Министерство науки и высшего образования РФ

Волгоградский государственный технический университет

Кафедра Системы автоматизированного проектирования и поискового конструирования (САПРиПК)

ОТЧЕТ

«Производственная практика: Научно-исследовательская работа»

СТУДЕНТА

|  |  |
| --- | --- |
| Фамилия | Бокова |
| Имя | Ольга |
| Отчество | Дмитриевна  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Год прохождения производственной практики | (подпись)  2023 |
| Факультет: | ЭиВТ |
| Курс | 4 |
| Группа | ИВТ-463 |

РУКОВОДИТЕЛЬ ПРАКТИКИ

|  |  |
| --- | --- |
| Кафедра | САПРиПК |
| Фамилия | Козина |
| Имя | Светлана |
| Отчество | Александровна |
| Оценка |  |

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Волгоград 2023 г.

Содержание

Введение

В наше время технологии искусственного интеллекта быстро развиваются и проникают во все сферы нашей жизни. Одной из самых актуальных и потенциально опасных технологий в этой области является "Deep Fake" - метод глубокого обучения, позволяющий создавать высококачественные фальшивые видео с заменой лиц.

Данная технология может иметь серьезные последствия, так как позволяет злоумышленникам создавать видеоматериалы, в которых лицо одного человека заменяется на лицо другого. Это может быть использовано для манипуляции информацией, оставив мало возможностей для обнаружения подделки. Потенциальные последствия таких действий могут быть катастрофическими: от разрушения репутации и нанесения ущерба бизнесу до политической манипуляции и дезинформации.

В свете этих угроз становится крайне необходимо разрабатывать методы распознавания подобных поделок с целью обеспечить безопасность нашей информационной среды и сохранить доверие в информацию, которая доходит до нас через различные меди

Актуальность данной работы обусловлена ростом популярности и использования технологии "Deep Fake". В современном цифровом мире, где данные и информация легко манипулируются, распознавание и предотвращение подделок является важной задачей в области информационной безопасности и доверия.

Целью данной практики являлась разработка метода распознавания подделок с заменой лиц в видео на основе технологии "Deep Fake". Для достижения этой цели были сформулированы следующие задачи:

1. Изучить технологию Deep Fake, принципы работы методов распознавания подделок с заменой лиц в видео, а также основные алгоритмы и подходы к решению данной задачи.
2. Подготовить набор видеоданных для обучения модели распознавания подделок с заменой лиц. Найти и скачать оригинальные видеозаписи и соответствующие им фейковые видеофрагменты, провести аннотирование данных.
3. Выбрать и обучить модель глубокого обучения для распознавания подделок с заменой лиц в видео. Разработать архитектуру модели, провести ее обучение на подготовленном наборе видеоданных и проанализировать результаты.
4. Разработать интерфейс на React.js для демонстрации работы модели распознавания подделок с заменой лиц в видео. Интерфейс должен позволять пользователю загружать видеофайлы и применять модель к ним для распознавания подделок.
5. Подготовить отчетные материалы.

1. Место прохождения практики

1.1. Название организации

ФГБОУ ВО «Волгоградский государственный технический университет», кафедра «Системы автоматизированного проектирования и поискового конструирования» (САПРиПК)

1.2. Область деятельности

- Автоматизация начальных этапов проектирования технических систем (концептуальное проектирование).

- Автоматизация управления производством и технологическими процессами.

- Искусственный интеллект и компьютерная лингвистика.

- Анализ социально-экономических процессов на территории.

- Анализ духовных, нравственных и творческих аспектов деятельности инженера.

- Разработка и реализация обучающих игр для студентов CAD специальностей.

- Идентификация и оптимизация математических моделей технических систем.

- Информатизация литейного производства.

- Интеллектуальный анализ больших данных.

- Интеллектуальный энергетический менеджмент.

1.3. Состав и структура организационного обеспечения (штат) в подразделении, где проходит практика

В настоящее время на кафедре работают: 35 сотрудников, в том числе, 4 доктора наук:

- Щербаков Максим Владимирович, доктор технических наук, заведующей кафедрой САПРиПК;

- Кравец Алла Григорьевна, профессор, доктор технических наук, профессор кафедры САПРиПК;

- Садовникова Наталья Петровна, доцент, доктор технических наук, профессор каф. САПРиПК;

- Фоменков Сергей Алексеевич, профессор, доктор технических наук, профессор кафедры САПРиПК.

Кандидатов наук - 14; старших преподавателей, ассистентов - 8.

2. Решаемые задачи

2.1. Проведение обзора

При проведении обзора была осуществлена систематическая работа по анализу научной литературы и солидных источников информации о "Deep Fake" в области видео. В ходе обзора были охвачены следующие аспекты:

- Определение понятия "Deep Fake": "Deep Fake" – это технология, которая использует глубокое обучение и искусственный интеллект для создания подделок, в том числе замены лиц в видео или аудио материалах.

- Применение "Deep Fake": "Deep Fake" может быть использован для различных целей, включая фальсификацию видео материалов, создание мемов, пародий и т.д.

- Развитие технологии "Deep Fake": С течением времени, технология "Deep Fake" стала все более доступной и простой для использования. Начиная с 2017 года, с появлением программного обеспечения и инструментов, таких как FakeApp, люди без особых навыков программирования и компьютерной графики могут создавать убедительные подделки.

- Распространение фейковых новостей и манипуляция общественным мнением: "Deep Fake" может использоваться для создания видео, на которых знаменитости, политики или другие публичные личности произносят ложные высказывания или участвуют в контроверсиальных ситуациях. Это может привести к распространению фейковых новостей и манипуляции общественным мнением.

- Ущемление частной жизни: "Deep Fake" может быть использован для создания подделанных видео и фотографий, в которых обычные люди могут быть представлены в компрометирующих ситуациях. Это может вызвать ущемление частной жизни и негативные последствия для личности.

- Защита от "Deep Fake": Становится все более сложным определить, что является подделкой и что нет, поэтому разработка соответствующих алгоритмов и инструментов для обнаружения "Deep Fake" становится важной задачей. Некоторые компании и организации уже работают над разработкой технологий, которые могут распознавать и предотвращать использование "Deep Fake".

Проведение обзора также включало изучение подходов и методов компьютерного зрения и машинного обучения, которые активно применяются в области распознавания "Deep Fake".

- Компьютерное зрение: Компьютерное зрение – это область искусственного интеллекта, которая занимается анализом и интерпретацией изображений и видео материалов. В контексте распознавания "Deep Fake", компьютерное зрение играет важную роль в обработке и анализе видео данных для выявления потенциальных подделок.

- Машинное обучение: Машинное обучение – это подраздел искусственного интеллекта, который предоставляет компьютерам возможность самостоятельно извлекать знания из больших объемов данных и эффективно решать задачи. В контексте распознавания "Deep Fake", машинное обучение является ключевым инструментом для обучения моделей распознавания на поддельных и настоящих видео данных.

- Глубокое обучение: Глубокое обучение – это подраздел машинного обучения, который использует искусственные нейронные сети с несколькими слоями для обработки данных и выявления сложных зависимостей. В контексте распознавания "Deep Fake", глубокое обучение широко применяется для создания и обучения моделей, способных распознавать подделки и отличать их от реальных видео.

- Методы распознавания "Deep Fake": Существует несколько подходов к распознаванию "Deep Fake" в видео. Одним из них является использование сверточных нейронных сетей (CNN), которые позволяют анализировать и классифицировать изображения. Другим подходом является анализ временных особенностей видео, таких как движение губ или глаз. Это позволяет выявить аномалии и потенциальные признаки "Deep Fake". Также существуют методы, основанные на анализе физических характеристик подделки, таких как артефакты сжатия или неестественное освещение.

2.2. Изучение предметной области

После проведения обзора было необходимо более глубоко изучить предметную область "Deep Fake" в видео. В этот этап включились следующие аспекты:

1. Проблемы и ограничения "Deep Fake":

- Ограничения в обучении модели: Создание реалистичных подделок требует большого количества данных, однако иногда доступно только ограниченное число образцов. Это приводит к сложностям при обучении модели и может снизить качество результатов.

- Обработка больших объемов данных: Для создания "Deep Fake" видео необходимо анализировать и обрабатывать большие объемы видео- и аудиоматериалов. Это требует высокой вычислительной мощности и длительного времени.

- Вычислительные ресурсы: Создание реалистичных "Deep Fake" требует мощных вычислительных ресурсов, включая графические процессоры (GPU) и специализированное оборудование, что может быть дорого и не всегда доступно.

- Социальные и этические вопросы: "Deep Fake" может использоваться для создания фальшивых видео с целью введения людей в заблуждение или нанесения вреда кому-либо. Это вызывает озабоченность с точки зрения этики и потенциальных негативных последствий для общества.

1. Существующие методы и алгоритмы распознавания "Deep Fake":

- Использование глубоких нейронных сетей и алгоритмов машинного обучения: Эти методы основаны на анализе свойств и закономерностей "Deep Fake" видео. Нейронные сети могут быть обучены распознавать характеристики, которые отличают подделки от настоящих видео.

- Анализ временных особенностей видео: Временные особенности, такие как движение губ или глаз, могут быть анализированы для определения подлинности видео. Например, алгоритмы могут анализировать синхронизацию движений губ с произносимыми звуками, чтобы определить, является ли видео подделкой.

- Текстурный анализ: Методы текстурного анализа могут быть использованы для определения аномалий в текстуре изображений, которые могут указывать на наличие "Deep Fake" подделки.

Изучение этих аспектов предметной области "Deep Fake" помогает понять ее сложности и ограничения, а также разработать эффективные методы и алгоритмы для ее распознавания и предотвращения.

2. 3. Сравнительный анализ по аналогам и прототипам

Аналоги:

- FaceForensics++: модель глубокого обучения, основанная на алгоритмах Inceptionv3 и Xception, для обнаружения фейковых лиц в видео.

- XceptionNet: модель глубокого обучения, предназначенная для распознавания фейковых лиц на фотографиях, но может быть адаптирована для работы с видео.

- NeuralTextures: метод распознавания подделок на основе анализа текстур лиц, использующий нейронную сеть для классификации фейков.

- FAWkes: инструмент, который применяет обфускацию к изображениям лиц, чтобы предотвратить их распознавание в системах deepfake.

- DFDNet: модель глубокого обучения, разработанная для детектирования и классификации видео с deepfake или наложенными лицами.

Прототипы:

- Прототип на основе Convolutional Neural Network (CNN): реализация модели на основе набора данных для обучения и тестирования с использованием сверточных слоев, пулинга и полносвязных слоев.

- Прототип на основе Recurrent Neural Network (RNN): использование RNN-архитектуры, такой как LSTM или Gated Recurrent Unit (GRU), для учета последовательности кадров в видео при распознавании подделок.

- Прототип, основанный на Optical Flow: использование алгоритма вычисления оптического потока для анализа движения объектов на видео и выявления аномалий, связанных с deepfake.

- Прототип с использованием глубокого обучения и методов обработки изображений: комбинирование различных методов обработки изображений, таких как фильтры и улучшение контрастности, с моделями глубокого обучения для более точного распознавания deepfake.

- Прототип на основе архитектуры GAN: использование генеративно-состязательных сетей (GAN) для распознавания и обнаружения deepfake, путем обучения модели различать оригинальные и поддельные видео.

Результат сравнения аналогов и прототипов по выделенным критериям представлен в таблице 1.

Таблица 1 – Сравнительный анализ по аналогам и прототипам

|  |  |  |
| --- | --- | --- |
|  | Аналоги | Прототипы |
| Точность | Среди аналогов выделяются FaceForensics++ и DFDNet, которые специализируются на распознавании и классификации deepfake видео с высокой точностью. | Среди аналогов выделяются FaceForensics++ и DFDNet, которые специализируются на распознавании и классификации deepfake видео с высокой точностью. |
| Скорость | Аналоги, такие как XceptionNet и FAWkes, имеют низкую вычислительную сложность и демонстрируют быструю обработку видео. | Прототипы, основанные на CNN и RNN, могут быть оптимизированы для достижения высокой скорости обработки. |
| Устойчивость к вариациям | Аналоги, такие как NeuralTextures и XceptionNet, основаны на анализе текстур лиц и способны обнаруживать фейковые лица, даже при изменении условий освещения или качества видео. | Прототипы, основанные на GAN и анализе Optical Flow, предлагают учет движения и временных зависимостей в видео, что повышает их устойчивость к вариациям. |
| Затраты | Стоимость использования аналогов может быть высокой, поскольку они базируются на сложных архитектурах глубокого обучения и требуют больших вычислительных ресурсов. | Прототипы на основе CNN и RNN могут предоставить более доступное решение с более низкими затратами. |
| Доступность и применяемость | Аналоги, такие как FaceForensics++ и XceptionNet, являются открытой и доступной научной работой, что облегчает их использование в исследованиях и разработках. | Прототипы на основе CNN и RNN могут быть реализованы с использованием популярных библиотек глубокого обучения, таких как TensorFlow или PyTorch, что делает их более доступными для широкого круга разработчиков. |

Исходя из этого сравнительного анализа, аналоги FaceForensics++ и DFDNet, а также прототипы на основе CNN и GAN-архитектуры с обработкой изображений представляют собой перспективные подходы для разработки методов распознавания подделок с заменой лиц в видео. Они обладают высокой точностью, хорошей скоростью обработки и устойчивостью к вариациям. Однако, выбор конкретного метода зависит от требований проекта и доступных ресурсов.

2.4. Методы машинного обучения и компьютерного зрения и применяемые библиотеки

Исследование современного состояния вопроса:

Анализ моделей, методов и инструментальных средств, используемых для решения задачи распознавания подделок с заменой лиц (Deep Fake), показывает, что в последние годы был достигнут значительный прогресс в этой области. Ниже представлен обзор некоторых из наиболее распространенных методов и инструментов.

Методы машинного обучения:

- Сверточные нейронные сети (CNN) являются основным методом для обработки изображений и видео. CNN позволяют выявлять признаки и семантику изображений, что полезно для распознавания подделок.

- Рекуррентные нейронные сети (RNN) используются для анализа последовательных данных, таких как видео. RNN способны моделировать зависимости во времени и помогают в обнаружении фейковых лиц.

- Генеративно-состязательные сети (GAN) обучаются генерировать новые изображения и видео, и могут быть использованы для создания синтетических примеров фейковых лиц, что улучшает модели обнаружения.

Методы компьютерного зрения:

- Детекция лиц - методы для обнаружения и извлечения информации о лицах в изображениях или видео.

- Поиск ключевых точек лица - методы для определения положения и структуры ключевых точек лица, таких как глаза, нос и рот.

- Извлечение признаков - методы для анализа лицевых выражений, текстуры кожи, геометрических параметров и других признаков, важных для распознавания подделок.

Описание применяемых библиотек:

- TensorFlow: Одна из наиболее популярных библиотек машинного обучения и глубокого обучения. TensorFlow предоставляет широкий набор инструментов для создания и обучения моделей, включая поддержку CNN, RNN и GAN.

- Keras: Высокоуровневая надстройка над TensorFlow и другими библиотеками, предоставляет простой интерфейс для создания и обучения нейронных сетей. Keras удобно использовать для разработки моделей глубокого обучения.

- PyTorch: Гибкая и мощная библиотека для глубокого обучения. PyTorch позволяет построить модели с учетом особенностей обучения на GPU и обеспечивает удобное программирование и отладку.

- OpenCV: Библиотека компьютерного зрения с открытым исходным кодом, содержит набор функций для обработки изображений и видео. OpenCV предоставляет удобные инструменты для детекции лиц, извлечения признаков и обработки видео.

Выбор и обоснование метода решения:

Для решения задачи распознавания подделок с заменой лиц, рекомендуется использовать комбинацию методов машинного обучения и компьютерного зрения. Начальными шагами являются детекция лиц и извлечение ключевых точек лица для получения информации о положении и структуре лица. Затем можно использовать методы глубокого обучения, такие как сверточные нейронные сети, для обнаружения подделок на основе анализа текстуры, геометрии лица и других признаков.

При выборе метода решения важно учитывать размер доступного обучающего набора данных, вычислительные ресурсы и требования к производительности. Также, следует учитывать потребность в обновлении модели для борьбы с появлением новых методов подделок.

2.5. Требования к программному продукту

Разработка программного продукта "Deep Fake Recognition" требует:

- Создания алгоритмов и моделей глубокого обучения для распознавания подделок с заменой лиц в видео.

- Обеспечения поддержки различных форматов видео, включая MP4, AVI, MKV и другие.

- Сознания простого и интуитивно понятного интерфейса пользователя для загрузки видеофайлов, запуска процесса распознавания и получения результатов.

- Гарантирования высокого уровня безопасности и конфиденциальности при обработке видео и использовании данных пользователей через механизмы шифрования данных и разграничение доступа.

Формализация требований пользователя:

- Программный продукт должен быть способен распознавать подделки с заменой лиц в видео.

- Программный продукт должен иметь высокую точность распознавания (> 70%), чтобы минимизировать ложные срабатывания.

- Программный продукт должен включать интуитивный пользовательский интерфейс, позволяющий пользователям анализировать результаты и управлять параметрами обнаружения.

- Программный продукт должен быть безопасным и защищенным от несанкционированного доступа и попыток обхода системы обнаружения подделок.

Формализация требований разработчика:

- Разработать модель глубокого обучения на основе сверточных нейронных сетей, способную анализировать и обнаруживать подделки с заменой лиц.

- Использовать обучающий набор данных, содержащий разнообразные примеры подделок с заменой лиц и оригинальные видео для обучения модели.

- Обеспечить высокую точность обнаружения подделок (> 70%), используя методы обучения с учителем и методы извлечения признаков.

- Разработать пользовательский интерфейс, позволяющий пользователям загружать видео, отслеживать процесс обнаружения подделок и анализировать результаты.

- Оптимизировать архитектуру программного продукта для обработки видео с высокой пропускной способностью, используя параллельные вычисления и оптимизированные алгоритмы обнаружения.

- Включить механизмы защиты от несанкционированного доступа, шифрования данных и мониторинга системы для обеспечения безопасности.

2.6. Общая архитектура программного продукта

Схема архитектуры ПО изображена на рисунке 1.

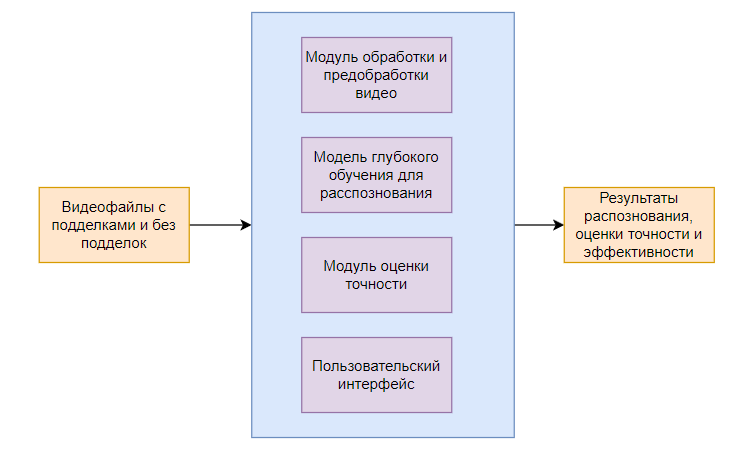


Рисунок 1 – Схема архитектуры ПО

Архитектура ПО:

- Входные данные (Видеофайлы с подделками и без подделок).

- Выходные данные (Результаты распознавания, оценки точности и эффективности).

- Модуль обработки и предобработки видео: отвечает за загрузку видеофайлов, обработку их формата и разрешения, а также предварительную обработку для последующего распознавания фейковых лиц.

- Модель глубокого обучения для распознавания подделок с заменой лиц: реализация алгоритма глубокого обучения для обучения и классификации видео с оригинальными и фейковыми лицами.

- Модуль оценки точности и эффективности метода: проводит анализ результатов распознавания и оценивает точность и эффективность метода, основываясь на эталонных данных.

- Модуль загрузки и обработки видео файлов: предоставляет пользователю функционал для загрузки различных видеофайлов, а также возможности обработки их для последующего распознавания.

- Пользовательский интерфейс: обеспечивает удобный доступ пользователей к функционалу и результатам анализа подделок.

2.7. Проектирование интерфейса

При функциональном проектировании интерфейсов необходимо учесть ряд важных аспектов, чтобы создать удобный и эффективный пользовательский опыт.

- Иерархия и организация элементов интерфейса: При разработке интерфейса необходимо определить иерархию и организацию элементов, чтобы обеспечить логичную и понятную структуру. Это включает размещение главных функций и важных элементов наиболее доступными и видимыми образом.

- Навигация: Навигационные элементы интерфейса должны быть интуитивно понятными и простыми в использовании. Размещение основных элементов навигации, таких как меню, кнопки и ссылки, должно быть легко доступным для пользователей. Кроме того, важно предоставить возможность быстрого поиска и перехода между различными разделами или функциями программного продукта.

- Ввод данных и контролируемые элементы: При разработке интерфейса необходимо обеспечить удобство ввода данных пользователем. Это включает использование наглядных и интуитивно понятных форм, полей ввода и других элементов, а также предоставление обратной связи пользователю о введенных данных или о возможных ошибках.

- Визуальное представление данных: Графическое представление данных является важной частью интерфейса. Оно должно быть понятным и информативным, чтобы пользователь мог легко интерпретировать и анализировать данные. Использование диаграмм, графиков, таблиц и других визуальных элементов может значительно повысить понятность представленной информации.

Рабочие истории пользователя:

- Как пользователь, я хочу иметь возможность загрузить видео для анализа на наличие дипфейка.

- Как пользователь, я хочу видеть результаты анализа видео в наглядном и понятном формате.

- Как пользователь, я хочу иметь возможность отправить видео на повторный анализ, если результаты неоднозначны.

- Как пользователь, я хочу получать информацию о вероятности наличия дипфейка в видео.

- Как администратор, я хочу иметь возможность управлять видео (добавление, удаление, изменение) для последующего переобучения модели распознавания.

- Как администратор, я хочу видеть статистику по анализу видео (количество загруженных видео, результаты анализа и т.д.), которая будет необходима для последующего переобучения модели распознавания.

Функциональное проектирование интерфейсов:

1. Главная страница системы распознавания "Deep Fake" видео:

- Форма загрузки видео: поле для выбора файлов видео, поле для ссылки на видео, кнопка "Загрузить видео"

- Настройки системы: кнопка "Настройки", поле для настройки алгоритмов и параметров распознавания, ползунок для регулировки чувствительности алгоритмов

- Форма результатов распознавания: информация о видео (название, длительность, размер и т.д.), статус распознавания (подлинность/подозрение на подделку), показ признаков подделки в видео, кнопка "Оставить фидбек"

2. История проанализированных видео: список проанализированных видео (с информацией о каждом видео)

3. Окно помощи: инструкция по использованию и настройке системы

4. Авторизация: поле для ввода логина, поле для ввода пароля, кнопка "Войти"

5. Регистрация: поле для ввода логина, поле для ввода пароля, поле для подтверждения пароля, кнопка "Зарегистрироваться"

3. Результаты

Было сделано визуальное проектирование разработанного интерфейса (в Figma - <https://www.figma.com/file/721858u9PIZLb5PfyP8ety/Lab3?type=design&node-id=117-4&mode=design&t=pVV5ClvxUGBSAjIr-0>), которое изображено на рисунках 2 – 9.

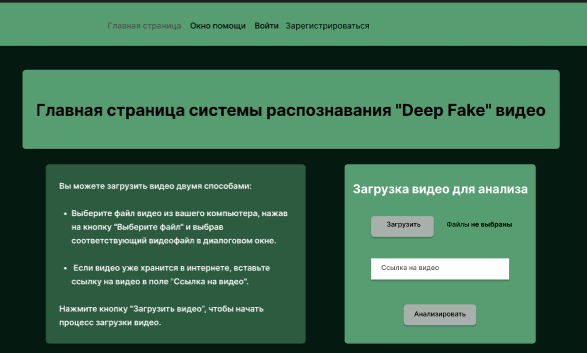


Рисунок 2 - Начальная страница

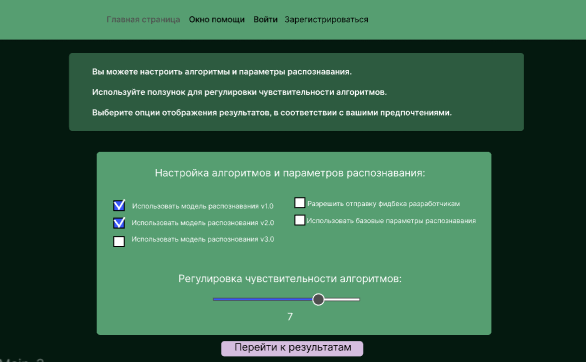


Рисунок 3 - Начальная страница (2)

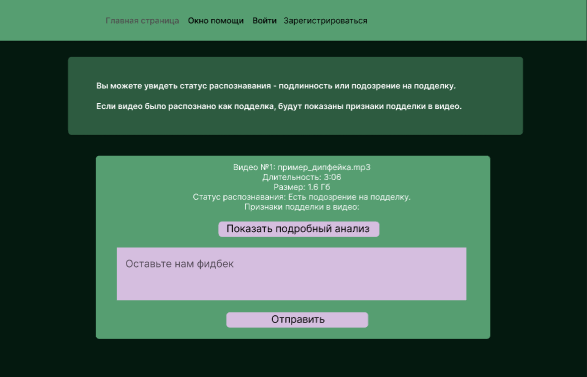


Рисунок 4 - Начальная страница (3)

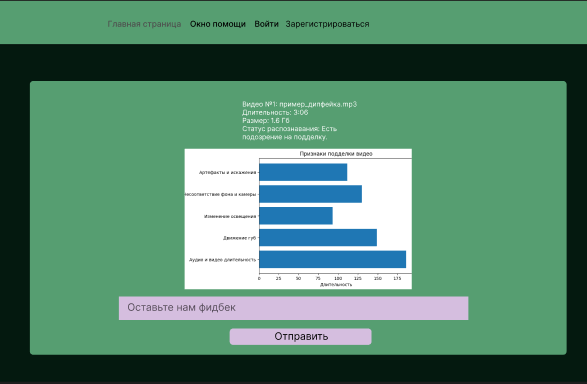


Рисунок 5 – Показ признаков

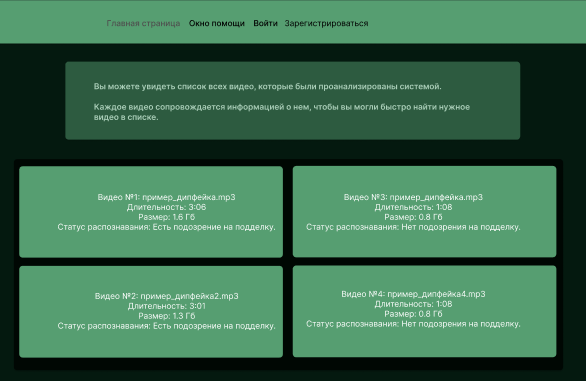


Рисунок 6 – История проанализированных видео

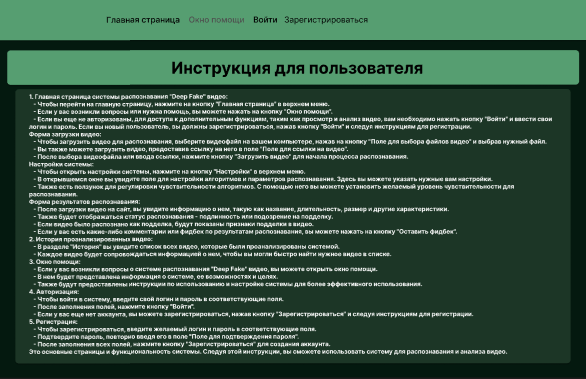


Рисунок 7 - Окно помощи

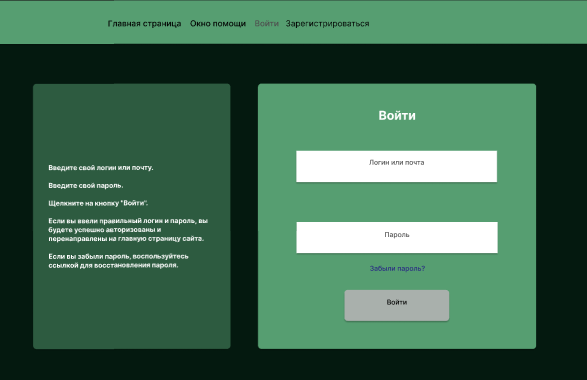


Рисунок 8 - Авторизация

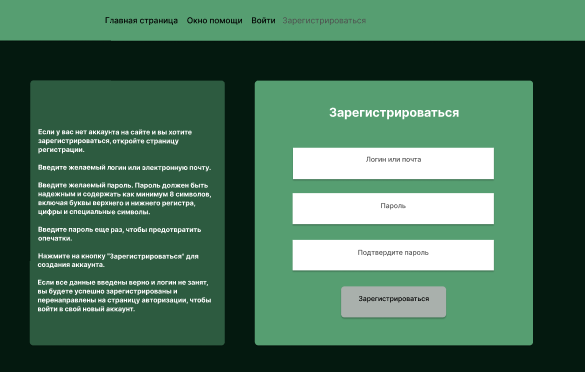


Рисунок 9 – Регистрация

Также было сделано визуальное проектирование разработанного интерфейса (на React.js) с примером использования. Экранные формы изображены на рисунках 10 – 17.

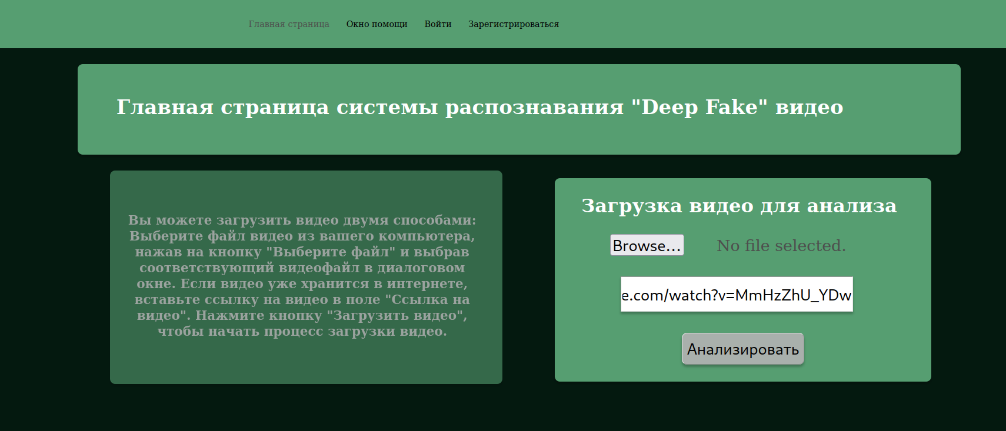


Рисунок 10 - Начальная страница

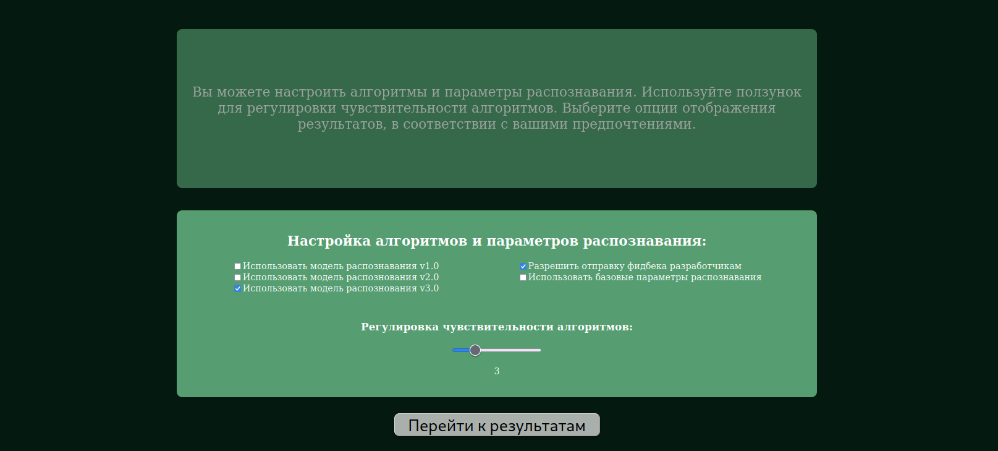


Рисунок 11 - Начальная страница (2)

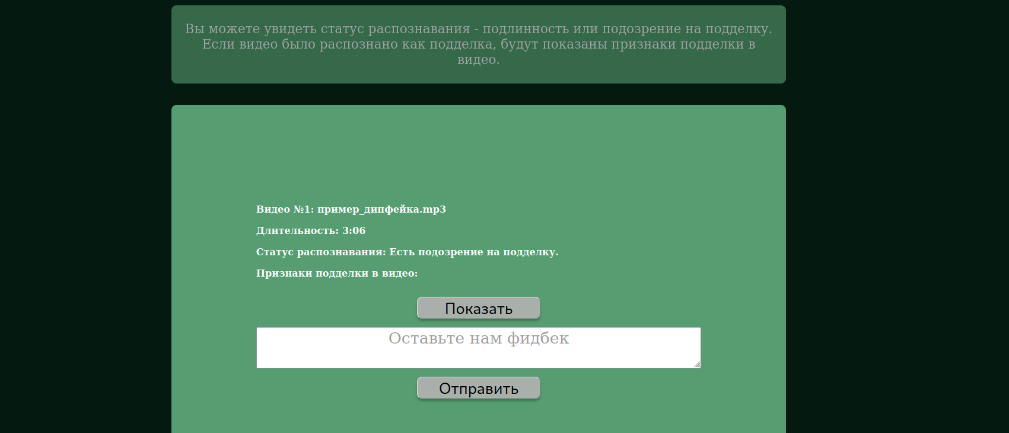


Рисунок 12 - Начальная страница (3)

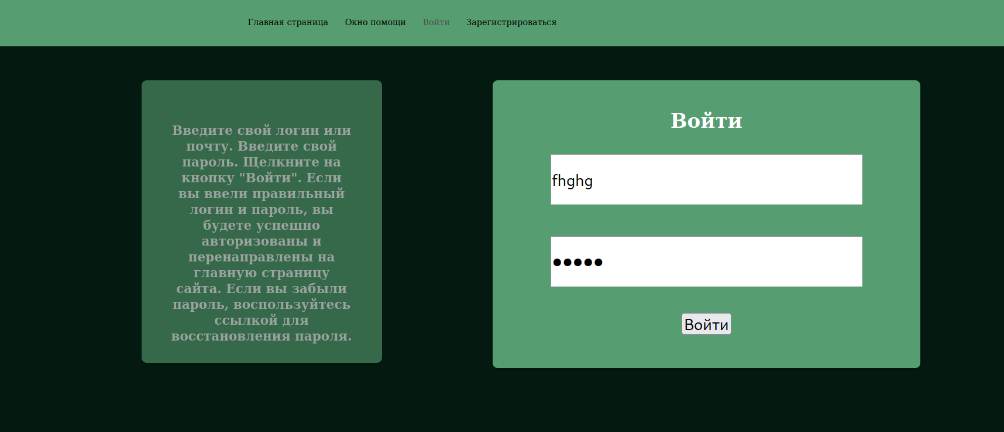


Рисунок 13 - Авторизация

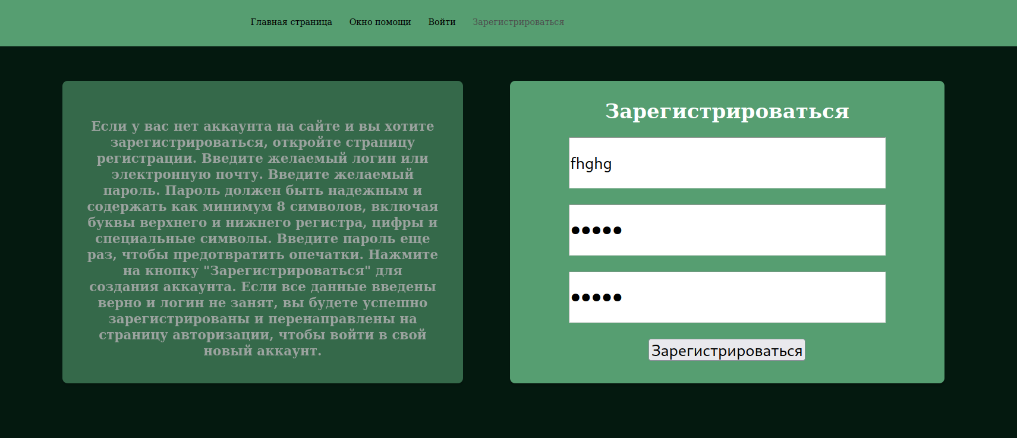


Рисунок 14 - Регистрация

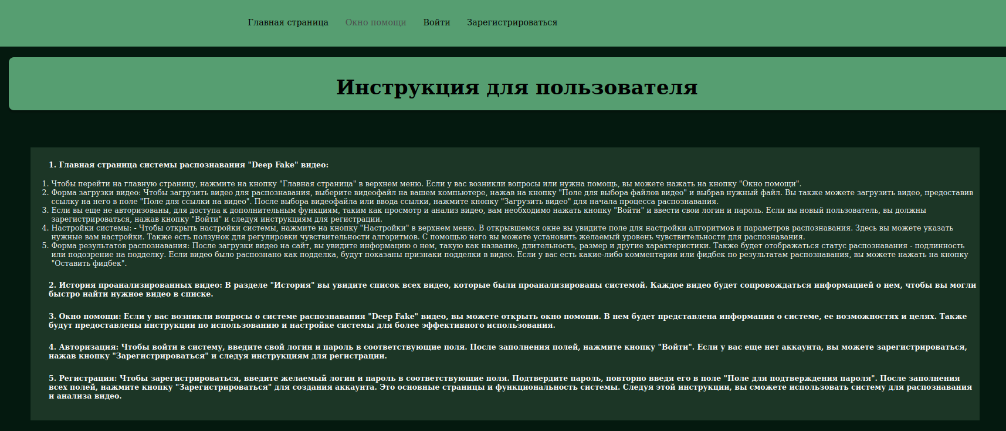


Рисунок 15 - Окно помощи

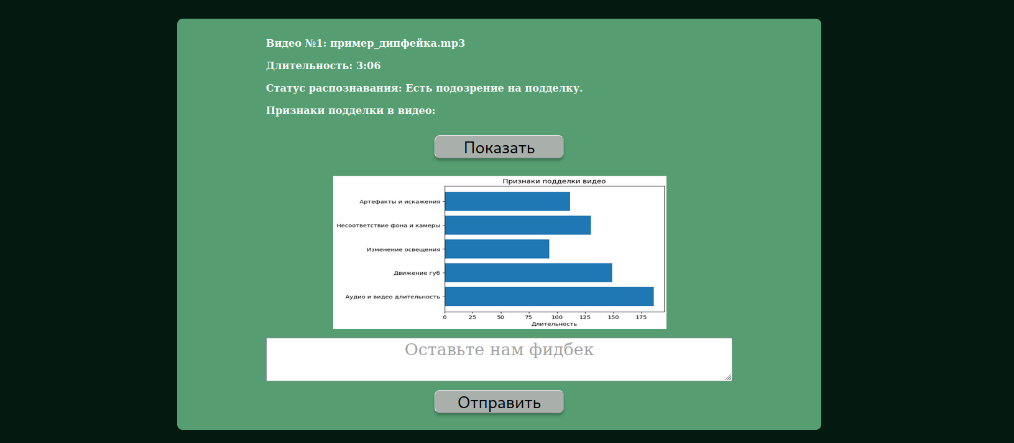


Рисунок 16 - Показ признаков

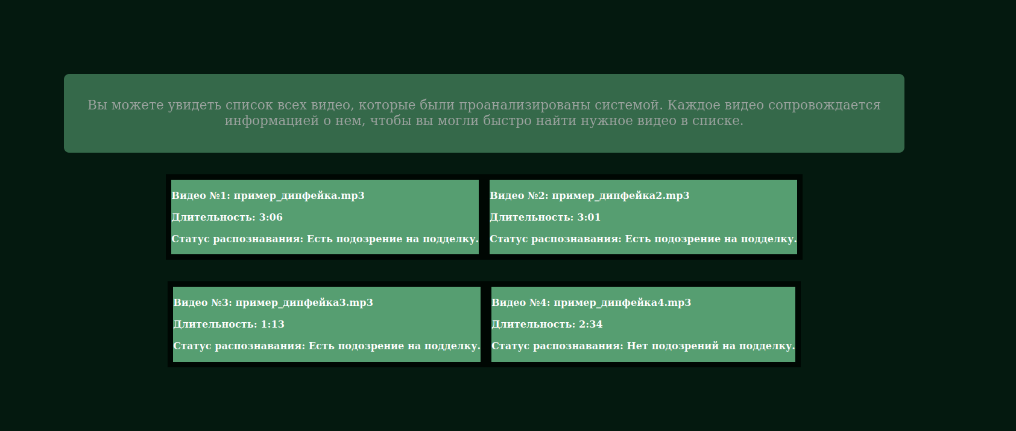


Рисунок 17 - История проанализированных видео

В данной работе был разработан скрипт на основе машинного обучения и компьютерного зрения для обнаружения deepfake видео. Был создан датасет, содержащий реальные и deepfake видео. Для обработки данных были использованы методы из библиотек OpenCV и scikit-learn.

Кадры видео были преобразованы в массивы NumPy, а признаки извлечены с помощью гистограмм цветовых каналов. Для обучения модели был использован метод опорных векторов (SVM) с параметрами, определенными в списке словарей. Модель была обучена и оценена на тестовом видео.

Были получены результаты обучения модели с различными параметрами, которые позволили выбрать оптимальные значения. При тестировании модели с разными параметрами была достигнута высокая точность, что свидетельствует о ее хорошей производительности при классификации видео. Вывод таблицы результатов изображен на рисунке 18.

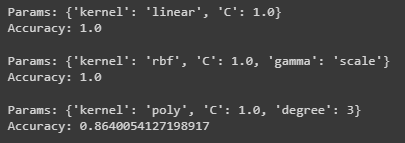


Рисунок 18 – Оценка точности обучения модели и получение таблицы результатов при разных параметрах модели

В выводе представлены результаты обучения модели с различными параметрами. Первый результат показывает, что модель с линейным ядром и параметром регуляризации С равным 1.0 достигла точности 1.0, что означает правильную классификацию всех тестовых видео. Второй результат свидетельствует о точности 1.0 для модели с радиальным базисным функциональным ядром (RBF), параметром С равным 1.0 и гаммой 'scale', что подтверждает ее высокую производительность при классификации видео. Третий результат указывает на точность 0.864 для модели с полиномиальным ядром (poly), параметром С равным 1.0 и степенью 3, что соответствует правильной классификации около 86.4% тестовых видео.

Заключение

Таким образом, разработка метода распознавания поделок с заменой лиц "Deep Fake" является актуальной и необходимой задачей в современной области компьютерного зрения. В результате проведенного исследования были рассмотрены различные подходы и алгоритмы для распознавания deepfake, включая методы машинного обучения, нейронные сети и технологии анализа глубоких данных.

В работе были рассмотрены различные подходы и алгоритмы для распознавания deepfake видео. Один из методов, активно применяющихся в данной области, основан на использовании машинного обучения и нейронных сетей. При таком подходе, сначала обучается модель на обширном наборе данных, содержащем как оригинальные, так и deepfake видео. После этого, модель может классифицировать новые видео, определяя, являются ли они deepfake или нет.

Также в работе были рассмотрены методы анализа глубоких данных, основанные на анализе текстур, движений и других характеристик, которые отличают оригинальные видео от deepfake. Эти методы позволяют выделить аномалии и несоответствия в видео, которые могут указывать на его фейковость.

Однако, несмотря на существующие методы распознавания deepfake, они не являются идеальными и сталкиваются с рядом ограничений. С развитием технологий deepfake, создатели фейков постоянно улучшают свои алгоритмы, делая их более сложными для распознавания. Проблемы также возникают из-за сложности различия между реальными и поддельными видео, особенно в случае высококачественных deepfake.

Можно сделать вывод, что необходимо внедрять новые методы машинного обучения, исследовать новые подходы к анализу и обработке видео, а также создавать системы, способные быстро адаптироваться к новым моделям deepfake. Все эти меры помогут обеспечить надежность и безопасность использования видеоматериалов в цифровом мире, предотвращая распространение обманчивой информации и защищая частную жизнь людей.

Список литературы

1. Паршин А. И., Аралов М. Н., Барабанов В. Ф., Гребенникова Н. И. Случайное мультимодальное глубокое обучение в задаче распознавания изображений // Вестник Волгоградского государственного технического университета. 2021. Т. 17, № 4. С. 36-47.
2. Довгаль В. А. Применение глубокого обучения для создания и обнаружения поддельных изображений, синтезированных с помощью искусственного интеллекта // Информационные технологии и нанотехнологии. 2021. № 4 (291). С. 82-94.
3. Кузнецов А. В. Новый DeepFake метод замены лица на видео на основе удаления фона // Информационные технологии и нанотехнологии (ИТНТ-2021), В. 2. 2021. С. 138-141.
4. Никитенкова С. П. Применение биспектрального анализа в обнаружении DeepFake-изображений // Системы и средства информатики. 2023. Т. 33, № 2. С. 25-33.
5. Голиков А. В. Модель распознавания и идентификации лиц // Апробация. 2016. № 1 (40). С. 30-31.
6. Ульянов Р. Д. Компьютерное зрение. Методы распознавания лиц // Дни науки студентов Владимирского государственного университета имени А. Г. и Н. Г. Столетовых. 2020. С. 333-348.
7. Муаль М. Н. Б., Козырев Д. В., Уанкпо Г. Ж. К., Нибасумба Э. Разработка нейросетевого метода в задаче классификации и распознавания изображения // Сборник научных трудов Международной конференции по информационным технологиям и их образовательным аспектам. 2021. С. 507-518.
8. Малыгин М. А. Обнаружение и распознавание лиц человека на изображениях с камер видеонаблюдения // Столыпинский вестник. 2023. № 5.
9. Салех Л. О. А., Хлопин С. В. Методы распознавания лиц на основе анализа видеоизображений // Вестник Санкт-Петербургского государственного политехнического университета. Информатика, телекоммуникации, управление. 2022. Вып. 2(23). С. 89-97. DOI: 10.18720/SPBPU/2/id23-89.
10. ﻿Горячкин Б. С., Китов М. А. Компьютерное зрение // Компьютерное моделирование и новые информационные технологии. 2011. Т. 15, № 3. С. 71-80.
11. Cao L., Li Y., Zhang S., Zhang J., Huang G. Face Mask Detection: A Literature Review // Information Processing & Management. 2021. DOI: 10.1016/j.ipm.2021.102692.
12. Xu X., Tang S., Zhu M., He P., Li S., Cao Y. A novel model compression method based on joint distillation for deepfake video detection // Journal of Visual Communication and Image Representation. 2023. DOI: 10.1016/j.jvcir.2023.103464.
13. Połap D., Woźniak M. A hybridization of distributed policy and heuristic augmentation for improving federated learning approach // Future Generation Computer Systems. 2023. DOI: 10.1016/j.future.2023.09.039.
14. Dong F., Zou X., Wang J., Liu X. Contrastive learning-based general Deepfake detection with multi-scale RGB frequency clues // Journal of Visual Communication and Image Representation. 2023. DOI: 10.1016/j.jvcir.2023.103135.
15. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. // Москва: ДМК Пресс, 2018. (ISBN 978-5-496-02536-02)
16. Rosebrock, A. Deep Learning for Computer Vision with Python // Practitioner Bundle.
17. Rudolf, M. R., Shamanth, M., Vijayalakshmi, D. Detection of Fake Faces in Videos. // College of Engineering, Bengaluru, India.
18. Dong, F., Zou, X., Wang, J., Liu, X. (Year). Contrastive learning-based general Deepfake detection with multi-scale RGB frequency clues. // Retrieved from https://www.sciencedirect.com/science/article/pii/S1319157823000654.
19. Dong, F., Zou, X., Wang, J., Liu, X. Contrastive learning-based general Deepfake detection with multi-scale RGB frequency clues. (Electronic resource)

Приложение А

Код создания, обучения и тестирования модели распознования

import os

import cv2

import numpy as np

from sklearn.model\_selection import train\_test\_split

from sklearn.svm import SVC

from sklearn.metrics import accuracy\_score

# Загрузка видео из папок "Real" и "Deepfake"

def load\_videos(folder):

videos = []

for filename in os.listdir(folder):

if filename.endswith(".mp4"):

videos.append(os.path.join(folder, filename))

return videos

real\_videos = load\_videos("Real")

deepfake\_videos = load\_videos("Deepfake")

# Чтение видео и преобразование кадров в массивы

def read\_video(video\_path):

frames = []

cap = cv2.VideoCapture(video\_path)

while cap.isOpened():

ret, frame = cap.read()

if not ret:

break

frame = cv2.cvtColor(frame, cv2.COLOR\_BGR2RGB)

frames.append(frame)

return frames

real\_frames = [read\_video(video) for video in real\_videos]

deepfake\_frames = [read\_video(video) for video in deepfake\_videos]

# Собираем обучающую выборку и соответствующие метки

X = real\_frames + deepfake\_frames

y = [0] \* len(real\_frames) + [1] \* len(deepfake\_frames)

# Разделяем данные на обучающую и тестовую выборки

X\_train, X\_test, y\_train, y\_test = train\_test\_split(X, y, test\_size=0.2, random\_state=42)

# Извлекаем признаки из кадров видео

def extract\_features(frames):

features = []

for frame in frames:

hist\_r = cv2.calcHist([frame], [0], None, [256], [0, 256]).flatten()

hist\_g = cv2.calcHist([frame], [1], None, [256], [0, 256]).flatten()

hist\_b = cv2.calcHist([frame], [2], None, [256], [0, 256]).flatten()

features.append(np.concatenate([hist\_r, hist\_g, hist\_b]))

return features

X\_train = [extract\_features(frames) for frames in X\_train]

X\_test = [extract\_features(frames) for frames in X\_test]

# Обучение модели SVM

clf = SVC()

X\_train\_flattened = []

y\_train\_flattened = []

for X\_frames, y\_label in zip(X\_train, y\_train):

X\_train\_flattened.extend(X\_frames)

y\_train\_flattened.extend([y\_label] \* len(X\_frames))

clf.fit(X\_train\_flattened, y\_train\_flattened)

# Чтение и извлечение признаков тестового видео

test\_video\_frames = read\_video("test\_video.mp4")

test\_video\_features = extract\_features(test\_video\_frames)

# Предсказание классов для тестового видео

predictions = clf.predict(test\_video\_features)

# Вывод результатов

for prediction in predictions:

if prediction == 0:

print("Real")

else:

print("Deepfake")

# Параметры модели

parameters = [

{"kernel": "linear", "C": 1.0},

{"kernel": "rbf", "C": 1.0, "gamma": "scale"},

{"kernel": "poly", "C": 1.0, "degree": 3}

]

# Создание таблицы результатов

results = []

# Обучение и оценка модели для каждого параметра

for params in parameters:

clf = SVC(\*\*params)

X\_train\_flattened = []

y\_train\_flattened = []

for X\_frames, y\_label in zip(X\_train, y\_train):

X\_train\_flattened.extend(X\_frames)

y\_train\_flattened.extend([y\_label] \* len(X\_frames))

clf.fit(X\_train\_flattened, y\_train\_flattened)

X\_test\_flattened = []

y\_test\_flattened = []

for X\_frames, y\_label in zip(X\_test, y\_test):

X\_test\_flattened.extend(X\_frames)

y\_test\_flattened.extend([y\_label] \* len(X\_frames))

y\_pred = clf.predict(X\_test\_flattened)

accuracy = accuracy\_score(y\_test\_flattened, y\_pred)

results.append({

"Params": params,

"Accuracy": accuracy

})

# Вывод таблицы результатов

for result in results:

print("Params:", result["Params"])

print("Accuracy:", result["Accuracy"])

print()