

Разработка программного инструмента для обнаружения модификаций цифровых фотографий

Выполнила: Игнатенко Татьяна Андреевна

Руководитель: Власов Владимир Николаевич, к.ф.м.-н., доцент, КОИ ФИТ НГУ

Консультант: Авдюшенко Александр Юрьевич, к.ф.м.-н., аналитик, ООО “Яндекс”

Актуальность

Широкая доступность мощных фоторедакторов дает возможность почти каждому вносить модификации в фотографии.

Нередко такой возможностью **злоупотребляют с целью повышения доверия к ложной информации, распространяющейся в сети.**



Создание ложного впечатления о политических лидерах



Илиас Меркури @imerkouri · 8 июл.

Масштаб личности



111 359 693

Модифицированное



Оригинал

Демонстрация ложного технического превосходства



Модифицированное



Оригинал

Актуальность

Для поддержания верной картины мира людям необходим инструмент, позволяющий определять присутствие модификаций на фотографиях.

Существующие инструменты

Инструменты, которые ставят изображению вердикт

Используют примитивные методики анализа изображений, которые **выдают много ложных результатов.**

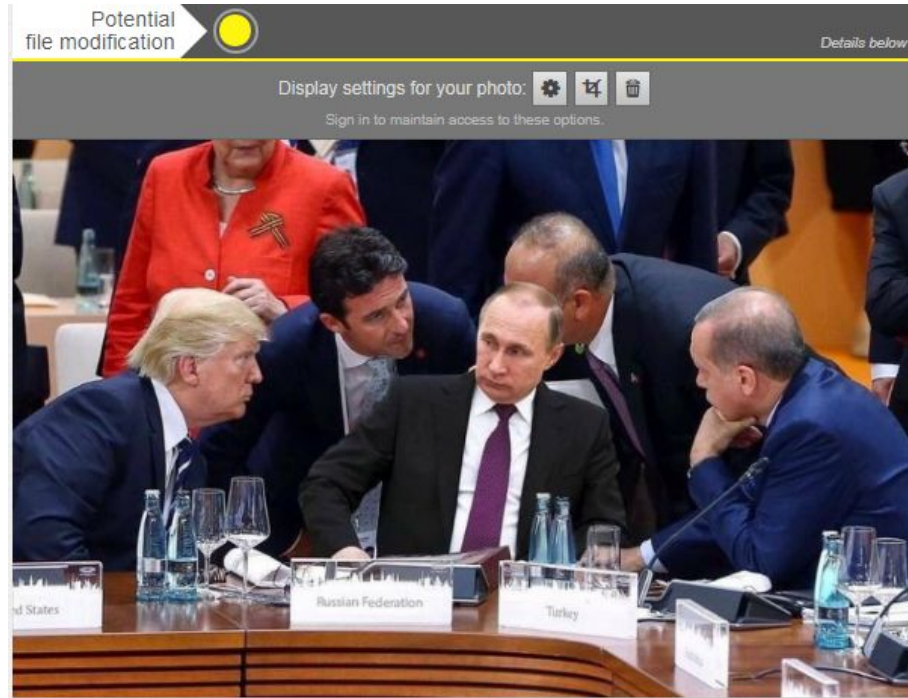
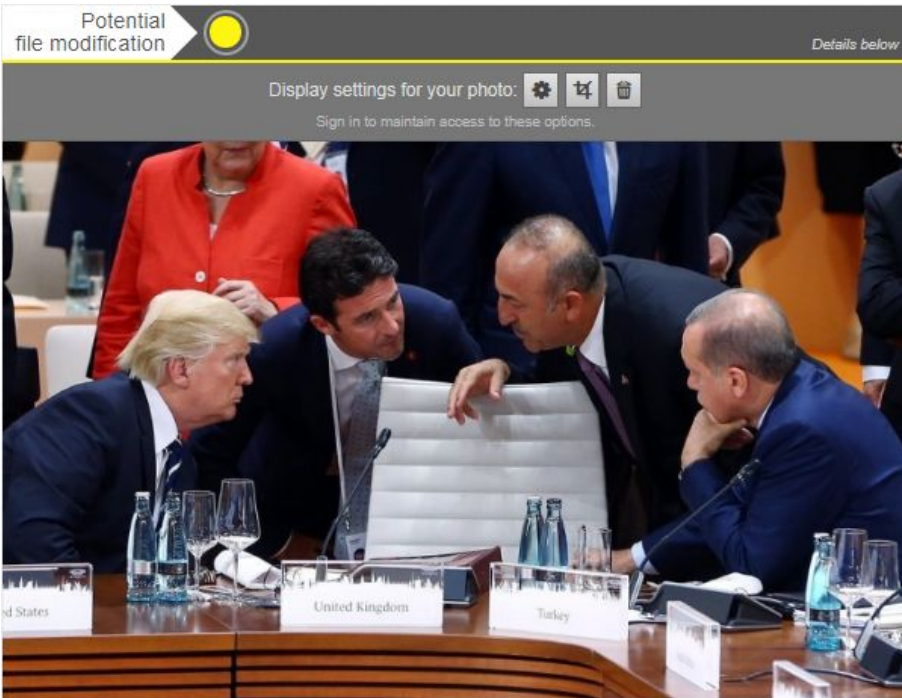
Примеры таких инструментов:

- izitru?
- Image Edited?
- Picture manipulation inspector

izitru?

Potential file modification

Our forensic tests suggest this file has been re-saved since initial capture. Because this file is not a camera original, it is possible that it was modified.

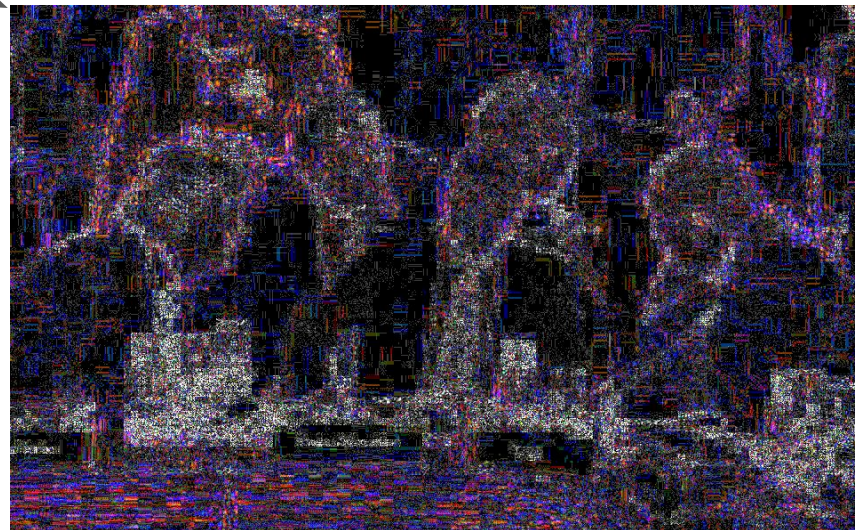
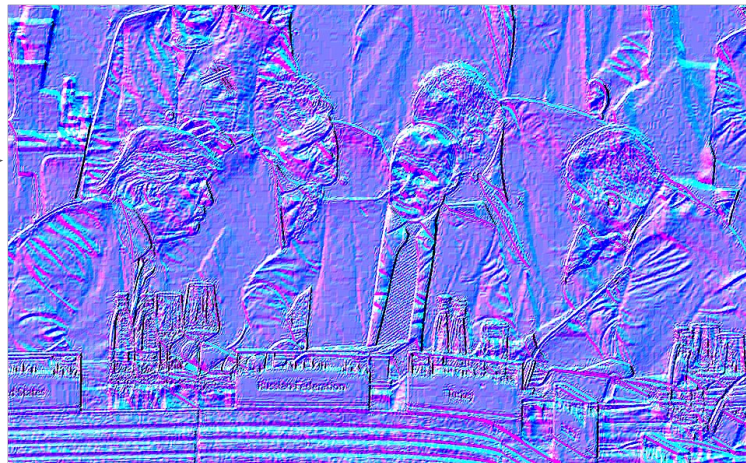


Инструменты, которые не ставят вердикт

Используют продвинутые методики, позволяющие человеку, анализирующему их результаты, с бóльшей вероятностью обнаружить модификацию, но **требуют специальных знаний и большого опыта для успешного применения.**

Примеры таких инструментов:

- Image forensic
- Fotoforensics
- Forensically





Цель

Разработать инструмент, **с высокой точностью** определяющий наличие “вставки” на фотографии, результаты работы которого **понятны неспециалистам.**



Решение

Реализовать инструмент, который будет **выдавать вердикт** на основании интерпретации результатов **“продвинутых” методов.**

Машинное обучение



```
graph TD; A[Машинное обучение] --> B[Классические методы]; A --> C[Нейросетевые методы]
```

Классические методы

(SVM, RF, метод k-ближайших соседей и др.)

Нейросетевые методы

(полносвязные, сверточные и рекуррентные нейросети)

Машинное обучение

Сверточные нейронные сети:

- учитывают пространственную близость пикселей
- показывают лучшие результаты в области анализа изображений
- не требуют feature engineering (выделения признаков объектов)
- имеют меньше весов, чем полносвязные сети

Формирование обучающей выборки

→ Использован набор данных CASIA v2.0



Со вставкой



Без вставки

Формирование обучающей выборки

→ Для сбалансированности выборки был написан генератор модификации “вставка”

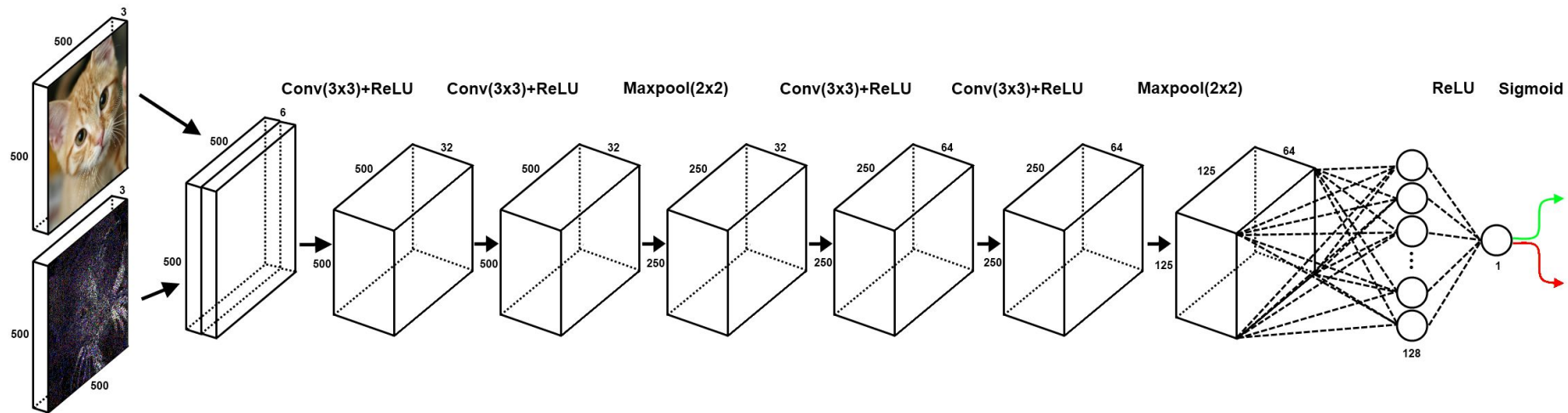


Со вставкой



Со вставкой

Архитектура нейронной сети



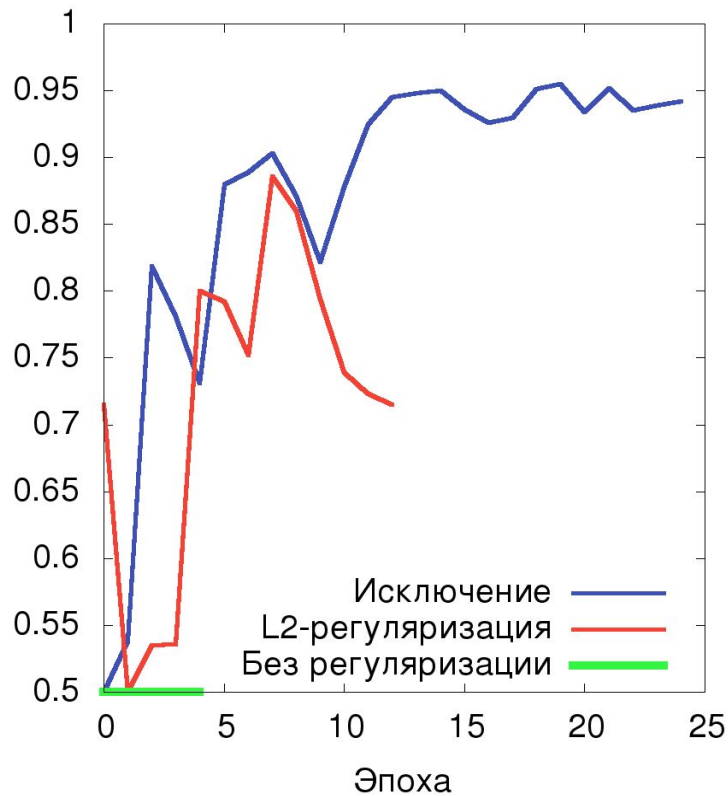
Настройка нейронной сети

Настройки нейронной сети

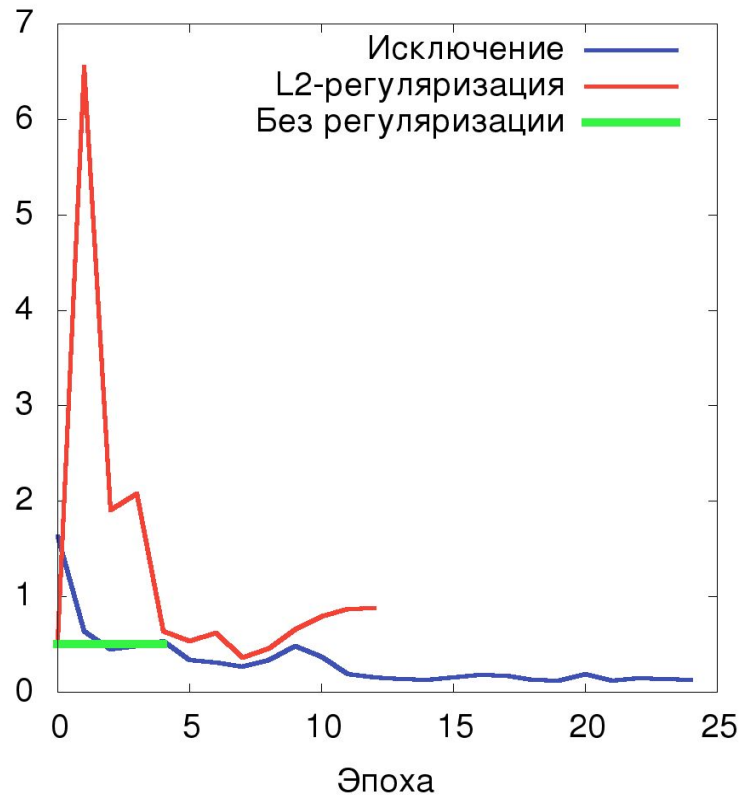
- Нормализация входных данных
- Инициализация сети

Борьба с переобучением

Точность

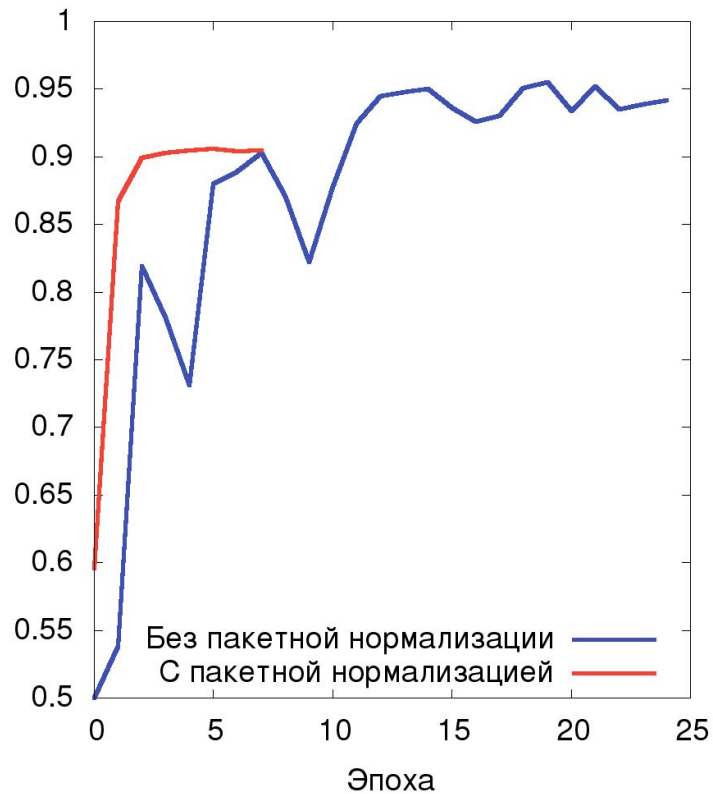


Значение функции потерь

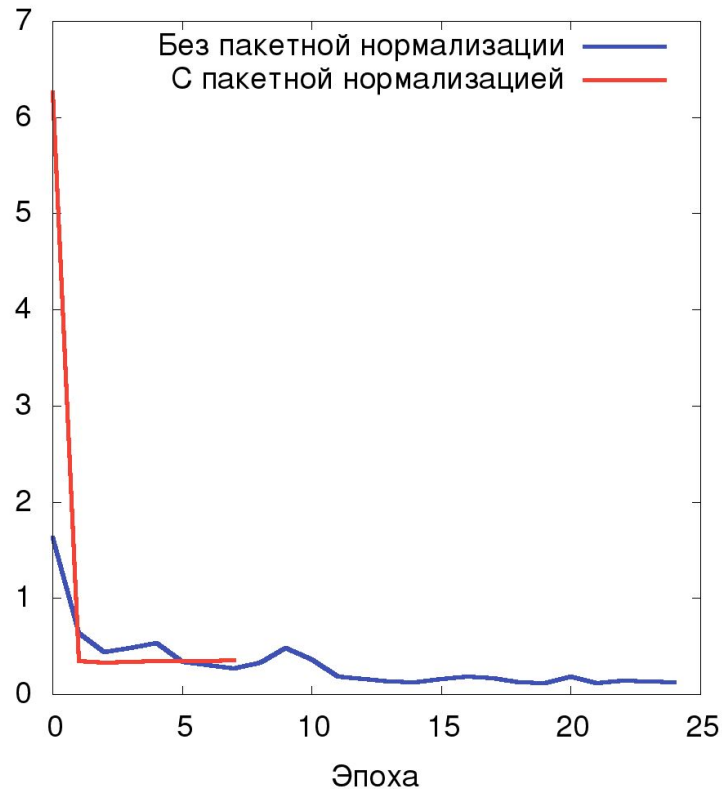


Ускорение обучения

Точность



Значение функции потерь



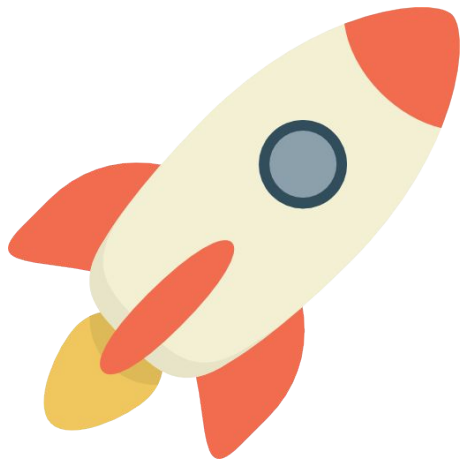
Реализация веб-интерфейса





Точность итоговых предсказаний

Точность 84.3% была получена на контрольной выборке, состоящей из 1000 фотографий.



Дальнейшие планы

- Реализовать плагин для браузеров Google Chrome, Mozilla Firefox
- Добавить возможность выделять области вставки на изображении



Апробация

Диплом I степени на МНСК-2018:
Технологии искусственного интеллекта

Список публикаций

Игнатенко Т.А. Инструмент для определения наличия модификаций вида “вставка” на цифровых фотографиях //Материалы 56-й Международной научной студенческой конференции МНСК-2018: Информационные технологии/ Новосиб. гос. ун-т. – Новосибирск, 2018. – Тезисы