Stage 0: Adversarial attacks and anomaly detection in MIR

Vinod Subramanian, QMUL, ROLI Ltd.

Abstract

The abstract goes here.

Index Terms

MIR

I. Introduction

MUSIC Talk about large collections of data and where they are used. Then talk about issues and challenges that lead to anomaly detection as a solution. Then talk about challenges that lead to adversarial attacks and defenses as a solution.

II. Related Work

A. Anomaly detection

1) Summarize the survey paper on anomaly detection from 2007. This survey paper talks a lot about older approaches to anomaly detection that are still relevant
2) For mechanical failures there are deep learning aproaches for anomaly detection, mostly inspired by the fact that it is harder to define the anomaly.
3) Work done on anomaly detection in medicine to identify diseases from measurements automatically
4) Work done on anomaly detection on GTZAN dataset using classicalmachine learning and on mammal sound recognition

B. Adversarial attacks

1) Discovery of adversarial examples and the conclusion that the cause was non-linearity
2) Transferability of adversarial examples between models and datasets
3) Different defenses against the atttacks
4) Adversarial attacks in speech and music

III. Research questions and methods

A. Recreating adversarial attack experiments in audio

1) Transferring adversarial examples in audio between models with identical inputs
2) Can adversarial examples be played over the air
3) Can you create a universal perturbation that has a high chance of making an audio an adversarial example
4) Robustness of adversarial examples to different types of compression

B. Adversarial attacks for audio

1) Unlike computer vision audio domain uses different types of input features for deep learning. It would be interesting to see if it is possible to design an adversarial attack in the time domain that is robust to the different input representations
2) Design attacks for a specific task such as singing voice transcription. Singing voice transcription has a few different high accuracy models to work with so it is a good candidate to perform adversarial attacks on.

C. Defenses against attacks

1) Apply existing defenses to the audio problem to see if they work
2) Design defenses that are tailored to the specific tasks that I choose to work on
3) Explore the idea of using adversarial examples as a data augumentation technique to create higher accuracy models

D. Anomaly detection in note level datasets

1)

IV. Timeline

Table listing different projects, their timeline and targetted conferences

V. Conclusion

Summarize the whole proposal

Acknowledgment

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.