УДК 004.932.2

КЛАСТЕРИЗАЦИЯ ИЗОБРАЖЕНИЙ ДЛЯ ДОМЕННОГО ОБОБЩЕНИЯ В ЗАДАЧЕ ЛИЦЕВОГО АНТИСПУФИНГА

Мещеряков И.Д. (Университет ИТМО), **Бузин А.Э.** (ООО “ЦРТ-Инновации”)
Кабаров В.И. (Университет ИТМО)
Научный руководитель – к.т.н. Шуранов Е. В.
(Университет ИТМО)

Аннотация

В данной работе исследовалось явление доменного обобщения и его влияние на обучение модели лицевого антиспуфинга. В работе для решения задачи доменного обобщения рассмотрен подход одностороннего доменного обобщения. Исследуются 2 подхода к решению задачи – с помощью классических алгоритмов кластеризации и с помощью кластеризации через вариационные автоэнкодеры. Данные подходы сравниваются с бейзлайном архитектуры одностороннего доменного обобщения по набору метрик для валидационных наборов данных.

Введение

Из-за большой вариативности условий сбора данных, таких как различный фон, условия освещения, разрешение и тип камеры, состав актеров и т.д., модели машинного обучения, используемые в качестве детекторов атак, обычно не могут быть обобщены на новые наборы данных. Домен – определенный набор условий сбора данных. Отличительные признаки, используемые для обнаружения «Spoof» данных, для разных доменов выглядят по-разному, что сильно мешает обобщающей способности глубоких нейронных сетей. Например, для одних открытых наборов данных характерны края изображений, демонстрируемых камере, а для других в целом более тусклые цвета для образцов класса «Live» чем для образцов класса «Spoof». Если модель обучается на простом, но эффективном признаке (например, тусклые цвета или края изображения), то мы не можем использовать её для данных, собранных при других условиях.

Основная часть

Задача доменного обобщения – это задача обучения нейронной сети на определенном количестве доменов таким образом, чтобы ее результаты были применимы к другим доменам (или фактически не зависели от них). Один из подходов решения данной задачи – обучение модели с применением архитектуры одностороннего доменного обобщения [1]. Основная идея данного подхода состоит в том, чтобы обучить модель на обобщенное пространство признаков, где распределение «Live» данных компактно, в то время как распределение «Spoof «данных распределено по доменам, но компактно внутри каждого из доменов. Для применения данного подхода необходимо произвести «доменную разметку», то есть каждому набору данных соотнести определенный домен. В данной работе рассматривается гипотеза, согласно которой одному набору данных может соответствовать только один домен. Для доменной разметки рассматривались 2 способа – классические алгоритмы кластеризации и кластеризация через вариационные автоэнкодеры [2].

Для исследования классических алгоритмов кластеризации были выбраны 3 типа характеристик: характеристики лица (наличие лицевых аксессуаров и лицевых отличительных признаков, состояния рта и глаз, углы поворотов лица и т.д.), характеристики изображения (блики (засвет изображения), равномерность освещения лица, количество света, который попал на матрицу при съемке, плотность оттенков серого и резкость изображения), характеристики медиафайла (разрешение файла, вид компрессии, размер лицевой ограничительной рамки и т.д.). Для проведения экспериментов рассматривались как предобработанные, так и не предобработанные метрики.

Среди классических алгоритмов кластеризации рассматривались смеси гауссовых распределений и алгоритм DBSCAN. Другие методы кластеризации не позволили выделить информацию о доменном сдвиге в пространстве признаков [3].

При кластеризации с помощью вариационных автоэнкодеров исследовалось обучение экстрактора признаков на основе нейронной сети, который переводил лица с фотографий из наборов данных в пространство эмбеддингов для автоэнкодера. Эмбеддинги использовались автоэнкодером для перевода в 3-мерное пространство с последующей кластеризацией. В частности, исследовалось влияние разных функций потерь (Softmax, AM-Softmax [4] и ArcFace [5]) при обучении экстрактора.

Полученные результаты

Исследование проводилось на 24 различных наборах данных – открытых и закрытых. Тестирование проводилось на 4 открытых наборах данных. Были проведены эксперименты с классическими алгоритмами кластеризации и вариационными автоэнкодерами.

Способ формирования доменной разметки с помощью классических алгоритмов кластеризации показал лучшее качество по метрике EER.

В качестве дальнейших исследований планируется рассмотреть более качественную предобработку признаков, извлечение дополнительных характеристик медиафайла и создание «предварительной» ручной доменной разметки на основе открытых наборов данных, что позволит перевести задачу из «обучение без учителя (unsupervised learning)» в «обучение с частичным привлечением учителя (semi-supervised learning)».

Список литературы

1. Jia Y, Zhang J, Shan S, Chen X. Single-side domain generalization for face anti-spoofing. InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2020 (pp. 8484-8493).
2. Cai J, Fan J, Guo W, Wang S, Zhang Y, Zhang Z. Efficient deep embedded subspace clustering. InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2022 (pp. 1-10).
3. Кластеризация изображений для доменной генерализации [Текст]: отчет о НИР; рук. Кабаров В.И., исполн. Мещеряков И.Д.
4. Wang F, Cheng J, Liu W, Liu H. Additive margin softmax for face verification. IEEE Signal Processing Letters. 2018 Apr 4;25(7):926-30.
5. Deng J, Guo J, Xue N, Zafeiriou S. Arcface: Additive angular margin loss for deep face recognition. InProceedings of the IEEE/CVF conference on computer vision and pattern recognition 2019 (pp. 4690-4699).