|  |  |
| --- | --- |
|  | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |

ФАКУЛЬТЕТ **Информатика и системы управления**

КАФЕДРА **Компьютерные системы и сети (ИУ6)**

НАПРАВЛЕНИЕ ПОДГОТОВКИ **09.04.01 Информатика и вычислительная техника**

МАГИСТЕРСКАЯ ПРОГРАММА **09.04.01/07 Интеллектуальные системы анализа, обработки и интерпретации больших данных**

**Отчет**

|  |  |
| --- | --- |
| **по лабораторной работе №** | 2 |

**Название:** Выявление логических закономерностей по данным мониторинга

**Дисциплина:** Дистанционный мониторинг сложных систем и процессов

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Студент | ИУ6-12М |  |  | С.В. Астахов | |
|  | (Группа) |  | (Подпись, дата) | | (И.О. Фамилия) |
|  |  |  |  | |  |
| Преподаватель |  |  |  | | Ю.А. Вишневская |
|  |  |  | (Подпись, дата) | | (И.О. Фамилия) |

Москва, 2023

# **1. Методы распознавания дипфейков**

Очевидно, что прежде, чем приступить к разработке системы распознавания дипфейков, необходимо произвести сравнительный анализ существующих методов обнаружения дипфейков. Приведенная ниже классификация методов составлена на основе статьи инженерно-исследовательского центра цифровой криминалистики [1].

## **1.1. Методы на основе нейросетей**

Так, как нейросети являются довольно универсальной и относительно простой в конфигурации математической моделью ИИ, не требующей предобработки данных, первые алгоритмы определения дипфейков использовали именно их. Такие модели обрабатывают предоставленное видео в покадровом режиме, оценивают вероятность появления дипфейка в каждом кадре и затем обобщают полученные результаты для всего видео. В этой группе можно выделить две подгруппы: модели на основе трансферного обучения и специально созданные нейросети.

Трансферное обучение — технология, позволяющая уменьшить набор данных, необходимый для тренировки глубокой нейросети, за счет использования предварительно подготовленной сети, обученной на другом наборе данных, но выполняющей задачу, аналогичную требуемой [2].

Пример применения такого подхода: необходимо обучить нейросеть классифицировать изображения еды. Пусть, при этом, существует уже обученная нейросеть для классификации изображений животных. В сети для классификации животных более глубокие слои будут отвечать за определение общих паттернов, необходимых для дальнейшего “понимания” изображений (например, определение форм и границ предметов). Необходимо будет лишь заменить и обучить самые верхние слои сети, которые буду отвечать за интерпретацию промежуточных результатов (например, определять по геометрической форме тип животного или блюда). Иллюстрация работы технологии трансферного обучения приведена на рисунке 1.

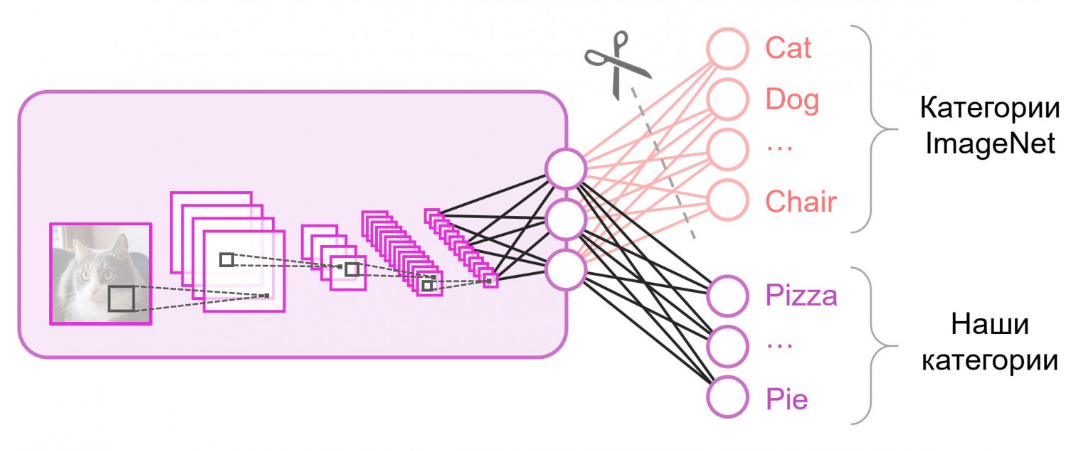


Рисунок 1 — использование технологии трансферного обучения

Примером применения трансферного обучения для решения задачи определения дипфейков является нейросеть, полученная учеными из Мэрилендского университета (рисунок 2) [3].

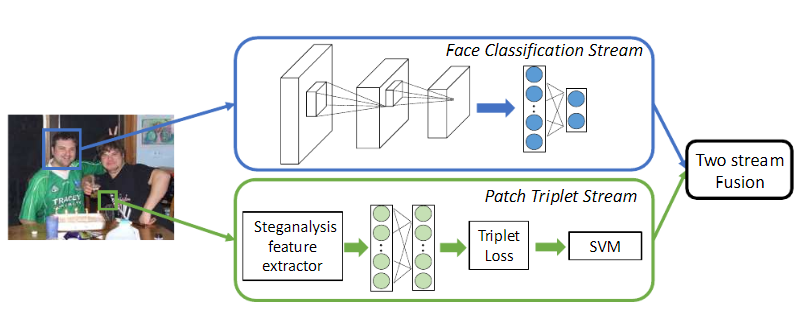


Рисунок 2 — применение трансферного обучения для задачи определения дипфейков

В представленной модели есть два параллельных потока обработки изображения, результаты которых объединяются лишь на самой последней фазе. Верхний поток основывается на методе трансферного обучения на основе нейросети, натренированной для классификации человеческих лиц. Этот поток работает с такой информацией, как, например, форма и геометрия лица. Нижний же поток ищет более скрытые закономерности и артефакты, такие, как локальные изменения уровня зашумленности изображения.

Альтернативой трансферному обучению является разработка собственных архитектур нейросетей. Примером такой сети может быть система, разработанная в Национальном институте информационных и коммуникационных технологий Японии [4].

Схема их разработки представлена на рисунке 3. Сначала изображение обрабатывается предобученной сверточной нейросети VGG-19 [5]. На данном этапе, как и в случае трансферного обучения, целью является выделение базовых паттернов в изображении. Затем данные передаются в капсульную нейросеть, которая анализирует изображение на более высоком уровне (рисунок 3).

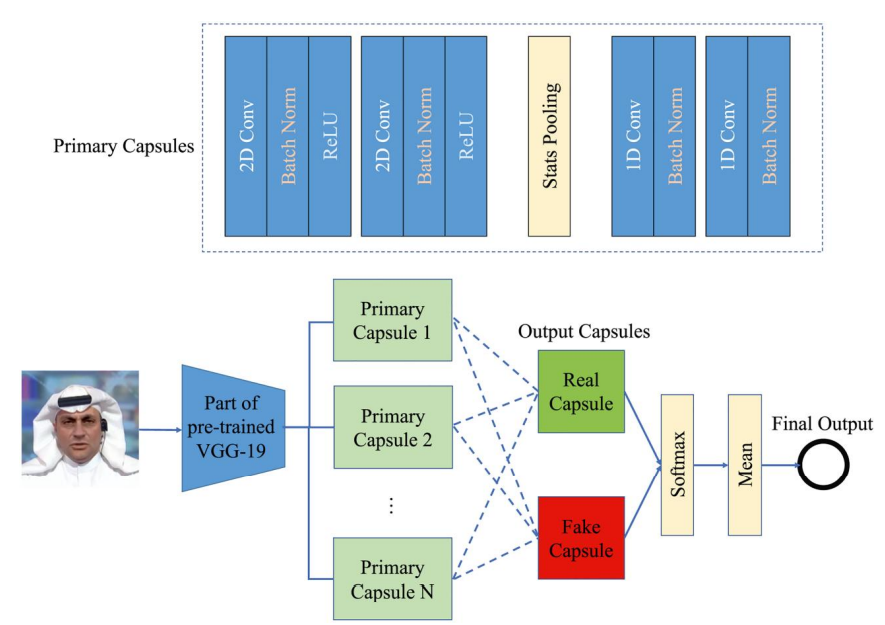


Рисунок 3 — структура системы обнаружения дипфейков с использованием капсульной нейросети

Капсулы используются для представления объектов или их частей, которые затем объединяются для формирования более высокоуровневых представлений. Капсулы - это группы нейронов, которые кодируют свойства объекта, такие как его положение, ориентация и размер, а также вероятность того, что объект присутствует. Капсулы разработаны таким образом, чтобы быть эквивариантными, то есть они могут распознавать объект независимо от его положения или ориентации. Капсульные сети показали свою эффективность в улучшении точности задач распознавания изображений, особенно в случаях, когда объекты затенены или имеют несколько ориентаций [6].

## **2.1. Методы, основанные на временной согласованности**

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. <https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/bme2.12031>
2. <https://habr.com/ru/companies/binarydistrict/articles/428255/>
3. <https://www.researchgate.net/publication/319284586_Two-Stream_Neural_Networks_for_Tampered_Face_Detection>
4. <https://arxiv.org/pdf/1810.11215.pdf>
5. <https://arxiv.org/pdf/1409.1556v1.pdf>
6. https://neurohive.io/ru/osnovy-data-science/kapsulnaja-nejronnaja-set-capsnet/