ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

These proactive solutions not only address the specific vulnerabilities identified but also aim to elevate the standard of security in anticipation of future threats, reflecting a commitment to an adaptive and resilient security posture (Table 1).

Conclusion

In conclusion, the penetration tests conducted within the scope of this study have illuminated significant security gaps in IP cameras, revealing an urgent need for robust and resilient cybersecurity measures in the expanding landscape of IoT devices. The penetration testing on proprietary devices, ethically bound and contained within a controlled setting, has emphasized the pressing necessity for enhanced security measures in the face of growing cyber threats. The vulnerabilities identified call for manufacturers and cybersecurity experts to foster a culture of advanced defense strategies and robust security protocols. This research underpins the importance of integrating security as a core component in the design and development of IoT devices. As the number of interconnected devices escalates, so too does the complexity of potential cyber threats, mandating a proactive and adaptive security posture. The adoption of comprehensive security standards, development of user-centric security tools, and elevation of end-user security awareness are essential for preserving privacy and ensuring the integrity of our digital infrastructure. This study serves as a catalyst for continued efforts toward securing the digital ecosystem, advocating for preemptive measures that protect against the dynamic and sophisticated nature of modern cyber threats, thus reinforcing the resilience of our increasingly connected world.

References

1. Akhilesh, R., Bills, O., Chilamkurti, N., & Chowdhury, M. J. M. (2022). Automated Penetration Testing Framework for Smart-Home-Based IoT Devices. Future Internet, 14(10), 276. https://doi.org/10.3390/fi14100276

2. Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111, 2287-2310. https://doi.org/10.1007/s11277-019-06986-8

3. Al-Hawawreh, M., & Sitnikova, E. (2020). Developing a security testbed for industrial internet of things. IEEE Internet of Things Journal, 8(7), 5558-5573. https://doi.org/10.1109/jiot.2020.3032093

4. Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. IEEE Internet of Things Journal, 6(5), 9042-9053. https://doi.org/10.1109/jiot.2019.2926365

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, 6(5), 8182-8201. https://doi.org/10.1109/jiot.2019.2935189

УДК 004

РАЗРАБОТКА МУЛЬТИБИОМЕТРИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ ГЛУБОКОЙ НЕЙРОННОЙ СЕТИ

Аббасов Алмазбек Алижанович
a_abbassov@mail.ru
Исайнова Алия Насиповна
issainova_an@enu.kz
Евразийский национальный университет им. Л.Н.Гумилева,
факультет информационных технологий,
кафедра информационной безопасности
Научный руководитель - Исайнова Алия Насиповна

В современном мире информационная безопасность является одним из важнейших аспектов и решение этой проблемы в области разработки и эксплуатации информационных

систем различного назначения (военных, технических, экономических, медицинских, социальных и др.), а также связано с разработкой всевозможных требований к обеспечению их безопасности и созданием программно-аппаратных средств от несанкционированного доступа. В этой связи становится все более востребованным разработка и внедрение мультибиометрических систем, которые обеспечивают высокий уровень защиты. Мультибиометрическая система - это система, которая использует несколько биометрических признаков для аутентификации личности. Эти признаки могут включать в себя отпечатки пальцев, геометрию лица, радужку глаза, голос и другие уникальные характеристики человека.

В данной статье рассматривается процесс разработки мультибиометрической системы, основанной на глубокой нейронной сети. В текущей реализации используется существующая модель для обнаружения лиц, в библиотеке face recognition и mediapipe, в связи с чем был использован фреймворк FaceMesh, который использует глубокое обучение для точного и быстрого обнаружения различных анатомических особенностей лица, таких как глаза, брови, нос, рот и др.

Библиотека face_recognition - это инструмент для распознавания лиц, который предоставляет простой интерфейс для обнаружения и сопоставления лиц на изображениях. Она основана на библиотеке dlib и позволяет легко интегрировать возможности распознавания лиц в приложения с использованием Python с высоким уровнем точности. Для предварительной обработки изображения и быстрой техники обнаружения объекта на кадре был использован Каскад Хаара. Идея каскада Хаара заключается в том, чтобы использовать несколько простых классификаторов, каждый из которых является набором фильтров Хаара, для пошагового выявления объектов на изображении. Каждый классификатор в каскаде проверяет, присутствует ли объект на определенном участке изображения, и в случае необходимости передает результат следующему классификатору в каскаде.

Ниже показан пример работы Каскада Хаара (см. рисунок -1)

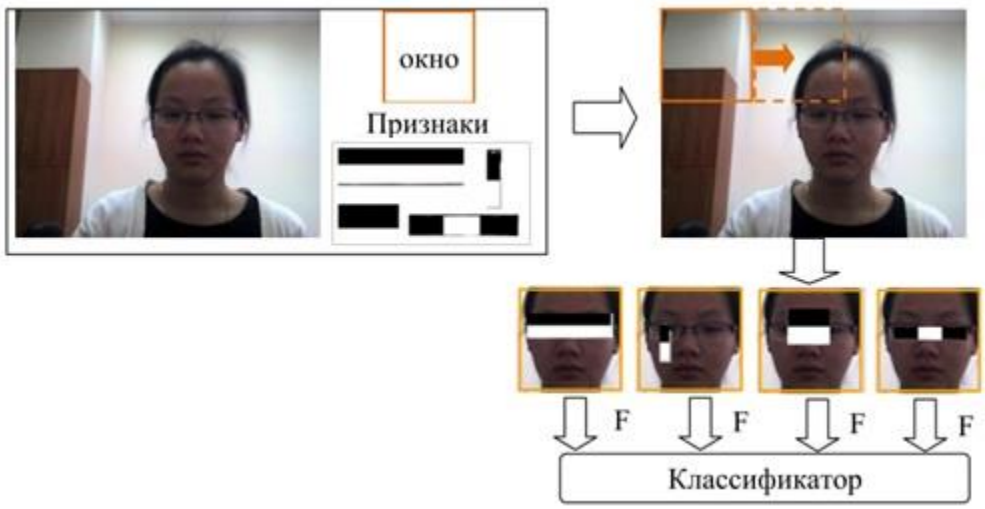

Рисунок-1. Метод обработки изображения Каскадом Хаара.

Для детекции ключевых точек глаз, и последующей обработки радужной оболочки глаза использовался фреймворк MediaPipe, который предоставляет 468 лицевых ориентиров FaceMesh. Для работы глазных точек на модели необходимо выбрать соответствующие точки. Для обработки был выбран правый глаз, соответстующие индексы для правого глаза: 33, 160, 158, 133, 153, 144 (см. рисунок-2).

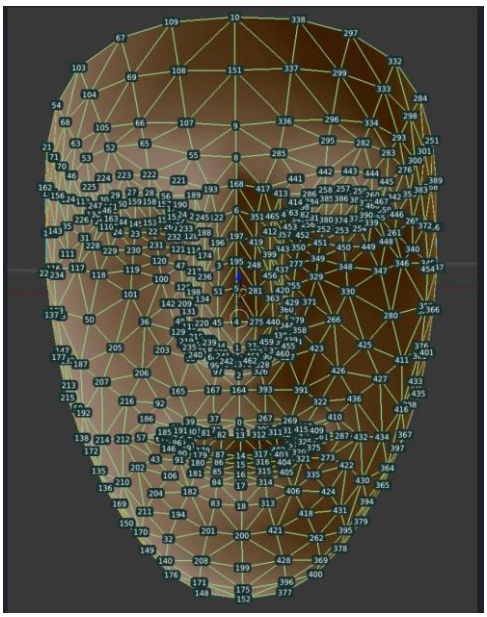

Рисунок-2. Доступные лицевые ориентиры фреймворка FaceMesh.

Программная реализация мультибиометрической системы включает в себя ряд функций на языке программирования Python:

```
def recognize_faces(image_path):
    print(f"Processing image: {image_path}")
    image = cv2.imread(image_path)
    rgb = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
    boxes = face_recognition.face_locations(rgb, model='hog')
    encodings = face_recognition.face_encodings(rgb, boxes)
```

Рисунок-3. Функция recognize face.

Функция **recognize_faces** (см. рисунок-3) для обработки изображения, которая принимает в качестве аргумента путь к файлу. Полученное изображение формата jpeg (320x320) преобразуется из формата BGR в формат RGB. Это необходимо для использования библиотеки face_recognition, которая ожидает изображения в формате RGB. Обнаружение лиц на изображении происходит с помощью метода face_locations из библиотеки face_recognition. Метод возвращает координаты ограничивающих рамок лиц на изображении. Извлечение эмбеддингов лиц осуществляется с помощью метода face_encodings из библиотеки face_recognition. Этот метод принимает изображение и координаты лиц, а затем возвращает эмбеддинги для каждого обнаруженного лица (см. рисунок – 4).

Эмбеддинг - это векторное представление изображения в пространстве признаков. Этот вектор содержит информацию о ключевых характеристиках изображения, которые были изучены и сжаты в числовую форму. Эмбеддинг позволяет представить изображение в виде набора чисел, который можно использовать для различных задач анализа изображений, таких как распознавание объектов, классификация изображений, поиск похожих изображений.

```
Processing image 1/5: my_face\Abbassov Almazbek\IMG-20240220-WA0029.jpg
[-0.15591042  0.13260853  0.0390452  -0.04466885 -0.11476433 -0.01305724
 -0.08401162 -0.06018587  0.10384583 -0.15784396  0.23294078 -0.09642887
 -0.22257502 -0.0432638  -0.02069029  0.15025438 -0.1470201  -0.05805705
 -0.02835031 -0.05823249  0.12813295  0.0305124  -0.07570557  0.06274808
 -0.07951678 -0.37450331 -0.03853465 -0.07140633 -0.03825151 -0.10497696
 -0.05374363  0.08360235 -0.1513539  -0.07249168  0.00430708  0.07283696
 -0.04482518 -0.00640963  0.13200359 -0.02041658 -0.14933591  0.01046109
  0.06832479  0.27804273  0.19157015  0.06723086 -0.01313315 -0.07645124
  0.21094091 -0.24170426 -0.00267547  0.14466532  0.04445995  0.09113915
  0.07755005 -0.095824    0.01765274  0.07629313 -0.1375543   0.02422678
  0.06026193 -0.10452224 -0.04951111 -0.07843382  0.22755259  0.10006876
```

Рисунок-4. Процесс извлечения эмбеддингов лиц из изображений.

Этот цикл извлечения эмбеддингов проходит по всем обнаруженному лицу на изображении. Добавление закодированного эмбеддинга в список известных эмбеддингов лиц и ему присваивается имя папки, в которой находится изображение в список имен известных людей.

Схожий цикл, но, на основе гистограммы цветовых каналов радужки глаза применяется для извлечения эмбеддингов с изображений. Этот метод представляет собой статистическое распределение интенсивности пикселей в каждом из цветовых каналов (красном, зеленом и синем) радужки глаза. Это означает, что для каждого цветового канала подсчитывается количество пикселей с определенной интенсивностью. применяется для обработки изображений с целью извлечения эмбеддингов радужки правого глаза. Все эти процессы проходят в фоновом формате, для обработки видеопотока в реальном времени были созданы иные функции.

Функция **process_iris_detection** (см. рисунок-5) предназначена для обработки кадра видеопотока и обнаружения радужки правого глаза на нем.

```python
def process_iris_detection(frame, x, y, w, h, iris_detector, extract_iris_embeddings, known_iris_encodings, threshold):
    eye_roi = frame[y:y + h, x:x + w]
    iris = iris_detector.detectMultiScale(eye_roi)
    for (ex, ey, ew, eh) in iris:
        iris_roi = eye_roi[ey:ey + eh, ex:ex + ew]
        iris_embedding = extract_iris_embeddings(iris_roi)
        for known_iris_embedding in known_iris_encodings:
            if compare_iris_embeddings(iris_embedding, known_iris_embedding) < threshold:
                cv2.putText(frame, text: "Iris Matched", org: (x + ex, y + ey - 10), cv2.FONT_HERSHEY_SIMPLEX, fontScale: 0.5,
                break
```

Рисунок-5. Функция process_iris_detection.

Функция **process_iris_detection**, принимает в качестве аргументов следующие параметры:

- **frame**: текущий кадр видеопотока
- **x, y, w, h**: координаты и размеры области интереса (ROI) глаза на кадре
- **iris_detector**: детектор радужки глаза (например, Haar Cascade)
- **extract_iris_embeddings**: функция для извлечения эмбеддингов радужки глаза из изображения радужки
- **known_iris_encodings**: известные эмбеддинги радужки глаза, с которыми будет сравниваться текущий эмбеддинг
- **threshold**: пороговое значение для определения совпадения эмбеддингов

Метод detectMultiScale возвращает прямоугольные области, где была обнаружена радужка. Извлечение области интереса (ROI) глаза из текущего кадра видеопотока на основе

переданных координат и размеров. Обнаружение радужки глаза в области интереса с помощью детектора радужки глаза. Цикл перебора всех обнаруженных прямоугольных областей радужки глаза. Извлечение эмбеддинга радужки глаза с помощью функции extract_iris_embeddings, передавая ей область интереса радужки глаза. Проверка условия сравнения эмбеддингов радужки глаза с известными эмбеддингами происходит Эвклидовым расстоянием между текущим и известным эмбеддингом и если расстояние меньше порога, считаем, что радужки совпадают. Вывод текста "Iris Matched" на кадр в позиции.

Эта функция позволяет обрабатывать кадр видеопотока, обнаруживать радужку глаза в области интереса и сравнивать ее эмбеддинг с известными эмбеддингами для определения совпадений.

Вышеописанные функции в совокупности образовывают мультибиометрическую систему для распознования лица и радужной оболочки правого глаза пользователя с применением глубоких нейронных сетей для повышения эффективности и быстродействия аутентификации пользователя по двум анотомическим признакам.

Запуск получение видеопотока с веб-камеры (см. рисунок-6), во всплывающем окне «Frame» можем наблюдать результат распознования по двум биометрическим признакам (см. рисунок-7).

```python
# Получение видеопотока для распознавания радужки глаза и лица
video_capture = cv2.VideoCapture(0)
while True:
    ret, frame = video_capture.read()
    processed_frame = process_frame(frame)
    cv2.imshow( winname: "Iris and Face Recognition", processed_frame)
    if cv2.waitKey(1) & 0xFF == ord('q'):
        break
```

Рисунок-6. Получение видеопотока с веб-камеры.

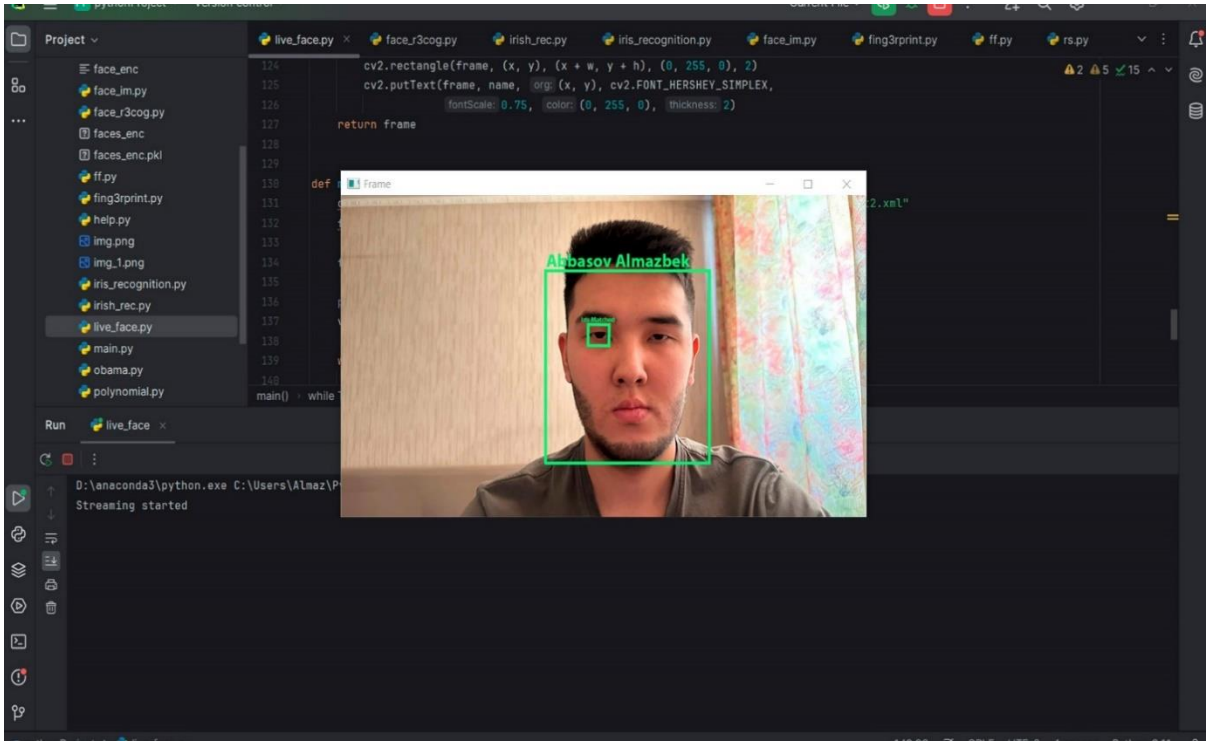

Рисунок-7. Результат работы программы.

В течение многих лет исследователи занимаются разработкой методов распознавания лиц, однако данная проблема до сих пор остается актуальной. Это связано с тем, что условия съемки лиц могут быть разнообразными и изменчивыми: освещение, угол обзора, возраст, выражение лица и другие факторы могут сильно влиять на процесс распознавания. При проектировании систем распознавания лиц часто стараются ограничить эти факторы, однако основной интерес представляет именно распознавание лиц на фотографиях, сделанных в неконтролируемых условиях. Благодаря прогрессу в области глубокого машинного обучения и появлению больших наборов данных для тренировки систем, в последние годы наблюдается значительный прогресс в этой области.

Данный метод мультибиометрической идентификации позволяет повысить безопасность аутентификации путем объединения нескольких биометрических данных человека с помощью нейронных сетей, что в свою очередь обеспечивает быстродействие и достаточную точность обработки.

Список использованных источников

1. Кухарев Г.А., Каменская Е.И., Матвеев Ю.Н., Щеголева Н.Л. Методы обработки и распознавания изображений лиц в задачах биометрии. – М.: Политехника, 2013. – 416 с.

2. Галушкин А. И. Нейронные сети: основы теории. / А. И. Галушкин. – Москва : Горячая линия-Телеком, 2019. – 456 с. – ISBN 978-5-9912-0082-0

3. Рыбалко С. Использование OpenCV и Face Recognition в системах распознавания лиц на одноплатных компьютерах типа Raspberry Pi / С. Рыбалко // Evergreens.com.ua : электронный журнал. – URL: https://evergreens.com.ua/ru/articles/open-cv-face-recognition.html. – Дата публикации: 25.01.2021.

РАЗРАБОТКА ИНСТРУМЕНТА OSINT ДЛЯ АВТОМАТИЧЕСКОГО СБОРА ИНФОРМАЦИИ ИЗ ОБЩЕДОСТУПНЫХ ИСТОЧНИКОВ

Акылбек Бота Алтынбековна
akylbek.ba@mail.ru
Научный сотрудник Института теоретической математики
и научных вычислений ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Шахметова Г.Б.

OSINT - это набор методов и техник, которые позволяют эффективно использовать свободно доступные источники информации.[1] В области кибербезопасности и сбора разведывательных данных открытые источники информации (OSINT) представляют собой сбор, анализ и использование публично доступной информации из различных онлайн и офлайн источников. В отличие от традиционных методов разведки, которые полагаются на классифицированные или конфиденциальные данные, OSINT использует открыто доступную информацию для выявления инсайтов, оценки рисков и поддержки процессов принятия решений.

Инструменты OSINT служат нескольким целям и находят применение в различных областях, включая кибербезопасность, правоохранительную деятельность, корпоративную разведку и конкурентный анализ. Вот некоторые ключевые цели и применения инструментов OSINT:

1. **Угрозовая Разведка:** Инструменты OSINT позволяют специалистам по кибербезопасностимониторить и анализировать онлайн-активности, выявляя потенциальные угрозы, уязвимости и злоумышленников. Путем сбора информации с форумов, социальных сетей и других открытых источников, они помогают предотвратить атаки и защитить информацию.

2. **Исследование Конкурентов:** В бизнесе инструменты OSINT используются для анализа деятельности конкурентов, их стратегий маркетинга, отзывов клиентов и других