Web-сервис тестирования алгоритмов компьютерного зрения на наличие уязвимостей к генеративным состязательным воздействиям

Выявление возможностей взлома алгоритмов компьютерного зрения с помощью специально искаженных изображений

Web-сервис производит автоматическое тестирование интеллектуальной системы на уязвимость к состязательным атакам через предоставленное API путем генерации для них состязательных примеров.

ЦЕННОСТНОЕ ПРЕДЛОЖЕНИЕ

Повышение безопасности использования алгоритмов компьютерного зрения за счет автоматического аудита их уязвимости

ОБЛАСТИ ПРИМЕНЕНИЯ

- Производство автономного транспорта
- Промышленные предприятия с роботизированными системами на основе компьютерного зрения
- Производители и пользователи камер с функциями распознавания лиц и поиска объектов
- Системы навигации

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА

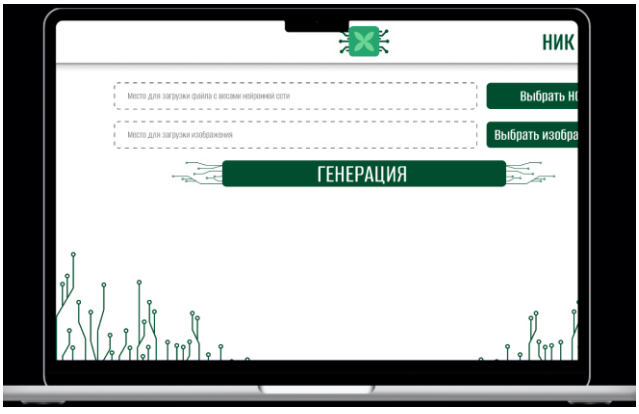
- Экономия на аппаратном обеспечении благодаря проведению тестирования на стороне сервера
- Отсутствие требований к знаниям программирования со стороны пользователя

СТАДИЯ РАЗРАБОТКИ

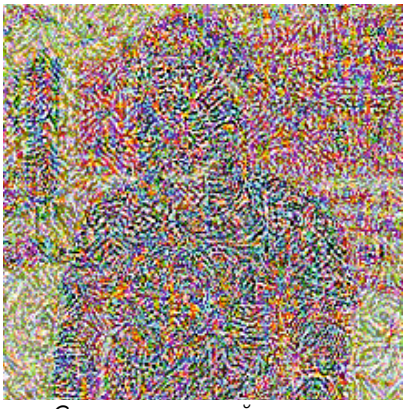
- Разработан пользовательский интерфейс, backend-части сервиса, реализованы и подключены алгоритмы генеративных атак
- Проведено комплексное тестирование

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Язык разработки: python3
- Поддерживаемые модели форматов torch, семейств YOLO и ResNet
- Реализовано более 40 алгоритмов атак
- Личный кабинет пользователя с историей генераций



Страница генерации состязательных примеров



Состязательный пример для проведения тестирования нейронной сети

ПРАВОВАЯ ОХРАНА

Свидетельство о государственной регистрации программы для ЭВМ №2025683406 «Программа для анализа уязвимости нейросетевых моделей YOLO к атаке Fast Sign Gradient Method»