использовать бинарные деревья поиска и кучу Фибоначчи. Это даст существенный выигрыш в производительности и сделает доступным удобное использование ресурсоемких алгоритмов. Также авторы классифицировали разрабатываемую систему и определили меры информационной безопасности.

The summary in English: Modern access control system has some drawbacks. The authors suggest creating a system that uses face recognition to identify and authenticate the user. The modern level of development of computing tools allows to create that system, and it will be quite effective. Elastic graph matching, principal component analysis, hidden Markov models can be used to provide required effectiveness. It will be also necessary to provide sure difference between an alive person and his camera or video images. Therefore, the authors proposed to monitor blinking and heartbeat of an identified object. The authors also advise to carry out the calculation on the GPU instead of the CPU and use binary search trees and Fibonacci heap. This will give a significant gain in productivity and make available to use easily resource-intensive algorithms. The authors also classified the developed system and defined means of information security.

Ключевые слова: контроль доступа, распознавание лиц, идентификация, аутентификация, биометрические данные, метод гибкого сравнения на графах, метод главных компонент, скрытые Марковские модели, персональные данные.

Keywords: access control, face recognition, identification, authentication, biometric data, elastic graph matching, principal component analysis, hidden Markov models, personal data.

Существует множество различных систем контроля доступа, применяемых в различных организациях: офисах, бюджетных учреждениях.

Все из них реализуют модель аутентификации на основе обладания чем-либо (обычно, персональной картой-пропуском). Однако такая модель несовершенна:

- карту можно банально потерять;
- хотя каждая карта зарегистрирована на определенного человека, воспользоваться ей может кто угодно, тем самым серьезно повлияв на безопасность предприятия;
- изготовление новых карты и их периодическая замена требуют специальной материальной инфраструктуры или обращения к сторонним компаниям.

Системы авторизации, созданные согласно модели аутентификации по биометрическим показателям лишены вышеописанных недостатков. Наиболее перспективой технологией распознавания биометрических показателей является технология распознавания лиц. Современный уровень развития процессоров позволяет выпроводить необходимый анализ изображений в течение нескольких секунд.

Существуют несколько алгоритмов анализа:

- метод гибкого сравнения на графах [1, 2];
- линейный дискриминантный анализ [2];
- скрытые марковские модели [3];
- метод главных компонент или principal component analysis (PCA) [4];
- active appearance models (AAM) и active shape models (ASM) [5];
- расчет и генерация зависимых хешей и их сравнение [2].

С использованием данных алгоритмов, их отдельных элементов и сочетаний можно создать гибкую и эффективную систему, которая будет содержать:

- автономный и автоматический анализ лиц людей, с принятием решений о допуске;

- возможность изменения пороговых значений для принятия автоматических решений о допуске или отказе;
- специальные алгоритмы определения живой человек перед камерой или его фотография (нивелируем основной недостаток таких систем);
- поддержку практически неограниченного количества пользователей без существенной потери производительности (благодаря использованию «Фибоначчиевой кучи»);
- защищенное хранение базы данных и защищенность каналов передачи, исключающих возможность несанкционированного доступа.

Как можно заметить были проигнорированы различные методы распознавания лиц с использованием нейронных сетей. Это было сделано не случайно. Поскольку, хоть нейронные сети и могут обеспечивать приемлемую для многих прикладных задач вероятность распознавания, но мы не можем построить алгоритм, в котором бы фигурировали четкие критерии. Всегда существует вероятность того, что при распознавании объекта в расчет берется не только его физиологические признаки, но и, к примеру, одежда, окружающий фон или уровень освещенности. В добавок вероятность этого скрыта от нас, ее невозможно высчитать математически. Все это приводит к тому, что в системах, для которых надежность и прогнозируемость результата критически важны, нейронные сети можно использовать только в качестве вспомогательного средства.

Переходя к структуре разрабатываемой информационной системы распознавания лиц, рассмотрим этапы его работы:

1) определение объекта перед камерой: живой человек или фотография;
2) получение изображения;
3) кадрирование изображения;
4) запуск алгоритмов распознавания (перцептивные хэши (пункты 4 – 5) и гибкого сравнения на графах (6));

5) перевод изображения в градации серого;

6) вычисление среднего значения для всех цветов;

7) бинаризация картинки;

8) создание перцептивного хэша;

9) создание графа лица;

10) высчитывание количества различий и анализ результатов.

Осветим некоторые пункты более подробно:

– Определение природы объекта перед камерой является важной задачей для системы распознавания лиц. Так как обычно такие системы используются для идентификации пользователя, нельзя допускать того, что бы системы реагировала на фото или видео людей, тем самым открывая возможность для ее обмана. Для решений этой задачи автор предлагает несколько подходов, основанных на признаках живых людей.

  - Определение, моргнул ли человек, для чего сравниваются несколько соседних кадров. Если человек моргнул, то это живой человек, а не фотография.
  - Определение изменения пульса человека. Для этого снимается видео, которое затем разбивается покадрово. Берутся два соседних кадра и сравниваются. Математически усиливаются различия между ними, например, по цвету. Если в этот момент не было сильных изменений, то кадры будут одинаковыми. Усиливая различия между кадрами, можно фиксировать изменение цвета кожи, возникающее из-за притока или оттока крови, а, следовательно, можно «увидеть» пульс человека. Никакая фото-видео съемка не сможет повторить результат живого человека.

- Получение изображения – определяется объект в кадре и происходит съемка 3х последовательных кадров, из которых выбирается лучший.
- Кадрирование изображения – использование цепного кода Фримена для построения контура (овала) лица и сохранения изображения только внутри этой области.
- Перевод изображения в градации серого – убирает зависимость от цветового диапазона и нормализует яркость. (рис. 1 Градации серого).
- Бинаризация картинки – оставляет только те пиксели, которые больше среднего (считаем их за 1, а все остальные за 0).
- Создание перцептивного хэша – перевод 64 отдельных битов в одно 64-битное значение. Порядок не имеет значения, если он сохраняется постоянным.
- Создание графа лица – лица представляются в виде графов со взвешенными вершинами и ребрами. На этапе распознавания один из графов (эталонный) остается неизменным, в то время как другой деформируется с целью наилучшей подгонки к первому (рис. 2 Граф лица).
- Высчитывание количества различий – на основе 2х хэшей сравниваем изображения, подсчитывая количество разных битов по алгоритму расстояния Хэмминга. Нулевое расстояние означает, что это, скорее всего, одинаковые картинки, а другие величины характеризуют, насколько сильно они отличаются друг от друга. Если это расстояние меньше порогового, то идентификация успешна.

Рисунок 1. Градации серого

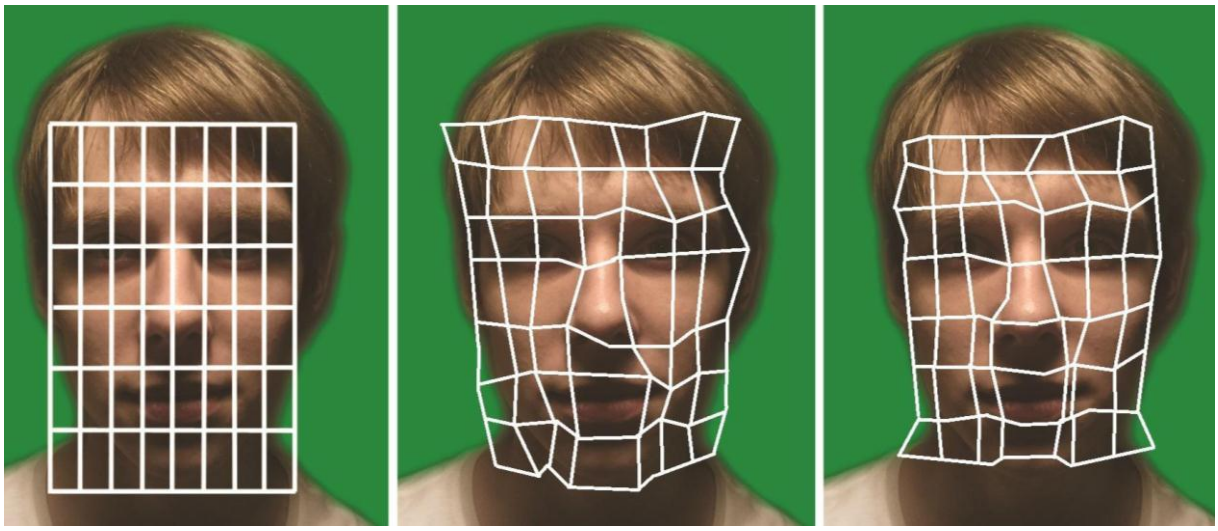

Рисунок 2 Граф лица

Для ускорения вычислений лучше проводить расчет на GPU вместо CPU. Вместе с использованием бинарных деревьев поиска или Фибоначчиевой кучи это обеспечивает существенный прирост

производительности без использования многокластерных систем, поскольку скорость математических операций на GPU существенно выше. Это в свою очередь позволяет использовать ранее недоступный метод гибкого сравнения на графах, который требует больших вычислительных мощностей.

Также заметим, что биометрические данные человека относятся к персональным [6]. Информационная система обрабатывающая такие данные является информационной системой персональных данных. В соответствии с действующим законодательством такая информационная система должна быть защищена согласно требованиями, утвержденным Постановлением Правительства РФ от 01.11.2012 № 1119 [7].

Для того чтобы узнать конкретный перечень обязательных (в зависимости от конкретных параметров системы) для реализации мер защиты, рассмотрим классификацию данной информационной системы. Для этого определим категорию обрабатываемых персональных данных, количество субъектов, данные которых будут обрабатываться и тип угроз информационной системы. Категорию персональных данных определим, как биометрические персональные данные. Рассматриваемый тип угроз – третий. К нему относятся угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе. Таким образом согласно Постановлению Правительства РФ от 01.11.2012 № 1119 для рассматриваемой информационной системы будет необходимо обеспечить 3-й уровень защищенности персональных данных, в независимости от того, обрабатываются персональные данные меньше или больше чем 100 000 субъектов и являются ли эти субъекты сотрудниками оператора или нет.

Необходимые меры и средства защиты информационных систем персональных данных в зависимости требуемого уровня защищенности

задает Приказ ФСТЭК от 18.02.2013 г. № 21 [8]. В соответствии с ним информационная система персональных данных 3-го уровня защищённости должна включать в себя перечень мер и механизмов защиты, содержащий 41 наименование. Все необходимые меры и средства защиты перечислены в Приложении к данному Приказу.

Выполнив вышеобозначенные условия получаем информационную систему аутентификации по биометрическим признакам, удовлетворяющую требованиям российского законодательства и пригодную для практического использования в решении задач по контролю и управлению доступом.

Литература:

1. Самаль Д.И., Старовойтов В.В. Подходы и методы распознавания людей по фотопортретам. — Минск, ИТК НАНБ, 1998. — 54с.

2. Самаль Д.И., Старовойтов В.В. Методика автоматизированного распознавания людей по фотопортретам // Цифровая обработка изображений. — Минск: ИТК, 1999.-С.81-85.

3. Gernot A. Fink. Markov Models for Pattern Recognition: From Theory to Applications. — ISBN-13: 978-3540717669.

4. Gorban, A.N., Kégl, B., Wunsch, D.C., Zinovyev, A. Principal Manifolds for Data Visualization and Dimension Reduction. — ISBN: 978-3-540-73750-6

5. T. Cootes, G. Edwards, and C. Taylor. Active appearance models. In Proceedings of the European Conference on Computer Vision.

6. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

7. Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных» от 1 ноября 2012 г. №1119.

8. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».