|  |  |
| --- | --- |
| **СОГЛАСОВАНО**  Доцент кафедры  ИАНИ ННГУ, к.ф.-м.н.  \_\_\_\_\_\_\_\_\_\_\_\_\_ Д.А. Яшунин  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2019 г. | **УТВЕРЖДАЮ**  Профессор кафедры  ИАНИ ННГУ, д.т.н.  \_\_\_\_\_\_\_\_\_\_\_\_\_ Н.В. Старостин  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2019 г. |

**Пояснительная записка №3**

**«По антиспуфингу по RGBD»**

**ОКР «Разработка и реализация программного обеспечения для обнаружения и распознавания лиц с использованием RGBD камеры»**

**(Шифр ПО «DeepFR»)**

**Н. Новгород**

**2019**

**Обзор Anti-spoofing методов по RGB-D изображениям**

*Spoofing или Presentation Attack (PA)* - попытка представиться владельцем биометрических данных используя артефакты, позволяющие обмануть биометрическую систему.

*Распространенные виды PA систем распознавания лица:*

* Print attack - использование распечатки лица владельца биометрических данных на бумаге
* Replay attack - использование изображения владельца снятого на камеру (фото, видео)
* Mask attack - использование 3D маски лица

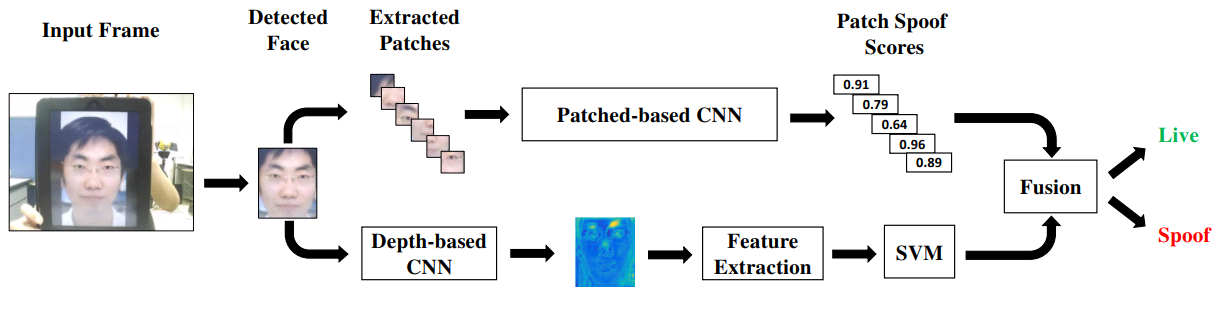
*Anti-spoofing (PA detection)* - система, которая должна распознавать приведенные выше типы атак с максимальной точностью перед тем как идентифицировать лицо. Известные подходы anti-spoofing методов:

* Анализ текстуры - выделение характеристик текстуры, присущих лишь PA. Довольно сложно реализовать из-за отсутствия явной корреляции по пиксельного RGB кода и особенностями текстуры.
* Анализ движения - выделение особенностей поведения. Не пригоден для frame anti-spoofing, не способен к детекции PA в виде видео владельца биометрических данных.
* Анализ качества изображения - выделение особенности эффектов, возникающих при повторном отображении: шумы, муар, блики, и.т.д. Подходит для выявления replay attack.
* Анализ глубины изображения - выделение особенностей глубины RGB-D изображений. Позволяет детектировать плоские PA, такие как print attack, replay attack.

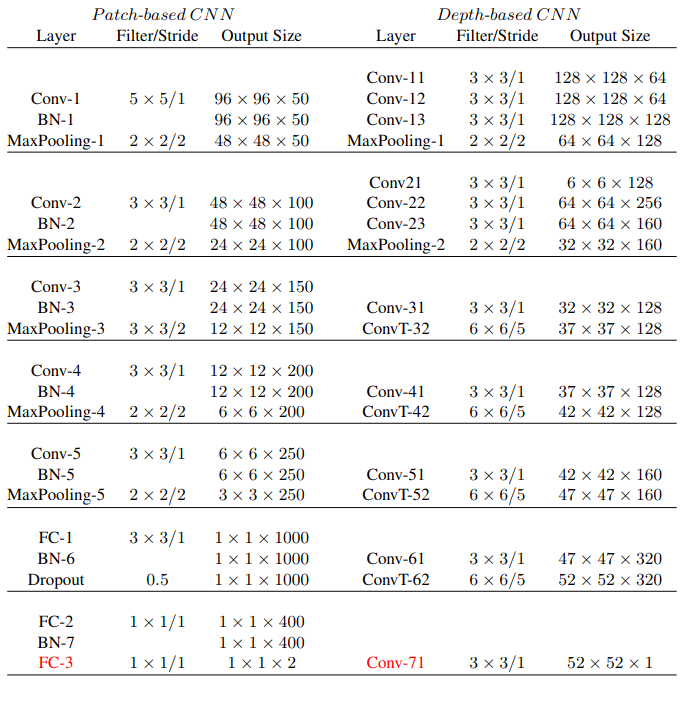
**Face Anti-Spoofing Using Patch and Depth-Based CNNs** [1]

Двух потоковый метод для распознавания print и replay атак. Каждый поток основан на сверточной нейросети. Один поток извлекает локальные характеристики изображения (патчи), не анализируя все лицо. Второй анализирует характеристики глубины всего изображения, с целью выработать паттерны 3D-модели изображения лица, соответствующего spoof-атаке. Затем слияние двух показателей подается на вход бинарному классификатору **life-spoof**.

*High Level Design:*

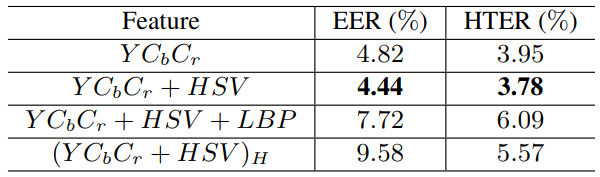


*CNNs structure:*



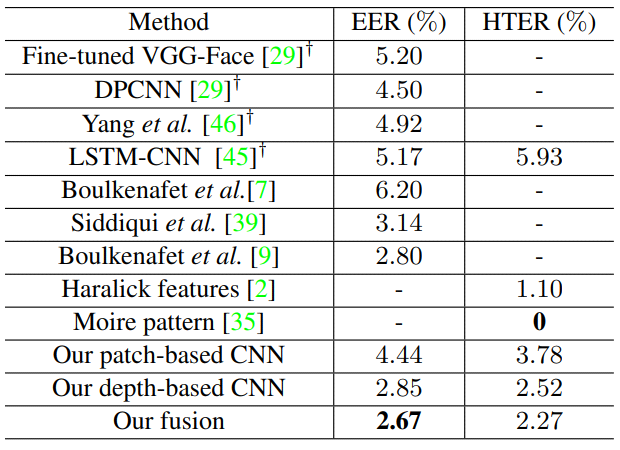
* Красным помечены выходные слои сетей
* После каждого слоя свертки идет слой ReLU
* Размер входных данных Patch CNN 96х96
* Размер входных данных Depth CNN переменный от сэмпла к сэмплу(в таблице пример для 128х128) //???

*Показатели производительности Patch CNN с разными типами входных векторов (CASIA-FASD dataset):*

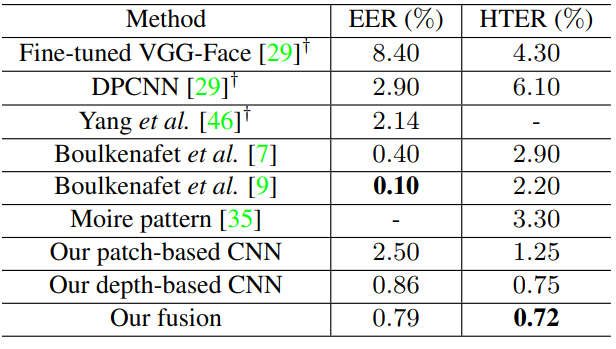


Результаты:

* CASIA-FASD dataset:



* Replay-attack dataset



* MSU-USSA dataset

