АНАЛИЗ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ ПО АЛГОРИТМУ НЕЙРОННОЙ СЕТИ

В.Н. Максименко, *доцент кафедры «Информационная безопасность» МТУСИ, к.т.н. vladmaks @yandex.ru;*
Т.С. Волошина, *магистрант МТУСИ, tania083@mail.ru*

УДК 621.391

Аннотация. Среди основных тенденций в области информационной безопасности выделяется тенденция построения единой комплексной системы безопасности, объединяющей разрозненные системы и службы безопасности. Создание единой централизованной системы безопасности является необходимым условием существования современных инфраструктур. Успехи в области спутниковых навигационных систем заложили хорошие перспективы для определения местоположения злоумышленника, совершившего кражу мобильного терминала сотовой подвижной связи. Комплексное использование спутниковой навигационной системы и системы видеонаблюдения значительно повышают точность идентификации личности злоумышленника. Метод идентификации человека по форме лица позволяет строить трехмерный образ лица и конфигурировать множество вариантов на случай поворота или наклона головы, изменения выражения лица, но требует высокой производительности вычислительных средств и большого объема памяти. В данной статье приведены результаты анализа системы распознавания лица по алгоритму нейронной сети. Использование параллельных вычислений на основе технологии нейронных сетей призвано сократить время распознавания лиц в реальном времени больших потоков людей.

Ключевые слова: нейронная сеть; информационная безопасность; доступность; целостность; конфиденциальность; информационная инфраструктура.

ANALYSIS OF THE PERSON RECOGNITION SYSTEM BY THE NEURAL NETWORK ALGORITHM

Vladimir Maksimenko, *associate professor of the «Information security» MTUCI, candidate of technical sciences;*
Tatyana Voloshina, *graduate student MTUCI.*

Annotation. Among the main trends in the field of information security there is a tendency to build a unified integrated security system uniting disparate systems and security services. Creating a unified, centralized security system is a prerequisite for the existence of the modern infrastructures. Successes in the field of satellite navigation systems laid good prospects for determining the location of the attacker who committed the theft of the mobile terminal of cellular mobile communications. The integrated use of satellite navigation systems and video surveillance systems significantly increase the accuracy of identification of the attacker. The method of identifying a person by the shape of a face allows you to build a three-dimensional image of the face and configure many options in case of turning or tilting the head, changing facial expressions, but it requires high performance computing tools and a large amount of memory. This article presents the results of the analysis of the facial recognition system using the neural network algorithm. The use of parallel computing based on neural networks technology is designed to reduce the time of face recognition in real time of large flows of people.

***Keywords*:** neural network; information security; availability; integrity; confidentiality; information infrastructure.

Операторы сотовой подвижной связи (СПС), помимо стандартных услуг голосовой связи, используя технологические возможности сетевых средств обработки, хранения и передачи информации, оказывают информационно-телекоммуникационные и гео-информационно-телекоммуникационные услуги, для информационной безопасности которых требуется реализация механизмов идентификации абонента и мобильного терминала [1, 2]. Абонент СПС с использованием мобильного терминала вовлекается в финансовые, банковские или социальные взаимодействия с другими субъектами информационных взаимодействий. Но в случае утраты мобильного терминала случайным или преднамеренным воздействием абонент теряет возможность получить информационные или финансовые услуги, что может нанести неприемлемый ущерб. В ряде случаев необходимо внедрение новых механизмов обеспечения ИБ, работающих со стандартными алгоритмами идентификации и шифрования, реализованных в сетях СПС [3, 4]. Однако, как показано в [5], чтобы обеспечить максимальную конфиденциальность информации, передаваемой по каналам связи, необходимо реализовать дополнительные средства защиты информации (ЗИ), такие как ввод числового кода, идентификатора мобильного терминала, использованием биометрических данных об абоненте. Попытки применить биометрические параметры для идентификации абонента сдерживались недостаточной вычислительной мощностью и отсутствием эффективных параллельных алгоритмов [5]. Сочетание возможности определения местоположения мобильного терминала и системы видеонаблюдения позволяет решить задачу расследования инцидента, связанного с утерей или кражей мобильного терминала [6]. На данный момент большое значение уделяется безопасности в местах большого скопления людей: на вокзалах, стадионах, в аэропортах, метро и т.д. Наиболее удобным в этих случаях является использование распознавание лиц по той причине, что распознаваемым нет необходимости задерживаться ради идентификации, а это играет важную роль в местах с большим потоком людей.

Для распознания лиц требуется плотность пикселей не менее 500 пикс/м во всей предполагаемой зоне распознавания, также желательно, чтобы камера позволяла задавать пределы открытия и закрытия диафрагмы объектива. Для четкости получаемого кадра время накопления заряда (выдержки) должно быть не менее 1/100 секунды.

Кроме этого, важно выполнение изложенных в стандарте ISO/IEC 19794-5:2013 или в ГОСТ Р ИСО/МЭК 19794-5-2013 требований к изображению, заносимому в базу данных. Выполнение этих и некоторых других условий, сведенных в табл. 1, позволит получить подходящий ракурс лица для распознавания [7].

Таблица 1

Параметр	**Требование**
Плотность пикселей	Не менее 500 пикс/м
Углы отклонения	Не более 15º по вертикали и горизонтали
Диафрагма отклонения	Регулируемая, с возможностью ручного управления
Размер матрицы	Не менее 1/3”
Выдержка	Не более 1/100
Освещенность	Не менее 150 лк; освещение лица должно быть равномерным
Требования к фото	Размер – не менее 320x240; однотонный задний фон; расстояние между зрачками не менее 60 пикс

Также для системы распознавания лиц требуются специальные камеры со встроенным детектором лиц, который позволяют распознавать лица непосредственно на камере и этим снижают нагрузку на сервер и сеть. Для получения более качественного изображения желательно использование камер со встроенными алгоритмами, обеспечивающими качество при различных условиях освещения: задней засветки, контрастного бокового освещения, плохого освещения, помех [8]. Разница между камерами для обзорного наблюдения и

камерами, предназначенными для распознавания лиц показана на рис. 1. На рис. 2 показаны этапы улучшения изображения с камер.

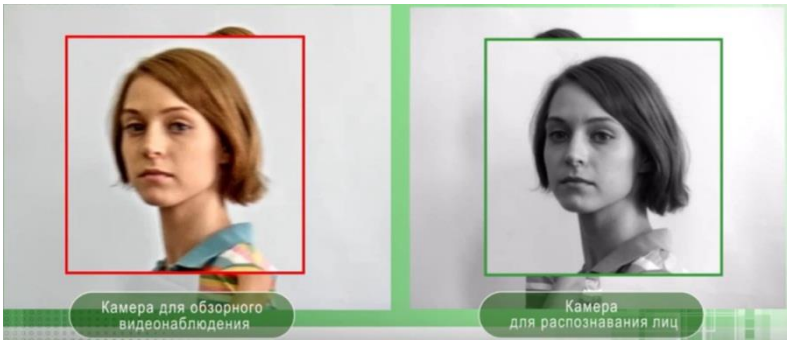

Рисунок 1

Рисунок 2

Описываемая система видеонаблюдения строится на базе «сервисной модели». Все изображения с камер поступают в единый центр хранения данных (ЕЦХД), который предоставляет доступ к видеокамерам и архивам данных, которые собирает с камер, установленных в подъездах, местах массового скопления людей, во дворах. Пользователями данной системы видеонаблюдения являются МВД, МЧС, службы городского управления, получающие изображения по защищенным каналам передачи данных. Защиту обеспечивают протокол *https* и шифрованный канал передачи данных с сертификатами. Камеры, в свою очередь, присутствуют в изолированном сегменте сети, поэтому доступ к ним возможно получить только через *VPN*. Сбор изображений поддерживает несколько сотен человек, а эксплуатацию ЕЦХД – всего несколько десятков [9].

Если использовать данную систему в масштабах меньших, чем городских (на охраняемых предприятиях с пропускным режимом, на предприятиях общественного питания, сферы развлечения и т.д.), то целесообразно использовать локальные базы данных и построенные на их основе «белые» или «черные» списки лиц. В случае обнаружения разыскиваемого лица необходимо реализовать автоматически заданную реакцию системы контроля доступа, установленного охранного оборудования и оперативное оповещение внутренних служб безопасности. Для большего охвата возможно предусмотреть связь такой локальной системы с городской системой распознавания лиц для оперативного поиска разыскиваемого лица, зарегистрированного в базе данных ЕЦХД. В таком случае возникает необходимость решения проблема минимизации обменных взаимодействий [10].

Для разработки алгоритма распознавания лиц для рассматриваемой системы существует несколько подходов. При эмпирическом подходе происходит значительное уменьшение участка изображения, где предполагается лицо, или строятся перпендикулярные гистограммы.

Данный метод не представляет сложности в реализации, однако непригоден для нескольких лиц в кадре, большого количества объектов на фоне или при разных ракурсах [11].

При втором подходе используются инвариантные признаки изображения лица: выявляются характерные части лица, его граница, изменение формы, контрастности и т.д., а затем объединяются и верифицируются. Данный подход возможно использовать при повороте головы, но при наличии других лиц на фоне распознавание невозможно, как и при эмпирическом подходе.

Для третьего алгоритма используется детектирование лиц с помощью неких шаблонов лица, определяемых разработчиком. При таком подходе целью алгоритма является проверка каждого сегмента на наличие такого шаблона, при этом этот процесс может производиться для разных ракурсов и масштабов, но требует множество трудоемких вычислений.

Последний подход основывается на обучении системы с помощью тестовых изображений. Для обучения используются базы данных, а каждый фрагмент изображения описывается как вектор признаков, с помощью которого классификаторы определяют, является ли исследуемая часть изображения лицом [12].

Таким образом, можно сделать вывод, что для системы распознавания лиц наиболее пригодным является последний подход, так как алгоритмы, основанные на эмпирическом подходе или инвариантных признаках, неприменимы для разных ракурсов, что имеет большое значение для рассматриваемой системы. Алгоритм на основе детектирования лиц лишен этого недостатка, однако требует ресурсоемких вычислений, что отрицательно скажется на системе с большим объемом данных, которая должна затрачивать на вычисления как можно меньше времени.

Систему распознавания лиц, основанную на подходе обучения с помощью тестовых изображений, целесообразно строить на основе нейронных сетей в первую очередь из-за необходимости работы с большой базой данных. В данном случае нейронная сеть рассматривается как некоторый алгоритм, который может быть реализован на высокопроизводительной системе конвейерного типа [13]. Кроме того, система распознавания лиц должна работать в режиме реального времени, т.е. необходимо малое время обработки данных. Решить и эту задачу позволяет нейронная сеть. Метод Виолы-Джонса, который также возможно использовать в данном подходе, дает обнаружение с ошибками при увеличении наклона лица относительно камеры, поэтому для данной системы не подходит. Метод нейронных сетей позволяет описывать одно изображение лица всего лишь 80 параметрами, что на выходе дает файл небольшого размера, хранящийся в базе данных. Это позволяет увеличить срок хранения данных на серверах с 5 до 100 дней. Именно на различиях этих 80 параметров строится система поиска. Для большей точности распознавания при таком подходе необходимо выявить параметры, которые останутся неизменны, если человек наденет очки, отрастит бороду или состарится с момента снятия фото, хранимого в базе данных [14].

Для уменьшения скорости обработки информации предлагается проводить последовательные вычисления по конвейерному принципу на базе высокопроизводительной вычислительной системы, т.е. вычисления, проводимые на каждом слое, выполняются по очереди, а затем полученные результаты подаются на вход следующего слоя.

Нейронная сеть в самой простой форме представляет собой персептрон, который имеет входные и выходные элементы и выполняет только самые простые операции. Для более сложных вычислений при распознавании лиц необходима структура с большим количеством скрытых слоев, как это показано на рис. 3 (структура персептрона).

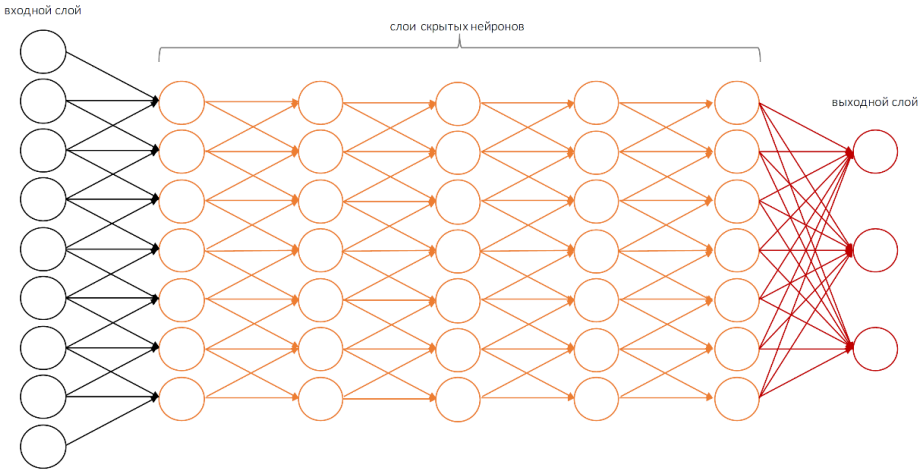

Рисунок 3

На вход при решении рассматриваемой задачи подается разбитое на группы 2x2, 3x3, 5x5 или 11x11 пикселей изображение, которое попадает в сеть слоев, составляющих набор признаков, который подается в классификатор – многослойный персептрон. Размер такой группы пикселей определяется разработчиками системы [15].

Нейронная сеть решает ряд классических задач разного уровня: от самых низкоуровневых до самых высокоуровневых. Среди них выделяются следующие задачи:

- Определение границ (boundaries) – самая низкоуровневая задача.
- Определение вектора к нормали (surface normals) – реконструкция трехмерного изображения из двумерного.
- Определение объектов внимания (saliency).
- Семантическая сегментация (semantic segmentation) – разделение объектов на классы по их структуре.
- Семантическое выделение границ (semantic boundaries) – выделение границ, разбитых на классы.
- Выделение частей тела человека (human parts).
- Распознавание самих объектов (detection) – самая высокоуровневая задача.

Алгоритм, использующийся в данной системе, обладает такой характеристикой, как сублинейное время поиска, так как вынужден работать с базами данных большого объема. Необходимость в таком параметре исходит из данных, представленных на рис. 4, где видно, что при увеличении количества хранимых в базе данных изображений увеличивается и время поиска, что при обработке больших баз данных может стать критично. Данные представлены для различных компаний-разработчиков алгоритмов обработки данных.

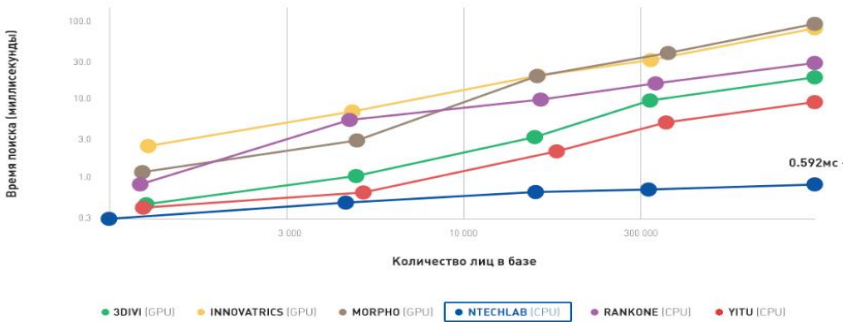

Рисунок 4

Исходя из этого, скорость поиска по большим базам данных изображений следующая:

- 250 млн изображений в БД – поисковое время менее 0,2 с;
- 500 млн изображений – менее 0,3 с;
- 1 млрд изображений – менее 0,5 с.

По графику видно, что наилучшие результаты показал алгоритм от *NtechLab*, который в настоящее время используется в системе видеонаблюдения Москвы. Помимо прочего, данный алгоритм тестировался на изображениях, сделанных в реальных условиях, и фотографиях детей, показав следующие результаты:

- реальные условия: *FNMR* = 0,271;
- лица детей: *FNMR* = 0,433.

На данный момент вычислительные мощности позволяют распознавать людей, попавших в ту или иную базу данных. В пример можно привести базу данных подконтрольных лиц, базу лиц в федеральном розыске, базу социальных сетей и базу данных бюро кредитных историй. Для зафиксированного лица в базу данных заносятся время и место фиксации перед камерой.

Однако стоит учитывать, что от распознавания человек может скрыться, если будет постоянно смотреть вниз, скрывая лицо, или наденет маску, изменяющую или скрывающую форму лица. В этом случае необходимо наличие сигнала от системы и дальнейшее вмешательство человека в процесс опознавания [16].

Аккумулирование массива таких данных дает возможность реализовать несколько сценариев использования системы в сфере безопасности и городского управления:

1. Поиск нарушителя. Если личность нарушителя неизвестна, но его лицо зафиксировала камера, сотрудник полиции загружает фото в систему и производит поиск по базам данных. Как результат – система выдает маршруты передвижения подозреваемого и возможное место его жительства. Кроме того, производится сверка с внешними базами данных и социальными сетями, что позволяет идентифицировать личность.
2. Мониторинг появления подозреваемых перед камерами. После загрузки фото в систему она в реальном времени проводит анализ видеопотока и при обнаружении искомого лица выдает данные об его местоположении.
3. Эффективный контроль соблюдений правил регистрации и проживания. Данные с камер подъездов позволяют отличить постоянных жителей от разовых посетителей, медиков, работников сервисных служб. Это помогает выявить расхождения со средними показателями и данными учета жильцов и обнаружить нелегальных мигрантов.

Подобную систему распознавания лиц возможно использовать не только для решения перечисленных задач. В перспективе система, например, может заменить дисконтные карты в розничной торговле, сохранив в базе данных только вектор признаков лица покупателя и тем самым решив проблему хранения личных данных – имен, фамилий, контактных данных. Также подобную систему возможно использовать локально, загрузив базу данных в мобильное устройство и сравнивая полученное изображение с тем, что хранится в БД. При таком подходе для получения изображения возможно использование не камер, а смарт-очков, что показал пример использования такой системы в Китае.

Таким образом, можно сделать вывод, что система распознавания лиц, которая является расширяемой за счет локальных систем, установленных в местах общего пользования, не только значительно повысит безопасность в многолюдных местах, но и обеспечит оперативную работу различных служб города. Кроме того, применение нейронных сетей позволит понизить требования к оборудованию за счет малого размера хранимых данных и тем самым увеличить срок их хранения, а также уменьшит время обработки данных.

Литература

1. Максименко В.Н., Васильев М.А. Методика расчета стандартизованных показателей качества дополнительных услуг на сетях подвижной связи // T-Comm: Телекоммуникации и транспорт, 2011. – Т. 5. – № 4. – С. 26-28.
2. Максименко В.Н. Услуга определения местоположения абонента как средство защиты в сети сотовой подвижной связи // Известия ЮФУ. Технические науки, 2007. – № 4 (76). – С. 151-155.
3. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи / Под ред. О.Б. Макаревича. – М.: Горячая линия-Телеком. 2007. – 360 с.
4. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности Экономика и качество систем связи, 2017. – № 2 (4). – С. 42-48.
5. Максименко В.Н., Даньков А.П. Идентификация абонента сотовой подвижной связи по голосу // Мобильные системы, 2006. – № 7. – С. 27-30.
6. Максименко В.Н. Услуга определения местоположения абонента как средство защиты в сетях сотовой подвижной связи / Известия ЮФУ. Технические науки, 2007. – № 4 (76). – С. 151-155.
7. Зотин А.Г., Пахирка А.И., Дамов М.В., Савчина Е.И. Улучшение визуального качества изображений, полученных в сложных условиях освещенности на основе инфракрасных данных // Программные продукты и системы, 2016. – № 3. – С. 109-120.
8. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
9. Tadviser.ru: [Электронный ресурс] // Как устроена городская система видеонаблюдения и распознавания лиц в Москве. URL: http://www.tadviser.ru/index.php/Проект:Как_устроена_городская_система_видеонаблюдения_и_распознавания_лиц_в_Москве (Дата обращения 28.10.18).
10. Максименко В.Н. Категорный подход к исследованию аспектов защиты информации и управления качеством сервисов и услуг в сетях сотовой подвижной связи // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 9. – С. 41-49.
11. Кухарев Г.А. Системы распознавания человека по изображению лица. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2006. – 176 с.
12. Пентланд А. Распознавание лиц для интеллектуальных сред // Открытые системы, 2000. – № 3. – С.17-20.
13. Саймон Х. Нейронные сети: полный курс, 2-е издание. Пер. с англ. – М.: Издательский дом «Вильмс», 2006. – 1104 с.
14. Ntechlab.ru: [Электронный ресурс] // Идентификация лиц. URL: https://ntechlab.ru (Дата обращения 30.10.18).
15. Форсайт Д.А., Понс Д. Компьютерное зрение. Современный подход. – М.: Вильямс, 2004. – 928 с.
16. Кухарев Г.А. Поиск изображений лиц в больших базах данных // Мир измерений, 2009. – № 4. – С. 22-30.