**УДК 004.932.2**

# МЕТОД УЛУЧШЕНИЯ ОБНАРУЖЕНИЯ АТАК ПРЕЗЕНТАЦИИ НА БИОМЕТРИЧЕСКУЮ СИСТЕМУ РАСПОЗНАВАНИЯ ЛИЦ С ПОМОЩЬЮ СВЕРТОЧНОЙ СЕТИ С МЕХАНИЗМОМ ВНИМАНИЯ

***Пикуль А.С.***[1] *(студент)*

*1 – Университет ИТМО*

*e-mail: aleksandrpikul134@gmail.com*

Предложен новый подход для улучшения распознавания атак презентации на биометрическую систему распознавания лиц с помощью сверточной сети с механизмом внимания. Проверена центральная гипотеза, которая заключалась в том, что с помощью механизма внимания возможно улучшить результаты работы исходной сверточной нейронной сети. В ходе экспериментов гипотеза была подтверждена. Наибольший прирост по качеству был достигнут на наборе данных NUAA – до внедрения механизма внимания в сверточную сеть ACER = 10,858%, после внедрения механизма внимания ACER = 7,028%.

**Ключевые слова**

Сверточные нейронные сети, механизм внимания, биометрия, презентационная атака, обнаружение атак презентации.

Глубокие нейронные сети можно разделить на три основные концепции: сверточные нейронные сети; рекуррентные нейронные сети; механизмы внимания.

Наиболее применимым подходом в обработке изображений на данный момент являются сверточные нейронные сети. Тем не менее данный подход уже не является наиболее развивающимся.

На сегодняшний день механизмы внимания становятся наиболее перспективным методом из-за значительных достижений сначала в области машинного перевода, а затем в обработки изображений. При работе с изображениями такая архитектура позволяет сети выделять наиболее важные для принятия решения области. Пример карты внимания на рисунке 1 [1].

Рис. 1. Пример карты внимания

Концепции глубоких нейронных сетей можно комбинировать между собой.

Рассмотрим сверточную нейронную сеть ResNet-18 (рис. 2 [2]). Ее архитектуру можно условно разделить на 4 блока – это блоки conv_layers1, conv_layers2, conv_layers3 и conv_layers4. На выходе каждого из блоков можно извлечь карты характеристик. При этом от блока к блоку карты характеристик передаются в необработанном виде.

Идея состоит в том, чтобы, получая карты характеристик, дополнительно обрабатывать их механизмом внимания, а выход передавать на вход очередного сверточного слоя.

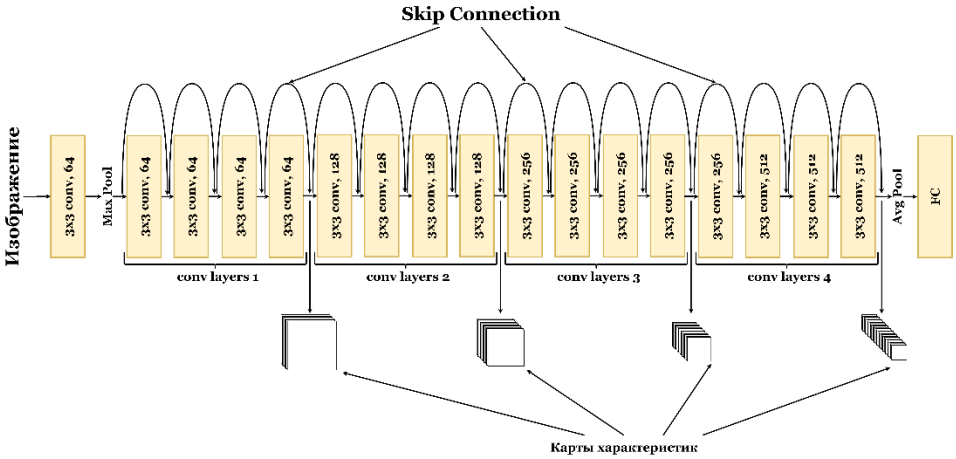



Рис. 2. Сверточная нейронная сеть ResNet-18

Существуют разные способы реализации механизма внимания. Наиболее простой вариант – однослойная нейронная сеть (рис. 3). На вход механизма внимания подается тензор, который извлекается после сверточного слоя. Извлеченный тензор проходит через блок внимания и передается на очередной блок свертки.

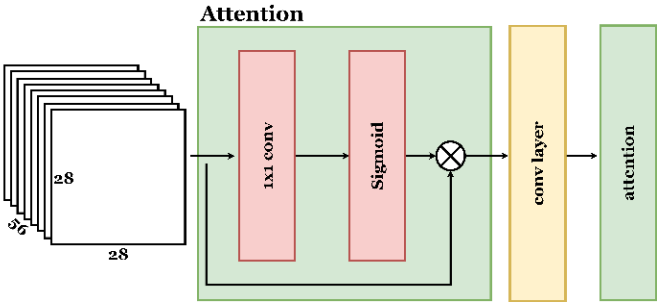



Рис. 3. Простейший механизм внимания

В результате получается следующая архитектура (рис. 4): на вход подается изображение лица. Полученное изображение обрабатывается сначала слоем свертки, затем слоем внимания. Для ResNet-18 эти шаги повторяются еще три раза для трех оставшихся карт характеристик, полученных после слоев свертки. Для принятия решения функция активации сигмоида выдает вероятность. Полученная вероятность сравнивается с заранее заданным порогом. Если полученная вероятность больше заданного порога, то считаем, что на входе был живой человек, если меньше, то на входе была атака презентации.

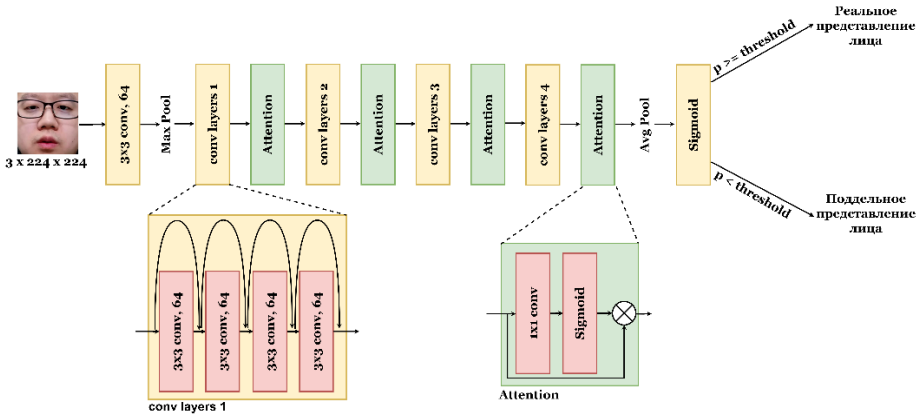



Рис. 4. Предложенная архитектура

Для обучения предложенной архитектуры применялись две базы данных: LCC-FASD (табл. 1 [3]) и NUAA (табл. 2 [4]).

Таблица 1

**Количество образцов в наборе данных LCC-FASD**

| | Оригинал | Подделка |
|---|---|---|
| Обучение | 1553 | 13508 |
| Тестирование | 389 | 3377 |

Таблица 2

**Количество образцов в наборе данных NUAA**

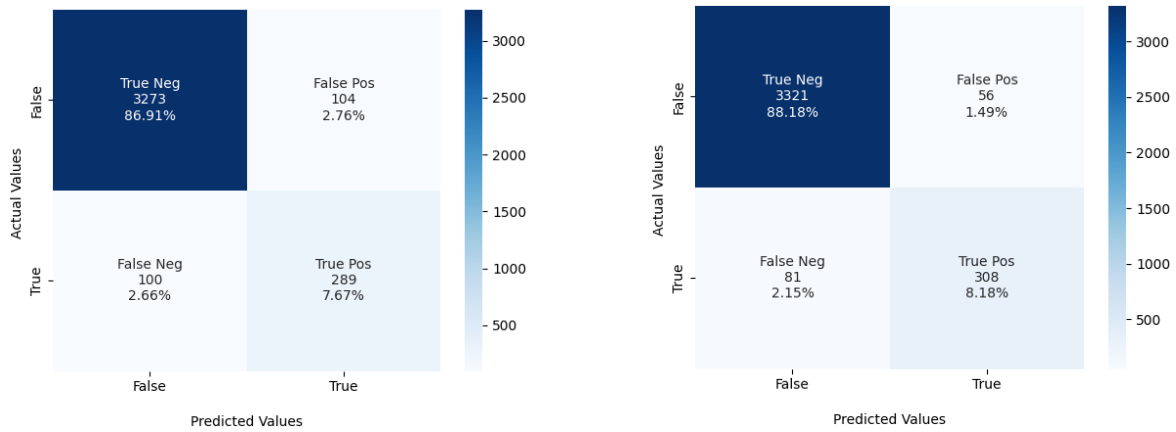
| | Оригинал | Подделка |
|---|---|---|
| Обучение | 1743 | 1748 |
| Тестирование | 3362 | 5761 |

Оценка качества производилась по трем метрикам: матрица рассеяния, ROC-кривая и ACER. Чем больше значение ROC-кривой и меньше значение ACER, тем лучше происходит распознавание атаки.

Гипотезу можно сформулировать следующим образом – действительно ли механизм внимания позволит улучшить результат распознавания для исходной сверточной нейронной сети. Тестирование проводилось в два этапа: тестирование ResNet-18 без механизма внимания и тестирование ResNet-18 с механизмом внимания.

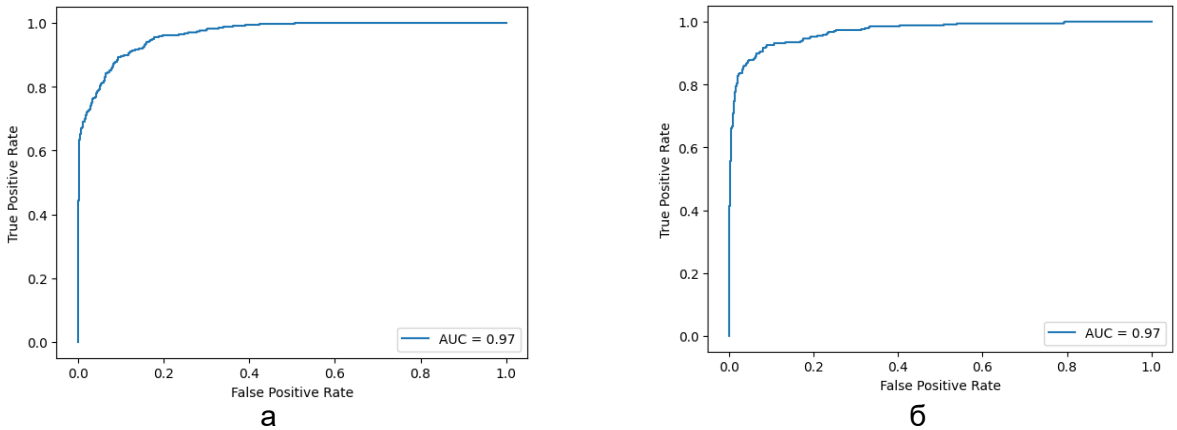
В ходе проведения экспериментов были получены следующие результаты.

1) На наборе данных LCC-FASD:




а б

Рис. 5. Матрица рассеяния для LCC-FASD: а) ResNet-18, б) ResNet-18 + механизм внимания




а б

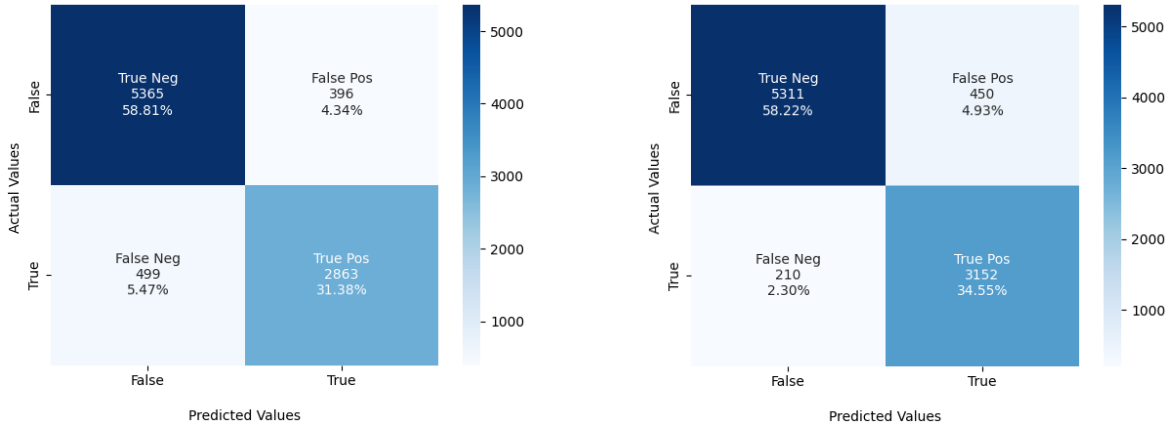
Рис. 6. ROC-кривая для LCC-FASD: а) ResNet-18, б) ResNet-18 + механизм внимания

Таблица 3

**ACER на наборе данных LCC-FASD**

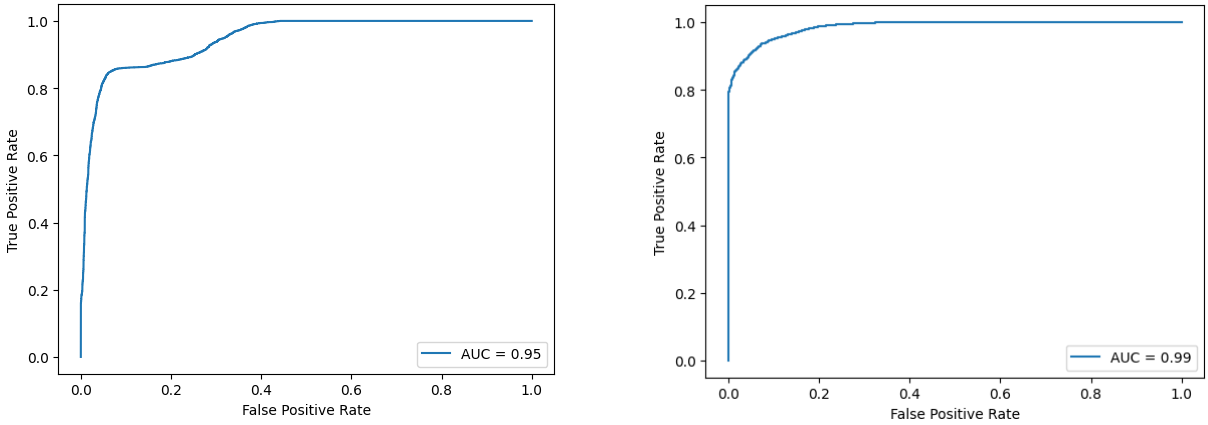
| | ResNet-18 | ResNet-18 + механизм внимания |
|---|---|---|
| ACER, % | 14,393 | 11,240 |

2) На наборе данных NUAA:




а б

Рис. 7. Матрица рассеяния для NUAA: а) ResNet-18, б) ResNet-18 + механизм внимания




а б

Рис. 8. ROC-кривая для NUAA: а) ResNet-18, б) ResNet-18 + механизм внимания

Таблица 4

**ACER на наборе данных NUAA**

| | ResNet-18 | ResNet-18 + механизм внимания |
|---|---|---|
| ACER, % | 10,858 | 7,028 |

При тестировании на наборе данных LCC-FASD было достигнуто уменьшение ошибки распознавания по метрике ACER на 3,153%. На NUAA – на 3,83%. Это означает, что результаты относительно обычного ResNet-18 были улучшены, следовательно, исходная гипотеза подтвердилась – с помощью механизма внимания возможно улучить работу исходной сверточной нейронной сети.

**Список использованных источников**

1. Visual Attention Network. [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2202.09741 (дата обращения 13.02.2024).
2. Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun. Deep Residual Learning for Image Recognition // 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – CVPR, 2016.

3. Large Crowdcollected Face Anti-Spoofing Dataset. [Электронный ресурс]. – Режим доступа: https://csit.am/2019/proceedings/PRIP/PRIP3.pdf (дата обращения 13.02.2024).
4. Xiaoyang Tan, Yi Li, Jun Liu, Lin Jiang. Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model // Computer Vision–ECCV, 2010.