

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ (РИНХ)

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Материалы V Всероссийской научной конференции

19–20 мая 2016 года

**Ростов-на-Дону
2016**

УДК 378+004.056

ББК 65.050.2

П 78

Проблемы информационной безопасности: Материалы V Всероссийской конференции 19–20 мая 2016 г. – Ростов н/Д: Издательско-полиграфический комплекс РГЭУ (РИНХ), 2016. – 209 с.

ISBN 978-5-7972-2222-4

В издании представлены работы профессорско-преподавательского состава, молодых ученых, магистров и студентов, посвященные проблемам информационной безопасности.

Материалы конференции предназначены для научных сотрудников, преподавателей, аспирантов, магистров и студентов.

Редакционная коллегия:

Е.Н. Тищенко (ответственный редактор),
Т.В. Богачев, Н.Е. Шейдаков, А.В. Скляров

*Утверждены в качестве материалов конференции
Редакционно-издательским советом РГЭУ (РИНХ).*

ISBN 978-5-7972-2222-4

© РГЭУ (РИНХ), 2016

СОДЕРЖАНИЕ

СЕКЦИЯ 1. ФУНДАМЕНТАЛЬНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 7

Ажмухамедов И. М., Князева О. М.

Применение нечеткого когнитивного моделирования
для решения задачи оценки качества информационных систем 7

Виржанский А. С., Ромашкин Д. О., Козубенко М. В.

Авторизация как обеспечение защиты от НСД 12

Выборнова О. Н., Кравченко К. Л.

Нечеткая когнитивная модель оценки рисков информационной
безопасности для ПАО «МРСК ЮГА» – «АСТРАХАНЬЭНЕРГО» 17

Ганжа А. Е., Жилина Е. В., Васюта С. Д.

Применение нейронных сетей в системах обнаружения атак..... 21

Гудонис В. М., Аншаков Н. А.

Использование системы распознавания лиц для контроля доступа..... 26

Завадская Е. Д., Антонова Е. К.

Использование методов социальной инженерии
для несанкционированного доступа к конфиденциальной
информации 31

Карпов А. С.

Марковские модели в системах биометрической идентификации..... 35

Катков Е. К.

Модификация навигационной аппаратуры для работы
в условиях ионосферных возмущений..... 40

Краснощёрова А. А., Ажмухамедов А. И., Кипарисова А. И.

Информационное воздействие на социальную подсистему
организации с целью повышения уровня информационной
безопасности 46

Македонский С. А.

Критическое осмысление анализа рисков информационной
безопасности 51

Маршаков Д. В.

Особенности представления знаний в интеллектуальных системах
защиты информации 56

Синицын Д. Р.

Нейронные сети в системах распознавания речи 60

2. Аналитические технологии [Электронный ресурс]. – Режим доступа: <http://www.neuroproject.ru/neuro.php>.

3. Обучение нейронных сетей [Электронный ресурс]. – Режим доступа: <http://www.neuropro.ru/neu1.shtml>.

Гудонис В. М., Анишаков Н. А.

Использование системы распознавания лиц для контроля доступа

В настоящее время широко распространены системы контроля доступа. Примерами могут послужить системы турникетов в учебных заведениях, на производствах, в метро. Для авторизации в каждой такой системе требуется уникальная карта – это не очень удобно и тянет за собой несколько проблем:

- карту можно банально потерять;
- хотя каждая карта зарегистрирована на определенного человека, воспользоваться ей может кто угодно, тем самым серьезно повлияв на безопасность предприятия;
- карты не долговечны и периодически их нужно менять, а это дорого.

Решить эти проблемы можно заменив «простые» системы доступа с применением карт, на систему с использованием распознавания лиц. Технически это возможно благодаря тому, что современные процессоры достигли такого уровня производительности, что скорость обработки изображений занимает несколько секунд, а после анализа мы получаем необходимые данные. 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 предлагаемого программного обеспечения, 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 2 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 3-х 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).

- Вычитывание количества различий – на основе 2-х хэшей (или графов) 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

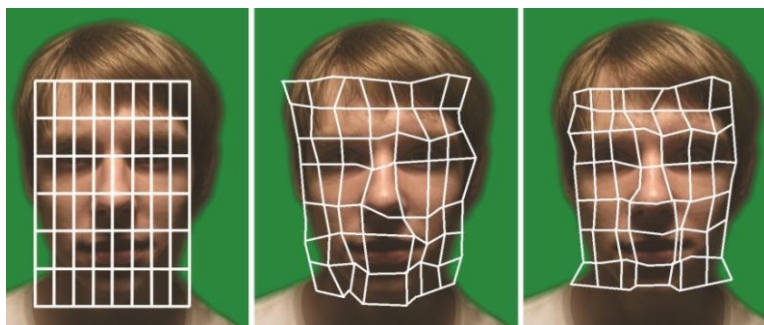


Рисунок 2 – Граф лица

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.

Библиографический список

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

Завадская Е. Д., Антонова Е. К.

Использование методов социальной инженерии для несанкционированного доступа к конфиденциальной информации

Информационные системы в настоящее время являются одними из главных источников ценной информации. Поэтому они подвергаются постоянным атакам со стороны нарушителей с целью получения этой информации. Самыми широко известными способами получения несанкционированного доступа к информации, хранящейся в ИС, являются технические методы, под которыми понимается использование специальных технических средств для съема информации по различным каналам: акустическим, вибро-акустическим, электромагнитным, оптическим и т.д. Но существуют и другие очень важные методы, требующие особого внимания – методы социальной инженерии. Под ними понимается воздействие на человека без использования технических средств. Многие недооценивают ущерб, который может нанести злоумышленник, посредством использования методов социальной инженерии, но по последним данным исследования компании Info Watch в 2015 году в 58% случаев виновными в утечке информации оказались сотрудники компаний, в 1% случаев – высшие руководители организаций [2]. Это доказывает, что люди, работающие в компании, являются одним из самых главных источников утечки информации, который часто забывают учитывать в построении системы безопасности предприятия.