Детектор ИИ-подделок голоса

Защита от мошеннических атак на основе подмены голоса (голосовых дипфейков)

Детектор представляет собой мобильное приложение для предупреждения о возможном использовании собеседником целевых подделок голосов. Программа анализирует спектральные и статистические метрики для выявления математических зависимостей, сопровождающих процесс генерации искаженной речи на основе голоса конкретного человека.

ЦЕННОСТНОЕ ПРЕДЛОЖЕНИЕ

Детектор предупреждает о мошеннических атаках с подменой голоса в режиме реального времени во время телефонного звонка. Для работы детектора не требуется высокоскоростное подключение к интернету и установка ресурсоемких приложений

ОБЛАСТИ ПРИМЕНЕНИЯ

- Сотовая связь: детекция подделки голоса в режиме разговора
- Мессенджеры: детекция нарушений аутентичности голосовых аудиозаписей
- Мобильные операционные системы: усиление встроенных мер безопасности

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА

- Низкие требования к вычислительным ресурсам (не используются нейросетевые модели)
- Не требуется стабильное соединение с 4G для передачи мобильных данных во время телефонного разговора
- Скорость: предупреждение формируется за 2 секунды (и менее), в том числе в режиме разговора

СТАДИЯ РАЗРАБОТКИ

Разработан программный комплекс на Python 3.10 с пятью модулями:

- подготовка метаданных
- извлечение признаков (MFCC, CQCC, ZCR, LPC-остаток)
- обучение GMM
- оценка метрик
- визуализация

Программный комплекс испытан в лабораторном окружении на данных, близких к реальным

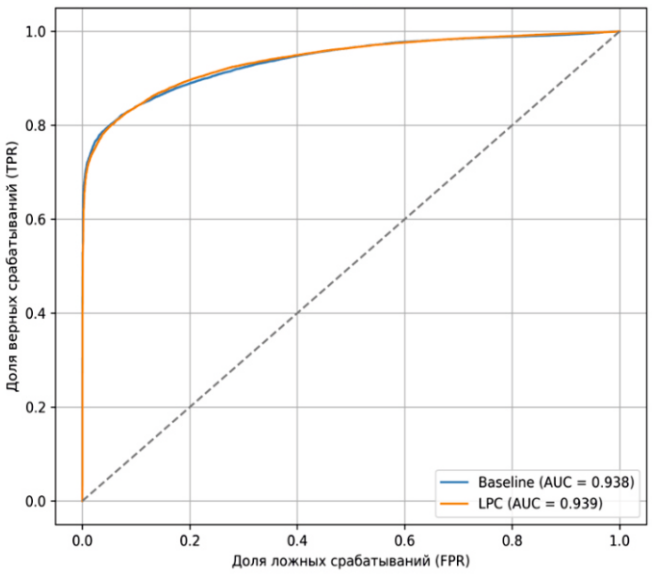
ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Пользовательские характеристики:

- время детекции: 2 сек.
- точность верификации речи, созданной ИИ: 93,9%

Требования к архитектуре:

- для десктопного использования – минимально CPU 2 GHz Quad–Core Intel Core i5
- для мобильного использования – CPU архитектуры ARM



ROC-кривые моделей обнаружения подмены голоса