Sound Source Localization and Distance Estimation in Open Environment using Simulation and AI

Master Thesis

Denis Rosset (mailto:denis.rosset@hefr.ch)

University of Applied Sciences and Arts Western Switzerland

July 2023

Abstract

Sound source localization is a well-known problem in the field of signal processing. It is used in many domains, such as robotics, surveillance, and military applications. This project aims to create a baseline to develop a system to localize a sound source in an open environment. We base our project on a neural network that takes a spectrogram as input and predicts the position of a vehicle. We train the neural network using a dataset of sounds recorded from vehicles on the street. We also use a simulation to augment the dataset. To make the model safe, we test it against adversarial attacks to understand how it behaves if someone attacks it.

Supervisors:

Michael Mäder: Professor in computer science
Beat Wolf: Professor in computer science

Principals:

Marc-Antoine Fénart: Professor in civil engineering
Gabriel Python: Scientific associate at Rosas

Expert:

Dr. Robert van Kommer

Acknowledgements

I want to express my gratitude to my supervisors, Michael Mäder and Beat Wolf, for the opportunity to realize this Master's thesis with their supervision and for their excellent advice during this project. I also want to thank Marc-Antoine Fénart for the help with the baseline definition and the lent material. Additionally, I want to thank Gabriel Python and every member of the Rosas team for their help, advice, and encouragement during this project. Finally, I would like to thank my family and friends for the support they provided during the realization of this project.

Acronyms

HEIA-FR Haute École d'Ingénierie et d'Architecture de Fribourg

HES-SO Haute École Spécialisée de Suisse Occidentale (University of Applied Sciences and Arts Western Switzerland)

AI Artificial Intelligence

DNN Deep Neural Network

CNN Convolutional Neural Network

GPU Graphics Processing Unit

CPU Central Processing Unit

RAM Random Access Memory

MPEG Moving Picture Experts Group

FFMPEG Fast Forward MPEG

SSH Secure Shell Protocol

RTP Real-time Transport Protocol

SFTP Secure File Transfer Protocol

FFT Fast Fourier Transform

PCM Pulse-code Modulation

FGSM Fast Gradient Sign Method

WAV Waveform Audio File Format

MP4 MPEG-4

USB Universal Serial Bus

MSE Mean Squared Error

ReLU Rectified Linear Unit

Contents

1 Introduction

Within the framework of the research project "NPR Teleoperation," the engineers of the HEIA-FR have developed the first concept in Switzerland of a remote-controlled automated vehicle. However, teleoperation only makes sense if the vehicle is automated. There can be no teleoperation without automation (economic factors), just as there can be no automation without teleoperation (legal, technical, and social factors). ROSAS then created the Autovete (Automatisation de véhicules téléopérés) project. HEIA-FR finances them to build up vehicle automation expertise. Detecting other emergency vehicles is mandatory for a vehicle to be fully autonomous. V2V (Vehicle-to-Vehicle) communication is a solution but is not yet integrated into emergency vehicles. So, to detect such a vehicle, two signals need to be processed: the sound of the emergency siren and the blinking lights of the vehicle. The first use case of this project focuses only on sound source distance estimation and localization. Detecting excessively noisy vehicles on the street is a simpler use case for this project to understand if sound source estimation and localization could work for vehicles in an open environment. The goal is to measure the sound level of the passing vehicles and compare it with the legal limits. If a vehicle exceeds the limit, the system can record its license plate and report it to the authorities. This way, the system can help reduce noise pollution and improve road safety. This system requires a microphone array, a camera, and a processing unit to achieve the needed detection. The microphone array captures the sound signals from different positions and sends them to the processing unit. The processing unit applies a sound source localization algorithm to estimate the direction and distance of the sound source. The camera captures the image of the vehicle and performs license plate recognition.

Big improvements in sound source localization are being achieved with the help of neural networks[1]. They can be used to reliably localize the origin of a sound using one or more microphone arrays (multiple microphones operating in tandem). A non-negligible problem is the small number of real-world datasets with moving sources in an open environment. A solution is to create datasets in realistic sound propagation simulation and use them to augment the real-world datasets. A model can then be trained on the augmented dataset and tested for its performance in real-world data.

Using neural networks to solve the sound source localization problem can lead to a new attack vector for the system. The system can be attacked by modifying the sound source or signal. Tests to understand how the system reacts to such attacks are necessary to understand the system's robustness.

1.1 Motivation

More and more cities are fighting against noise pollution in the streets. Excessively noisy vehicles are mainly causing this pollution. The project's main objective is to help elaborate a system to detect excessively noisy vehicles on the street and report them to the authorities. The system should know where the sound source is to achieve this detection. The system needs to localize a noisy vehicle on the street based on the sound it produces. This capability is important because when multiple vehicles are on a video or a picture, it is difficult to know which vehicle is noisy.

1.1.1 Objectives

The project's main objective is to help elaborate a system to localize a vehicle sound source in an open environment.

Since we realized the specification file at the start of the project before the baseline definition, we updated this objective section to match the new baseline more precisely. The initial objectives are available in the appendix A.2. We do a self-assessment on the specification file in the conclusion (chapter 6).

Objective n°1 Baseline The first objective is to define a baseline for the project. The baseline should contain the problem statement and the steps to complete the baseline. It should include a list of tasks, system design, development, and testing.

Objective n°2 Dataset according to the baseline The second objective is constructing a coherent dataset with the project's baseline. The dataset contains the target variable, features, and necessary pre-processing steps. This dataset will help represent and understand the problem.

Objective n°3 Model for sound source localization and distance estimation The third objective wants to create a neural network model to detect the origin of a sound using a microphone array. The neural network uses the dataset created in objective 2 for training and can localize the sound source accurately. An evaluation of the trained neural network model in a real environment allows us to see how it performs. We will also evaluate the model to understand how we can improve it.

Objective n°4 Realization of a dataset in a simulation The fourth objective is to create a new dataset in a simulation. The dataset will augment the real-world dataset and help provide a better neural network model. The dataset should be realistic and contain the same characteristics as the real-world dataset. We will evaluate the model trained with the augmented dataset to understand its usefulness.

Objective n°5 Attacking the model to understand how it reacts The fifth objective is to attack the model. We must evaluate the trained neural network model by testing it on modified data, such as by adding or removing noise. We must perform tests against adversarial attacks to understand how the model reacts.

1.2 Structure of the report

We define the structure of the thesis in multiple chapters organized as follows:

- **Chapter 2: Analysis and Litterature**: This chapter overviews the background knowledge necessary to understand the project, such as machine learning and sound propagation theory. It helps to understand the project's context and the state of the art.

- **Chapter 3: Design**: This chapter describes the design of the project's different parts. It presents the description of the project's architecture and components.
- **Chapter 4: Realization**: This chapter describes the work done to achieve the project's objectives, such as creating a dataset, creating a simulation, building a neural network model, and evaluating it using an appropriate metric.
- **Chapter 5: Results and Analysis**: This chapter presents the project's results, such as the performance of the neural network model and the evaluation metrics. It also analyzes the results and discusses the findings.
- **Chapter 6: Conclusion and future work**: This chapter concludes this project by discussing the main results and summarizing the key findings. This chapter also contains a section about the project's future and direction.

2
Analysis and Litterature

This chapter introduces technical concepts and background used in the conceptualized solution of the thesis. It also explains the analysis of the needs of the thesis and finds relations with the current state of research in sound source localization systems.

2.1 Baseline analysis

During the first weeks of the thesis, we had the opportunity to place an installation of microphones on the HEIA-FR main building roof. We took that opportunity to design the baseline and analyze how to build a system around this possibility.

After analyzing the road in front of the HEIA-FR main building, we decided to use the baseline to detect the position of vehicles driving on the road. The road is moderately busy, and the vehicles drive at a reasonable speed. The road is also straight, which makes it easier to detect the position of the vehicles. The baseline is shown in Figure 3.3. This analysis helps provide an intuitive understanding of the sound source localization system. The baseline comprises a vehicle as the sound source we want to record, multiple microphones recording the sound of the street, and an embedded system that manages the microphones.

2.1.1 Audio file format

The Waveform Audio File Format[1] is a standard for storing numerical audio data. The audio signal is continuous and is sampled to store it on a computer. The sampling rate represents the number of samples per second. The sampling rate is usually measured in Hertz (Hz). The numerical representation of the audio often used with wav is the PCM.

The PCM (pulse-code modulation)[2] is a method used to represent an analog signal with a binary. It is often used to represent uncompressed digital audio. The PCM is a sequence of amplitude values. The amplitude values are often stored as 8-bit, 16-bit, or 24-bit integers, depending on the quality. A representation of a sampled sinusoidal signal is shown in Figure 2.1.

[1] https://www.loc.gov/preservation/digital/formats/fdd/fdd000001.shtml

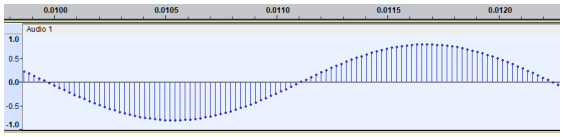


Figure 2.1: PCM representation of a sinusoidal signal

Each vertical line represents a sample. The horizontal axis represents the time, and the vertical axis represents the amplitude. The sampling rate is usually 44100 Hz, 48000 Hz, or 96000 Hz.

2.2 Sound Source Localization

Sound Source Localization (SSL) is the process of determining the position of a sound source. It usually uses a microphone array that captures the sound signals from multiple directions. Various applications use SSL [1], such as speech recognition [3], source separation [4], human-robot interaction [5] or room acoustic analysis [6]. In this thesis, SSL is used to estimate the distance and direction of a sound source to detect excessively noisy vehicles.

2.2.1 Spectrograms for sound visualization

Spectrograms are a visual representation of the frequency content of a sound signal. They are often used in sound source localization to identify the direction of a sound source. The spectrogram is a two-dimensional representation of the frequency content of a sound signal (figure 2.2).

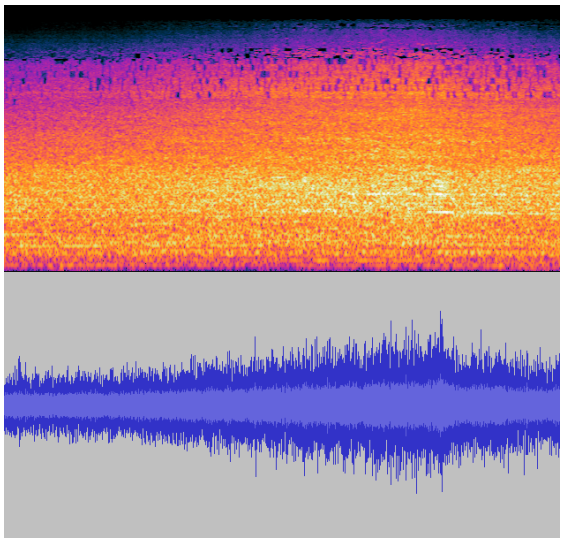


Figure 2.2: Spectrogram of a sound signal

Spectrograms are drawn by computing the Fourier transform of a sound signal. The most common way to compute the Fourier transform is to use the Fast Fourier Transform (FFT) algorithm [7].

The x-axis represents time, and the y-axis represents frequency. The intensity of the color at each point in the spectrogram represents the amplitude of the frequency component. A matrix of spectrograms allows

the representation of multiple channels, such as the ones recorded by a microphone array. On that matrix, each spectrogram represents the frequency content of a single channel (figure 2.3).

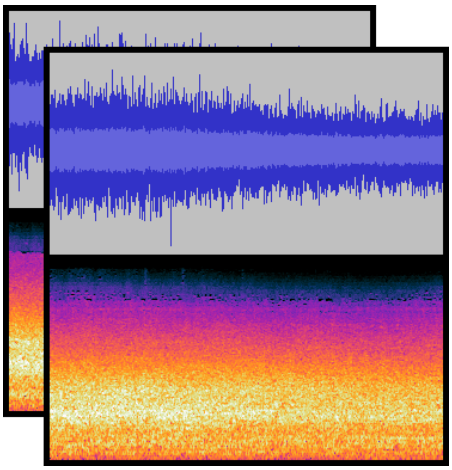


Figure 2.3: Dual channel spectrogram matrix of a sound signal

Looking at the frequency content of the sound signal allows us to identify the time delta of a recorded sound by using a multi-channel spectrogram. The bright spot on the spectrogram will indicate a jump in the amplitude and determine the start time of the recording of a loud sound. By comparing this time with the other channel, we can find the direction of the sound source by comparing the sound signal's time delta with the other channels' time delta (figure 2.4).

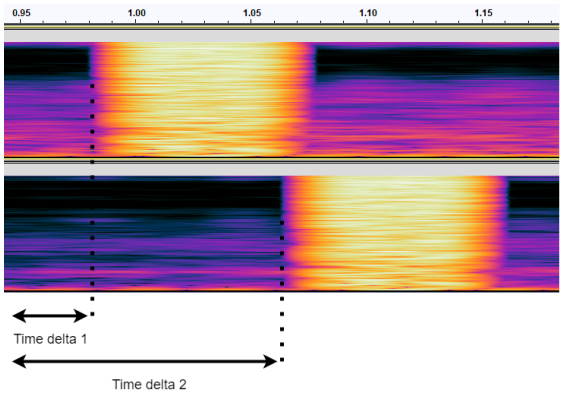


Figure 2.4: Spectrogram of two sound signals with time their delta

Since we know the distance between the microphones, we can determine the direction of the sound.

2.2.2 Signal estimation from Short Time Fourier Transform

The Griffin-Lim algorithm[8] is an iterative algorithm that uses a spectrogram to estimate the phase of a signal. The algorithm starts with a random phase and iteratively updates the phase until the spectrogram converges to the original spectrogram. This algorithm allows to reconstruct a signal from a spectrogram.

2.2.3 Origin of sound using two microphones

Admitting the following setup (figure 2.5), if the time delta 1 is greater than the time delta 2 of the other channels (setup 1), the sound source is closer to microphone 2. If the time delta 1 equals the time delta 2 (setup 3), the sound source is at the same distance to both microphones. If the time delta 2 is greater than the time delta 1 (setup 2), the sound source is closer to the microphone 1.

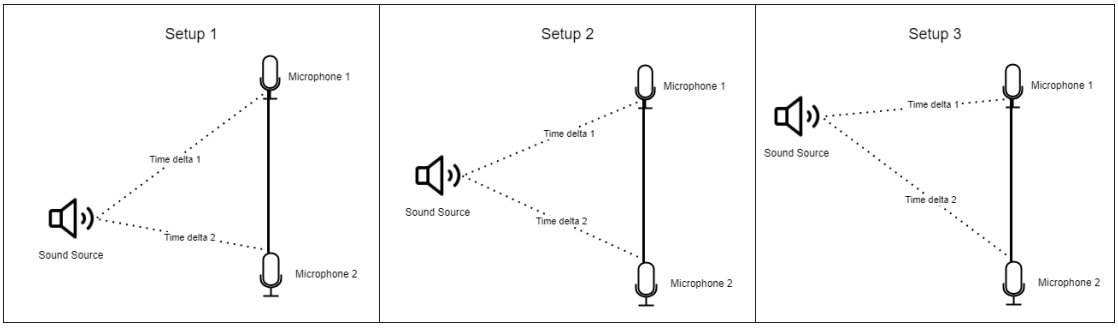


Figure 2.5: Sound source localization setup

As explained in [9], once the delay between the two microphones is known, the equation allows us to find the direction of the sound source by using trigonometric calculations. As in the figure 2.6, considering point M as the sound source and point A and B as microphones, the distance between the two microphones is d and the time delta between the two microphones is Δt, the angle α can be calculated.

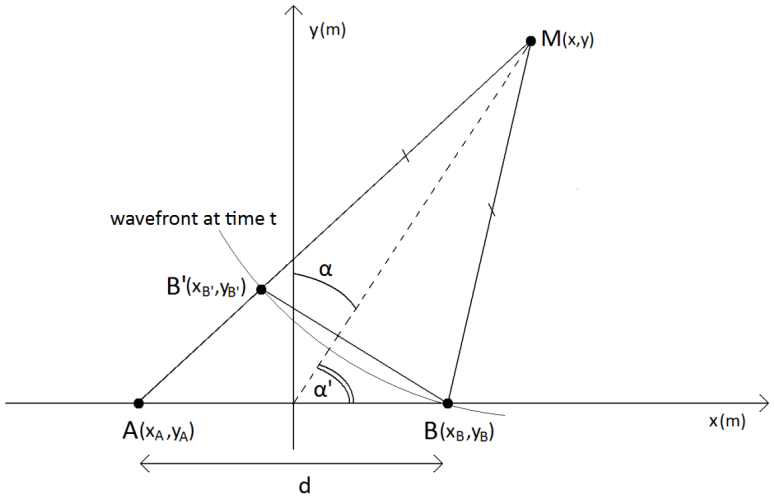


Figure 2.6: Equation formalization. Original image from [9]

Looking at the graphic allows us to find the following equation:

$$AB' = AM - B'M \tag{2.1}$$

With Pythagorean theorem:

$$AM = \sqrt{(X_a - X)^2 + (Y_a - Y)^2} \tag{2.2}$$

$$BM = \sqrt{(X_b - X)^2 + (Y_b - Y)^2} \tag{2.3}$$

The two microphones have the same Y coordinate, so $Y_a = Y_b = Y$ and $Y_a - Y_b = 0$ and $X_a = -X_B$ The equation becomes:

$$y = \pm\sqrt{\frac{AB'^2}{4} - x_B^2 + x^2(\frac{4 \cdot x_B^2}{AB'^2} - 1)} \tag{2.4}$$

The only variables are y and x. The value x_B represents the position of the microphones, which we take as reference points. The value AB' will not change even if the direction varies. Considering the speed of sound c, the distance AB' is:

$$AB' = c \cdot \Delta t \tag{2.5}$$

This equation gives us the possible positions of the sound source on a line. If we admit that the sound source is always in front of the microphones, we can eliminate the negative values of y and keep only the positive values. With that solution,

This setup shows that two microphones are enough to determine the direction of a sound source.

2.3 Artificial Neural networks

Artificial neural networks, also more simply called neural networks, are machine learning algorithms based on biological neurons used to solve various problems, including image recognition, speech recognition, and natural language processing. Neural networks learn from provided data to solve a problem without explicitly programming the solution. Many domains, like self-driving cars, facial recognition, and medical imaging, achieve state-of-the-art results using neural network models.

A neural network needs to be trained to solve a problem. The training consists of providing the neural network with examples to recognize patterns in the data. Once we finish the training, the model can solve the problem.

A neural network (figure 2.7) is composed of multiple neurons (the circles) that are organized in layers and connected to the neurons in the previous and next layers.

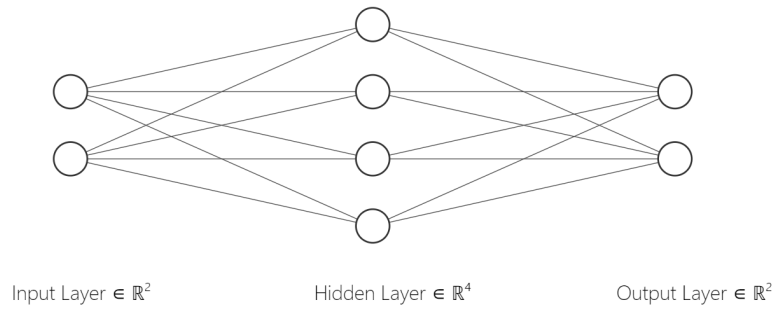


Figure 2.7: Neural network

There are two main phases in the life of a neural network: training and inference. We train the neural network on a large dataset during the first phase. The neural network learns to recognize patterns in the training data and tries to generalize them. During the inference phase, we use the neural network to classify new images.

Neural networks comprise multiple neurons. Neurons are mathematical functions with activation functions and weights. These determine how the neurons respond to inputs and connect to other neurons. Neural networks train themselves by adjusting the weights to minimize the error between the predicted and desired outputs. They use an optimization algorithm to adjust the neurons' weights [10]. Multiple optimization algorithms exist. The most used is gradient descent[11]. These algorithms minimize the error between the predicted and desired outputs.

2.3.1 Neuron

A neuron is a mathematical function that takes multiple inputs and produces an output. The activation function and the weights of the neuron determine the output. The activation function determines how the neuron responds to inputs. The weights determine the importance of the inputs. The neuron's output is calculated by multiplying the inputs by their weights and applying the activation function to the result. The neuron sends its output to the next layer of neurons.

Activation function Multiple activation functions exist for neural networks. The most common activation functions are the linear function, the sigmoid function, the tanh function, and the ReLU function (Figure 2.8).

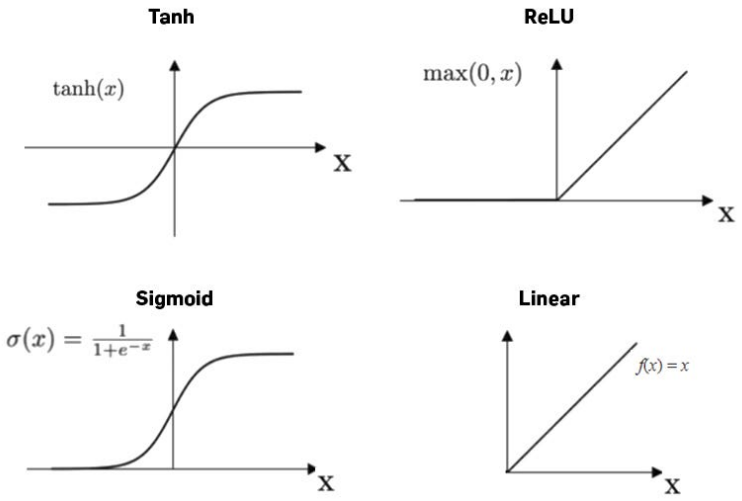


Figure 2.8: Activation functions

These functions will determine how the neurons respond to inputs. These functions have been surveyed in [Activation Functions in Deep Learning: A Comprehensive Survey and Benchmark][12]. It shows that the ReLU function is the most used activation function in deep learning. The ReLU function is defined as:

$$f(x) = max(0, x) \tag{2.6}$$

The ReLU function is used in most neural networks because it is fast to compute and provides good results.

Loss function Neural networks use a loss function to measure the error between the predicted and desired outputs. The loss function is a mathematical function that takes the predicted and desired outputs as inputs

and outputs a value representing the error between the predicted and desired outputs. The optimization algorithms use the loss function to adjust the neurons' weights to minimize the error between the predicted and desired outputs. When the loss function's value is low, the neural network accurately predicts the desired outputs.

There is a wide variety of loss functions, including the mean squared error and the cross-entropy.

The mean squared error loss function is defined as follows:

$$L(y, \hat{y}) = \frac{1}{n} \sum_{i=1}^{n} (y_i - \hat{y}_i)^2 \tag{2.7}$$

Where y is the desired output, $\hat{y}$ is the predicted output, and n is the number of classes.

The cross-entropy loss function is defined as follows:

$$L(y, \hat{y}) = -\sum_{i=1}^{n} y_i \cdot log(\hat{y}_i) \tag{2.8}$$

Where y is the desired output, $\hat{y}$ is the predicted output, and n is the number of classes.

We can multiply the loss function by the weights to give more importance to some classes. It helps when a dataset is unbalanced by giving more importance to the underrepresented classes. The weighted cross-entropy loss function is defined as follows:

$$L(y, \hat{y}) = -\sum_{i=1}^{n} w_i \cdot y_i \cdot log(\hat{y}_i) \tag{2.9}$$

Where y is the desired output, $\hat{y}$ is the predicted output, n is the number of classes, and w is the weight of the class.

Gradient descent Gradient descent is an optimization algorithm that minimizes the error between the predicted and desired outputs [11]. We use it to train neural networks. Gradient descent works by iteratively adjusting the neurons' weights to minimize the error between the predicted and desired outputs. It uses the gradient of the loss function to find the direction of the steepest descent. We adjust the weights in the opposite direction of the gradient. The gradient descent algorithm is defined as follows:

$$\theta_{n+1} = \theta_n - \alpha \cdot \nabla f(\theta_n) \tag{2.10}$$

Where θ_n is the current weight, α is the learning rate, and $\nabla f(\theta_n)$ is the gradient of the loss function. We repeat the algorithm until the loss function's value is low enough. The gradient descent algorithm is slow because it uses the entire dataset to compute the gradient of the loss function.

Mini-batch gradient descent Mini-batch gradient descent is a variant of gradient descent [13]. It uses a batch of samples to compute the gradient of the loss function. It is faster than full gradient descent because it uses a mini-batch of samples instead of the entire dataset. It is also more stable than gradient descent because it uses a mini-batch of samples instead of a single sample. The mini-batch gradient descent algorithm is defined as follows:

Backpropagation Backpropagation is an algorithm used to train neural networks[14]. Its utility is to compute the gradient of the loss function.

2.3.2 Neural network hyperparameters

Neural networks use different hyperparameters to control the training process. Some of the most common hyperparameters are the activation function, the learning rate, the number and type of layers, and the optimizer. We use these parameters to train the neural network efficiently. Multiple solutions exist to find the best hyperparameters for a neural network, but none are perfect [15].

Learning rate To train efficiently a neural network, we use a learning rate. It determines a factor of how much we adjust the weights during training. A high learning rate will adjust the weights by a large amount, hence training the neural network faster but less precisely. A low learning rate will adjust the weights by a small amount, hence training the neural network slower but more precisely. The learning rate is a hyperparameter that needs to be tuned to achieve the best results.

A solution to this problem is to use an adaptive learning rate. Adaptive learning rates are learning rates that change during training. They are used to train the neural network faster and more precisely. [Adaptive Learning Rate and Momentum for Training Deep Neural Networks][16] shows us how it can train neural networks efficiently without losing precision.

2.3.3 Deep Neural Networks

Deep neural networks are a type of neural network composed of multiple layers of neurons[17]. They are trained on a large dataset and are then used to classify new data. There are countless architectures [18] and implementations of neural networks, but they all share the same basic principles. The most known architectures of neural networks include CNNs[19], transformers[20], and many others.

2.3.4 Convolutional Neural Networks for sound source localization

Convolutional Neural Networks (CNNs)[19] are deep neural networks specifically used for image recognition. They often comprise convolutional, subsampling, and fully connected layers (Figure 2.9).

- Convolutional layers are used to extract features from images. These features are then fed into fully connected layers to perform classification. Each convolutional layer comprises multiple filters convolved with the input image to produce a feature map. The model trains the filters to extract specific features from the input image.
- Subsampling layers are used to reduce the size of the feature maps. The most common subsampling layer is the max-pooling layer, which takes the maximum value of a specific region of the feature map.
- Fully connected layers are trained to classify the features extracted by the convolutional layers. The output of the fully connected layers is a probability distribution over the possible classes.

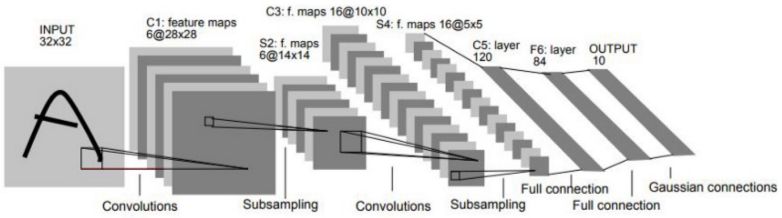


Figure 2.9: CNN architecture example with LeNet-5 [21] composed of two convolutional layers, two subsampling layers, and finishing with two fully connected layers.

Even if we mainly use CNNs to classify real-life photography, they can classify any image, including sounds. The report [A survey of sound source localization with deep learning methods][1] shows that deep neural networks achieve good scores in sound source localization. CNNs can use any image as input. Based on section 2.2.1, we can use the spectrograms as input in the network since we convert the sound into images during the spectrogram process. An approach for sound source localization is to use zones from which the sound can come as classes. The CNN will output a probability distribution over the possible classes. The class with the highest probability is the predicted class. The predicted class can then refer to a zone. The CNN then outputs a probability distribution over the possible classes. We need to define the possible classes before training the CNN. In this work[22], they approach the problem with 15 classes, using angles -60, -30, 0, 30, and 60 degrees multiplied by distances 1, 2, and 3 meters (Figure 2.10).

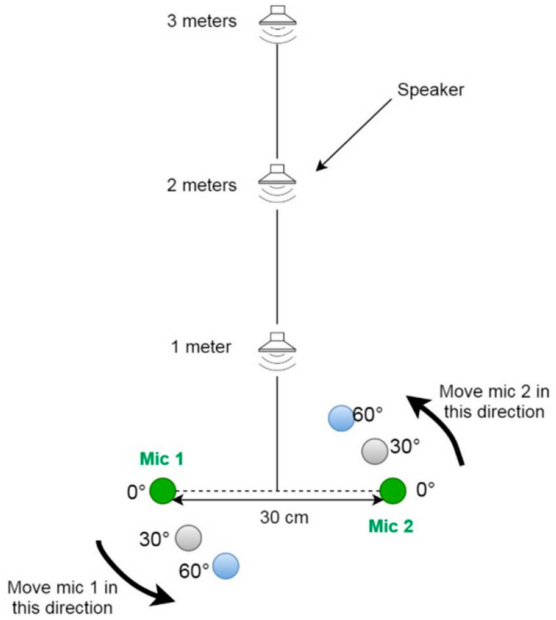


Figure 2.10: Class definition for the Yiwere classification approach[22].

This setup gives nine classes representing a different zone from where the sound can come from. The CNN will output a probability distribution over the nine classes, which allows determining the zone from where the sound comes from.

2.3.5 Dropout layers

Dropout layers help prevent overfitting in neural networks [23]. They are stochastic techniques used to forget part of the information during training to generalize better.

2.4 Datasets for machine learning

Datasets are needed to train and test neural networks. They are composed of data and labels. The data is the neural network input, and the label is the expected output. Each entry in the dataset is composed of the data and the corresponding label. An entry in a dataset can also be called a sample.

A balanced dataset contains nearly the same number of samples for each class. An unbalanced dataset contains a considerably different number of samples for each class.

2.4.1 Datasets for sound source localization

In the case of sound source localization, the data is audio, and the labels are the zones of the sound source.

Multiple datasets exist in sound source localization for neural networks. The most common are the DCASE 2019 task 3 dataset[24] and the DCASE 2020 task 3 dataset[25]. These datasets are composed of audio files and the corresponding labels. The labels are the zones of the sound source. They record the audio files in a room with a microphone array and a sound source. They move the sound source around the room and record the audio. They annotate the audio files based on the zones of the sound source. The annotations are done manually by listening to the audio files and annotating the zones. Multiple annotators then verify the annotations to ensure the quality of the annotations.

Although these datasets are good baselines for sound source localization, they do not suit the needs of this project. The datasets are recorded in a closed environment and do not reflect the baseline defined in this project. Still, these datasets are good baselines for sound source localization and help to understand how to create a dataset.

2.4.2 Dataset augmentation for audio classification

Since recording many audio files is time-consuming and costly, and since the dataset needs to be large to train a neural network, we can use dataset augmentation techniques.

Dataset augmentation is a technique used to increase the size of a dataset. It is used to improve the performance of a neural network by training on more data, thus becoming better at generalizing. The most common techniques[26] are flipping, rotating, and cropping images, but we realize the classification in this project on audio. Some other techniques are needed to augment the dataset. Techniques that work well on audio are adding noise, changing the pitch, or simulating new data[27].

2.4.3 Metrics review for neural networks

Accuracy The most common metric for neural networks is accuracy. The accuracy is the number of correct predictions divided by the total number of predictions. Accuracy is a good metric for classification problems since it tells us how the model performs. The accuracy is defined as follows:

$$\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total number of predictions}} \tag{2.11}$$

Accuracy is a useful metric for classification problems as it provides insight into how well the model performs. However, it may not be the best metric for unbalanced datasets. For instance, if a dataset contains 90% of class A and 10% of class B, a model that always predicts class A will have an accuracy of 90%. Although this model has high accuracy, it is ineffective since it always predicts the same class.

Recall Recall is another metric that we use. The recall is the number of true positives divided by the number of true positives and false negatives. The recall is defined as follows:

$$\text{Recall} = \frac{\text{True positives}}{\text{True positives} + \text{False negatives}} \tag{2.12}$$

Recall is a good metric for unbalanced datasets since it considers the number of false negatives.

F1 score Another metric that we can use is the F1 score. The F1 score is the harmonic mean of the precision and recall. The F1 score is defined as follows:

$$\text{F1 score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{2.13}$$

Loss The model calculates the loss metric during the training to update the neural network weights. We can use the loss value to represent how well the model performs. The loss is defined as follows:

The F1 score is a good metric for unbalanced datasets since it considers precision and recall.

Confusion matrix To have a visual understanding of how a model performs, we use a confusion matrix. A confusion matrix shows the number of correct and incorrect predictions for each class. The confusion matrix can be used with any number of classes and is a good way to visualize the performance of a model. The main aim of visualizing a confusion matrix is to see which classes the model misclassified and which are correctly classified. For example, in a binary classification problem, the confusion matrix is a 2x2 matrix. The confusion matrix is defined as follows:

$$\begin{bmatrix} \text{True positive} & \text{False negative} \\ \text{False positive} & \text{True negative} \end{bmatrix} \tag{2.14}$$

And the matrix can be visualized as follows:

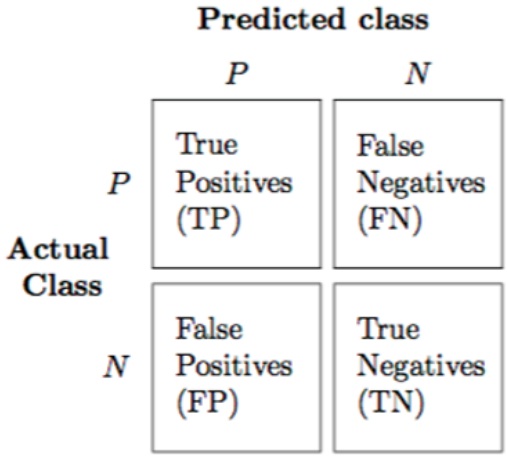


Figure 2.11: Confusion matrix visualization

The confusion matrix allows us to understand which classes are misclassified and better understand if the model has difficulty predicting certain classes.

2.5 Sound propagation

Sound propagation is the physical process by which sound waves propagate in a given environment. Multiple factors affect the propagation of sound waves, including reverberation, occlusion, doppler effect, and obstruction. These effects are needed to have a realistic representation of the sound in a given environment.

2.6 Dataset generation using simulation

Simulating a dataset is a technique used to augment a dataset without recording data from real life [27]. It helps to create a dataset with many samples.

Since this work aims to generate sounds in an open environment, a 3D-capable engine is necessary. Game engines are increasingly popular for simulation tasks since they are optimized for real-time rendering and can simulate complex 3D scenes [28]. The game engine must also simulate sound propagation to have a realistic audio representation in the simulation.

Microsoft Project Acoustics[2] is a plugin based on Microsoft's research[29]. The plugin simulates sound propagation. Various applications, including video games, virtual reality, and physics simulation, use this engine. It simulates wave effects like obstruction, reverberation, and occlusion in complex 3D scenes without requiring zone markup or raytracing. It works similarly to a raytracing engine but is precomputed and optimized for real-time performance.

It is available in the Unity game engine. It simulates sound propagation by using ray-based acoustics methods to check for occlusion, as shown in Figure 2.12:

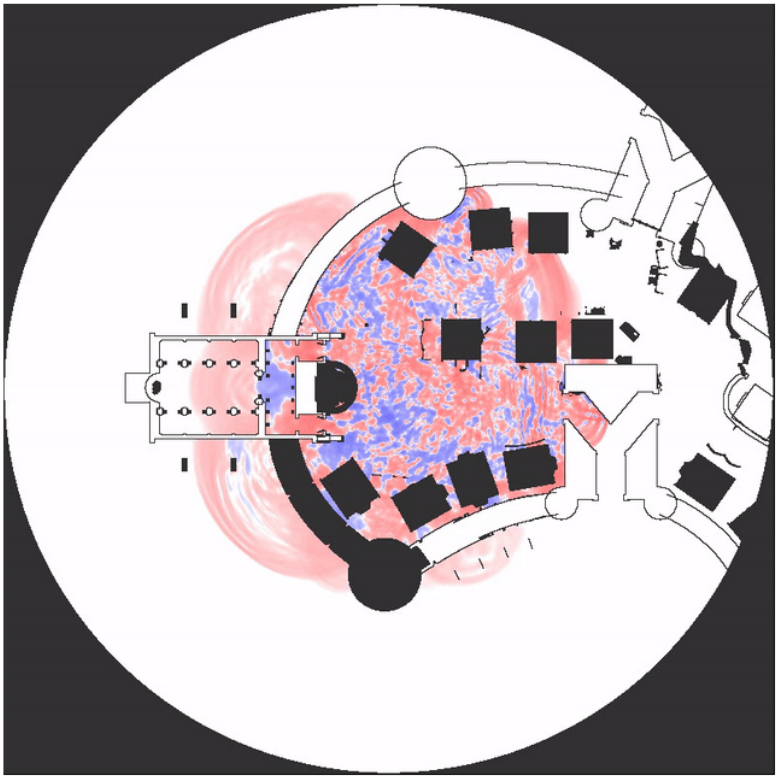


Figure 2.12: Ray-based acoustics method used in Microsoft Project Acoustics to detect occlusion[29].

The plugin can be used in any 3D environment by pre-calculating the possible path of the sound. Once we realize the pre-calculation, the plugin can simulate the sound propagation effects in real-time.

[2] https://learn.microsoft.com/en-us/gaming/acoustics/what-is-acoustics

2.7 Adversarial Attacks

Adversarial attacks are a manipulation technique that aims to fool a neural network by modifying the input data. The goal is to make the neural network misclassify. Adversarial attacks allow us to test the robustness of neural networks and understand how neural networks work and how we can improve them.

We classify adversarial attacks into two categories: white-box attacks and black-box attacks. White-box attacks are attacks where the attacker has access to the neural network's parameters and architecture. Conversely, black-box attacks are attacks where the attacker has no access the neural network's parameters and architecture.

One of the most common adversarial attacks is the Fast Gradient Sign Method (FGSM)[30]. It is a white-box attack that uses the gradient of the loss function to find the adversarial example. We calculate the adversarial example using the following equation:

$$X_{adv} = X + \epsilon \cdot sign(\nabla_X J(\theta, X, y)) \tag{2.15}$$

Where X is the input, y is the target class, ϵ is the magnitude of the perturbation, and $J(\theta, X, y)$ is the loss function. The loss function is the function that the neural network normally tries to minimize, but here is used to maximize the loss. We calculate the gradient of the loss function for the input X. The sign of the gradient is then calculated and multiplied by the magnitude of the perturbation ϵ. The result is added to the input to create the adversarial example X_{adv}. We feed the adversarial example into the neural network, which, if the attack succeeds, can output the wrong class (Figure 2.13).

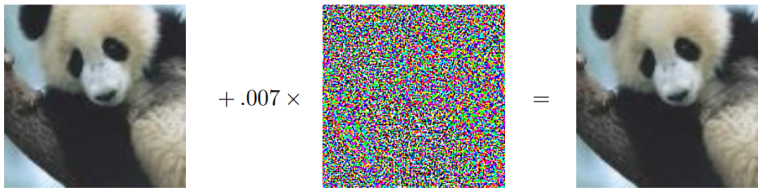


Figure 2.13: FGSM example in [30] with a neural network classifying a panda as a gibbon because of the attack.

3
Approach and Design

This chapter presents the design of the project. It is the description of the project's architecture and the project's components.

3.1 Baseline design

We must design a baseline since we start the project without previous work. The baseline is the starting point of the project. It is the simplest system that we can create to solve the problem. The baseline can then compare the results and improve the system.

Problem statement The problem we are trying to solve is to detect and localize a vehicle's sound source in an open environment.

The baseline system comprises three main parts: the vehicle recordings, the dataset creation, the model training, and the model testing. The system design is shown in Figure 3.1.

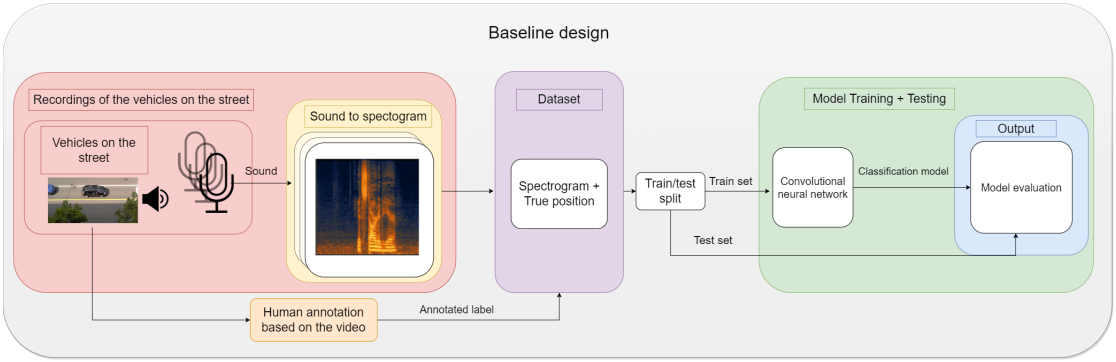


Figure 3.1: Baseline system design

In Figure 3.1, the red zone represents the vehicle recordings with multiple microphones and the transformation of the sound into spectrograms. We also record a video to have a ground truth to annotate the dataset. The purple zone represents the dataset creation with the spectrograms as data and the annotations from humans watching the videos as labels. We then split the dataset into a train and a test set. In the green zone, we feed the train set into a neural network to train it to predict the position of the sound source based on the spectrograms. We then test the model on the test set to evaluate its performance with unseen data.

Once we train and evaluate the model, we can use it to predict the position of a sound source based on a new recording. The model can be used in inference to detect the position of a sound source. The inference is shown in Figure 3.2.

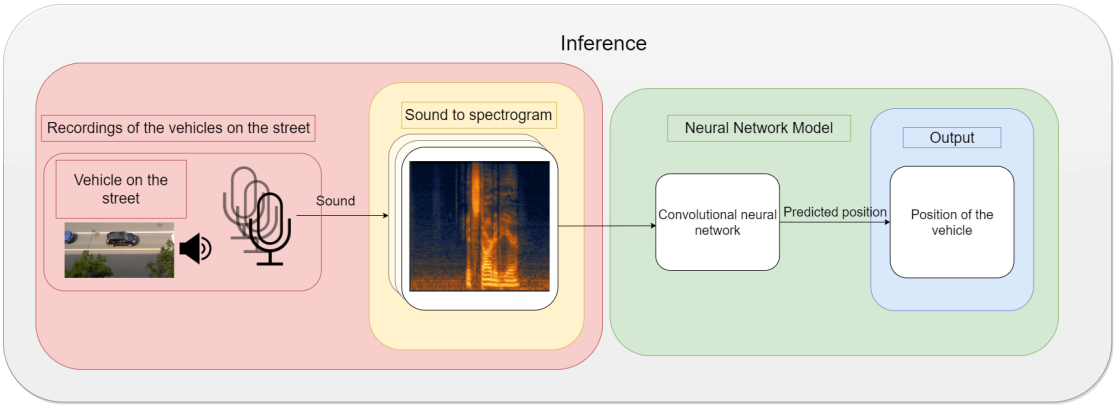


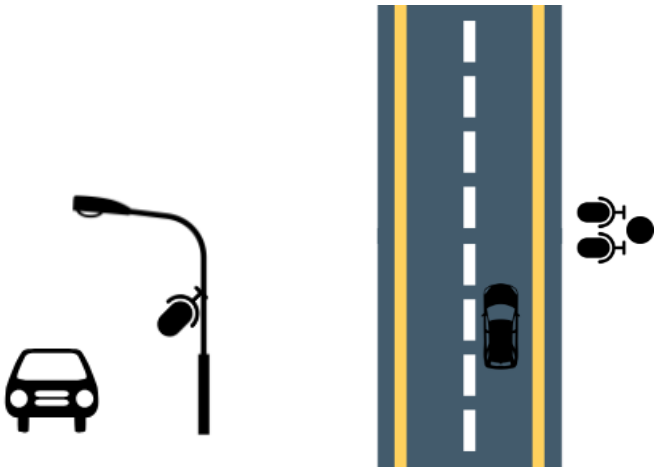
Figure 3.2: Baseline inference

The inference is similar to the training and testing, except that we do not have the ground truth since our model makes the prediction. We only have to do the spectrograms from the recording, and we can feed the spectrograms into the model. The model will then predict the position of the sound source.

We can further develop this idea to incorporate other sound sources for movement tracking in a generalized environment, such as emergency vehicle detection. The baseline is a valuable starting point to develop and test a system that can accurately identify and track sound sources.

3.1.1 Vehicle recordings

To create the dataset, we must have vehicle recordings with multiple microphones. We place de microphones on the side of the street as shown in Figure 3.3.



(a) Side view (b) Top down view

Figure 3.3: Baseline's microphone setup

We also need to record a video of the vehicle to have a ground truth to annotate the dataset. Vehicle recordings are the most crucial part of the baseline. We need to design a system that will allow us to record vehicles from the street and save the data. We designed the system managing the data recording and storage with two microphones, a camera, an embedded system, and a server to store the recordings. This system is shown in Figure 3.4.

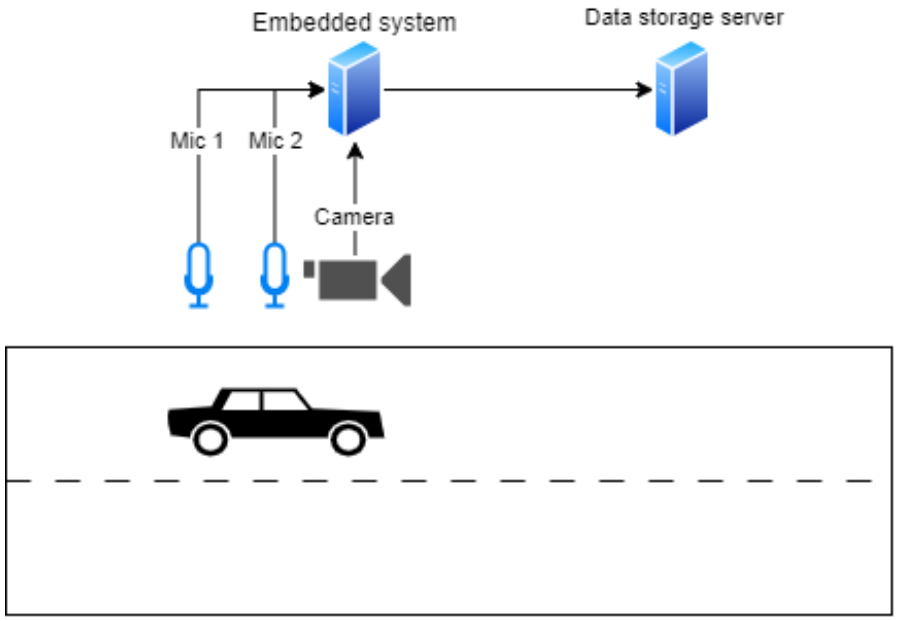


Figure 3.4: Recording system design

We defined two seconds of recording as our sample length. We chose this length arbitrarily, mainly

because it is long enough to have a vehicle passing by the microphones and short enough to have a reasonable size for the dataset.

Overall, the baseline provides a context to develop further a concept of an accurate sound source localization system for outdoor space.

3.1.2 Dataset conception

The dataset is the most crucial part of the baseline. We can determine the dataset's characteristics based on the analysis of the section 2.4.1. The dataset needs to contain the sound recorded by the microphone and the position of the sound source. To simplify the problem, we will use four classes as the main classification challenge in the project. The classes are the following:

- *left_to_right*: The vehicle goes from the left to the right of the microphone.
- *right_to_left*: The vehicle goes from the right to the left of the microphone.
- *no_cars*: No vehicles pass by the microphone.
- *multiple_cars*: Multiple vehicles pass by the microphone.

By adding a camera to the system in section 3.1.1, we can use the image captured by the camera to determine the ground truth of the sound source's position. The camera's position is the same as the microphone's position, and the camera is facing the road. These classes allow the creation of a dataset without precisely recording the vehicle's position. The *no_cars* and *multiple_cars* are here to ensure we will have a complete dataset, as with these four classes, we can cover every possible scenario recorded by the microphones and don't need to cherry-pick only the recordings that match our classification system.

We also used only two classes at the beginning of the project to ensure the concept's functionality when installing the system. These classes are the following:

- *left_to_right*: The vehicle goes from the left to the right of the microphone.
- *right_to_left*: The vehicle goes from the right to the left of the microphone.

3.1.2.1 Recorded data design

The input data needs to be an audio signal. Based on the analysis in section 2.1.1, we use the Waveform Audio File Format with pulse-code modulation to represent our audio signal. With this representation, we obtain a vector of floating point numbers representing the audio signal. Since we record multiple channels simultaneously, we can consider the channels as another vector dimension. We can then represent the audio signal as a matrix of floating point numbers.

3.2 Convolutional Neural Network design for Sound Source Localization

For our baseline, we use a convolutional neural network to predict the position of the sound source. We use a convolutional neural network because, based on the analysis in section 2.3.4, it is the most common neural network architecture for image classification and hence for sound source localization. We can use the spectrograms as image input and the convolutional neural network to classify the spectrograms.

The network design is composed of a feature extraction part and a classifier part. The feature extraction part comprises convolutional layers, ReLU, and pooling layers. The classifier part is composed of fully

connected layers. We use the feature extraction part to extract the features from the spectrograms and the classifier part to classify the features extracted. The full architecture is shown in Figure 3.5.

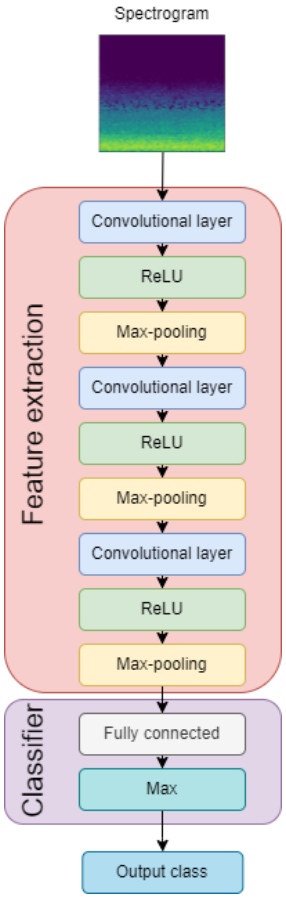


Figure 3.5: Baseline feature extraction

The feature extraction part comprises three blocks of one convolution, one ReLU, and one Max-pooling. The convolutional layers extract the features from the spectrograms. The ReLU layers introduce non-linearity in the network. The pooling layers reduce the dimensionality of the network. The classifier part is composed of one fully connected layer. The fully connected layer classifies the features extracted by the feature extraction part.

3.3 Simulation concept design

Since there are two main datasets in the project, we call the dataset described in section 3.1.2 real-life dataset and the one described in this section simulation dataset.

To improve the classification score of the baseline, we need to have more data. Multiple possibilities are available to achieve this goal. We can record more data, but it is time-consuming and expensive. We can also use a simulation to generate new data. In this project, we use a simulation to generate new recordings to add to the training dataset to achieve a better classification score on the baseline. The

simulation comprises the same elements in the recording system in section 3.1.1 except we simulate them. The simulation design is shown in Figure 3.6.

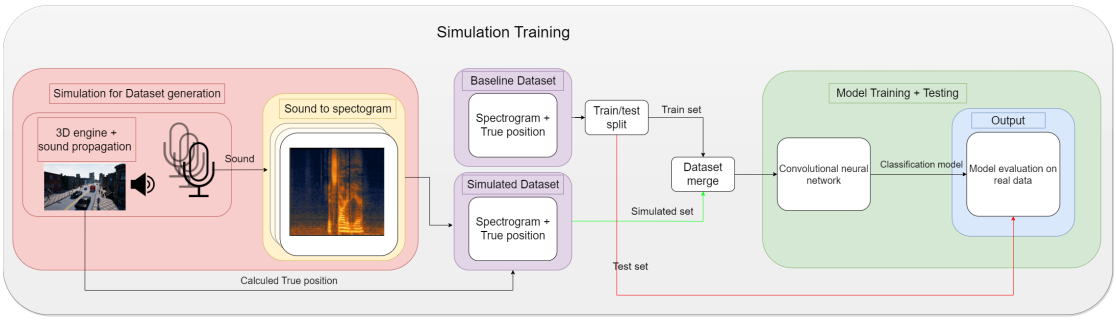


Figure 3.6: Simulation system design for training

There are differences with the baseline system. The main one is that we generate the data in a simulation. The second is that there is no need to annotate the dataset since we know the position of the sound source in the simulation, and we can deduce the position of the sound directly from the simulation. The last one is that we add the dataset generated by the simulation to the trainset of the baseline but not to the test set. This process allows us to understand better the simulation's impact on the real-life dataset classification score.

The main advantages of the simulation are that we can generate as much data as we want. We can generate data for any position of the sound source. The simulation is composed of a vehicle, a microphone, and a camera. Based on the section 3.1.2, we want to generate data for the classes *left_to_right* and *right_to_left*. We can generate data for the class *left_to_right* by placing the vehicle on the microphone's left and moving it to the right. We can generate data for the class *right_to_left* by placing the vehicle on the right of the microphone and moving it to the left. We did not generate data for the classes *no_cars* and *multiple_cars*.

3.3.1 Generalization aspect of the simulation

Simulation is a tool to generate data. But we must be cautious because the simulation can generate data that does not represent real-life data. If the simulation generates data that does not represent real-life data, the classification score on the real-life data will be low.

For the simulation to best generalize and better represent real-life data, we need to add randomness to the simulation in multiple ways.

Random speed The vehicle's speed is not constant in real life, and we need to add randomness to the vehicle's speed in the simulation. We can add randomness to the vehicle's speed by varying the speed assigned at the beginning of the simulation.

Random path At the beginning of the simulation, we define multiple points as possible start and end points for the vehicle journey. The vehicle's path is generated by randomly choosing a start and end point. We can then generate the vehicle's path by drawing a straight from the start to the end. This method matches the real-life scenario where the straight road in front of the HEIA-FR building constrains the vehicle's path.

Random starting time The vehicle's arrival time is not constant in real life. We add randomness to the vehicle's starting time in the simulation to match the real-life cases. We achieve it by varying the vehicle's waiting time at the simulation's beginning.

Random engine noise We need to assign an engine sound to the vehicle during the simulation to record the vehicle with the microphone. There are many vehicles in real life and many different engine noises. We reproduce this by randomly choosing an engine noise at the beginning of the simulation and playing it during the simulation.

Random background noise We add randomness to the background noise by randomly choosing a noise track at the beginning of the simulation and playing it during the simulation.

3.3.2 Simulation software design

The simulation generates audio data by playing scenarios and recording the sound generated. In the simulation, we represent the comportment analyzed in section 2.1.

3.4 Adversarial Attack design

Based on the analysis in section 2.7, we can use an adversarial attack to fool the model designed in section 3.2. This project uses the Fast Gradient Sign Method (FGSM) to generate adversarial inputs. The FGSM is a white-box attack meaning that we need the model's parameters to generate the adversarial inputs. Once we finish training the model, we can calculate the loss function's gradient concerning the input to find the direction that maximizes the loss function. Once we find the direction, we can add a perturbation multiplied by a value of epsilon to the input to generate the adversarial input. Once we generate adversarial inputs, we test them on the model to see how it reacts. We realize the attack on a specific value of epsilon. We can try to attack the model with different epsilon values to see how much noise is needed for the model to fail. We analyzed the results by comparing them with the baseline model's results.

3.4.1 Audio reconstruction design

Realizing the adversarial attack by modifying the spectrogram input is not enough to have a negative impact if we use the model for inference in a real-life scenario. Since the system designed in section 3.1 uses microphones as input, we need to transform the adversarial spectrogram back to audio. We can then play the audio on a speaker in front of the baseline system to see if the model still fails after the reconstruction of the audio signal.

3.4.2 Adversarial attack protection design

Once we generate the adversarial audio signal, we must again play it through a speaker and the microphone. We can analyze the adversarial audio signal before the classification and try detecting an attempted attack. We can use a classic CNN to classify the type of sound recorded. We can then use the classification score to detect an attempted attack.

4 Realization

This chapter explains how we realized every part of our project. We present the results for each part of this chapter in the chapter 5.

4.1 Realization of the data recording system

In this section, we explain how we realized the data recording system. We first explain the hardware we use and how we install it. Then, we explain how we record the data and process it to get the needed data. Finally, we explain how we use the data to train our model.

4.1.1 Hardware for the recordings

To record real data that suits our baseline, we must design a system to record and save lots of data. As we had the opportunity to place it on the HEIA-FR, we decided to design a system containing an embedded system, two microphones, a camera, and an embedded system. For the hardware, we chose to ensure that the system is easily replicable and that the system is not too expensive. We use hardware available at the HEIA and Rosas. The global architecture of the system is shown in Figure 4.1. This diagram helps us understand how each system component is connected and how to access them.

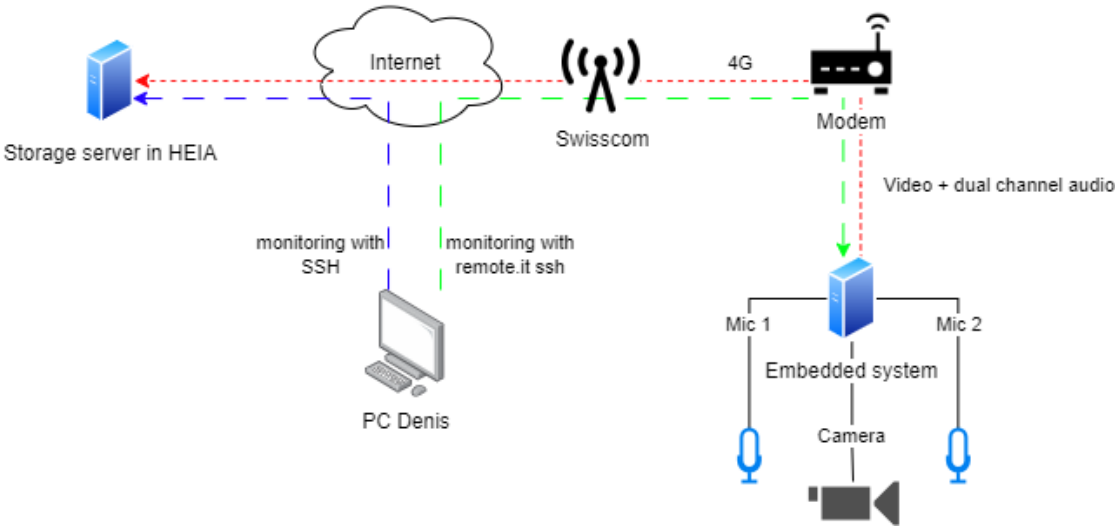


Figure 4.1: Global architecture

The HEIA-FR has a small balcony on the 4th floor with hardware installed for other projects. We use this balcony to install our system. The balcony is on the side of the street. It comprises a barrier on which we can attach hardware to have a good view of the street.

To record real data that suits our baseline, we must get hardware to record and save the data. The hardware we use is the following:

Microphones We use two microphones to record the sound. We use the *nsrt mk3 dev kit* from *convergenceinstruments* [1] with the USB audio interface (Figure 4.2). Prof. Marc-Antoine Fénart chose the microphones himself. We use two microphones to have a stereo sound recording.

Figure 4.2: Microphone used for the recordings

Camera The camera used is a webcam from Rosas that was available at the moment of the installation. We use the *C310 webcam* from *logitech* [2] since it meets our needs (Figure 4.3).

[1] https://convergenceinstruments.com/
[2] https://www.logitech.fr/fr-fr/product/hd-pro-webcam-c920

Figure 4.3: Webcam used for the recordings

Embedded system We use the *Raspberry Pi 4* from *raspberrypi* [3] as an embedded system (Figure 4.4). We use this embedded system because it is powerful enough to run the recordings and was available at the HEIA-FR. Since our microphones and our camera have USB connectors, we needed an embedded system with at least 3 USB connectors.

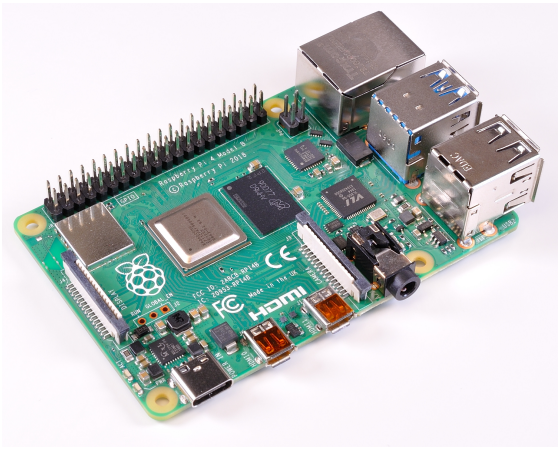


Figure 4.4: Raspberry Pi 4 used for the recordings

Storage We asked the HEIA-FR for a storage server in the school to upload the data. They lend us a server with two terabytes of storage accessible from the school network and the internet.

[3] `https://www.raspberrypi.org/products/raspberry-pi-4-model-b/`

Data transmission Since there is no network cable on the HEIA-FR's balcony, we use a 4G modem lent by the HEIA-FR to transmit the data to the storage server. We use a 4G LTE N300 router from D-Link [4] (Figure 4.5) to transmit the data. We use a SIM card from Swisscom, also lent by the school to transmit the recordings via the Internet.

Figure 4.5: D-Link router used for the recordings

We connect the raspberry pi to the router via an ethernet cable and the router access to the internet via the 4G modem. They are put in a waterproof suitcase to protect them from the weather (Figure 4.6).

Figure 4.6: 4G router and modem in their case

3D support To attach the microphones, we design 3D pieces with CAD software to 3D print them. We use *tinkercad* to design the pieces. After the design, we give the 3D models to the mechanics at ROSAS to 3D print them (Figure 4.7).

[4] https://eu.dlink.com/

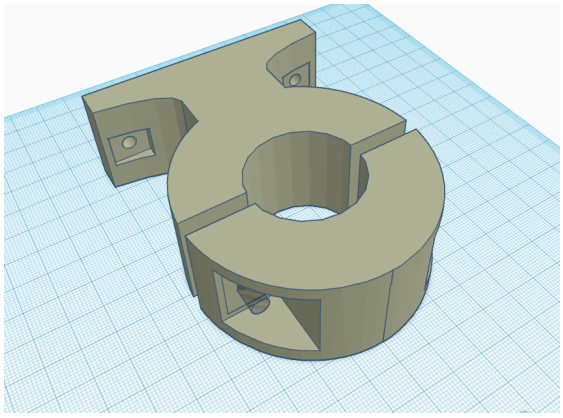


Figure 4.7: 3D pieces

We installed the microphones on the barrier with the 3D-printed clamp (Figure 4.8).

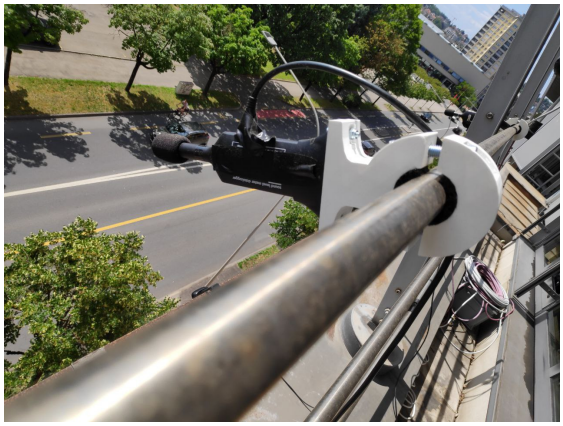


Figure 4.8: Microphones installation on the barrier.

We can see the complete setup in Figure 4.9. We can see the yellow case containing the Raspberry Pi and the two microphones with their 3D-printed support. We taped the camera to the side of the balcony. We connect the microphones with a 3-meter USB cable to the Raspberry Pi. The HEIA-FR'balcony has a roof, so the hardware is protected from rain.

Figure 4.9: Hardware installation on the HEIA-FR's balcony.

Once we made the installation, we can start the recordings.

4.1.2 Software for the recordings

To record the data, we must have software to control the hardware. We must also have software to transmit the recorded data to the storage server. This subsection describes the software used to make the system work.

Operating system We used *Raspberry Pi OS* [5] as the operating system for the Raspberry Pi because it is the official operating system and has a great community helping each other. It is based on *Debian* [6] and is optimized for the Raspberry Pi. It is also easy to install and use.

Audio recording Since each microphone has its sound card, we must treat them as one sound card per microphone on the operating system. This can cause issues if we start the recording at a slightly different time. This problem can, for example, be the case when we execute two consecutive commands, one after the other, in a script to start the microphone recording. We can use *Advanced Linux Sound Architecture (ALSA)* [7] to manage each sound interface and combine them into one virtual sound interface to be able to start the record from both sound cards at the same time. We can do this setup in a configuration file for ALSA. We used the following configuration file to combine the two sound cards into one virtual sound card:

```
pcm.mic1 {
  type hw
  card NSRTmk3Dev
  device 0
}

pcm.mic2 {
  type hw
  card NSRTmk3Dev_1
  device 0
}
```

[5] https://www.raspberrypi.org/software/operating-systems/
[6] https://www.debian.org/
[7] https://www.alsa-project.org/

```
pcm.mic12 {
  type multi
  slaves.a.pcm mic1
  slaves.a.channels 1
  slaves.b.pcm mic2
  slaves.b.channels 1
  bindings.0.slave a
  bindings.0.channel 0
  bindings.1.slave b
  bindings.1.channel 0
}
```

This configuration file will create a virtual sound card called mic12 that will combine the two sound cards: *mic1* and *mic2*. We can then use this virtual sound card to start the recording on both sound cards simultaneously.

Video recording and synchronization We use *ffmpeg* [8] to record the video and the audio synchronously. The command used to record the video and the audio is the following:

```
ffmpeg -f alsa -thread_queue_size 2048 -i plug:mic12 -f v4l2 -thread_queue_size
↪ 2048 -input_format mjpeg -video_size 600x400 -i /dev/video0 -c:a aac -map 0:a -
↪ map 1:v -segment_time 00:10:00 -f segment /mnt/videos/$current_date/output%05d.
↪ mp4
```

This command combines the video from the device */dev/video0* and the virtual sound card *mic12* in a single file containing audio and video.

Before installing the system on the HEIA-FR balcony, we calculated the delay between the video and the audio by clapping in front of the webcam and the microphones. Since the delay found was inferior to 100 milliseconds and we only recorded two seconds of video to provide ground truth, we admitted it was negligible for the dataset annotation task.

Raspberry Pi access for administration We used a server from the HEIA-FR to store the data. We can access the server through OpenSSH on the local network of the HEIA-FR.

Since we don't want to go to the HEIA-FR every time we want to access the Raspberry Pi, and we don't want to have ports open on the internet, we use *remote.it* [9] to access the Raspberry Pi remotely. *Remote.it* is a service that allows us to access the Raspberry Pi remotely without opening ports on the internet. It creates a VPN between the Raspberry Pi and the *remote.it* server and gives us the VPN address on the *remote.it* web application. We can then access the Raspberry Pi through the VPN.

Data transmission Since the data we transmit could be sensitive, we transferred it using a secure file transfer protocol. SFTP is a network protocol that provides file access, file transfer, and file management functionalities over a secure channel. We used *OpenSSH* [10] to transfer the data. OpenSSH is a suite of secure networking utilities based on the Secure Shell (SSH) protocol. OpenSSH encrypts all traffic (including passwords) to eliminate eavesdropping, connection hijacking, and other attacks. To transfer the data, we mounted the storage server as a local drive on the Raspberry Pi by using the following command:

```
sshfs drosset@proxy51.rt3.io:/home/drosset/workspace/videos /mnt/videos -p 33838
```

[8] https://www.ffmpeg.org/
[9] https://remote.it/
[10] https://www.openssh.com/

This command will ask for a password to connect to the server and provide us with a local drive on the Raspberry Pi that is, in reality, the server's drive. We can then use this local drive to store the data directly on the storage server.

4.2 Dataset creation

For most of the dataset management, we used Python. Python is a programming language that gives us many dataset management tools. We used Python to split the recordings into smaller files, annotate the dataset, and manage the folders.

Once we set up the hardware and the software allows us to record the vehicles on the street, we can build a dataset. The recordings of the vehicles contain audio and video in mp4 files of ten minutes each. We must split the recordings into smaller files to get to the two seconds of length defined in section 3.1.1. We split the recordings into two seconds files. Since splitting a video can be time-consuming, we launch it in a subprocess to execute it concurrently on multiple files. We used the following script:

```
for file in files:
    subprocess.call(['ffmpeg', '-i', directory + '/' + file, '-c:v', 'libx264', '-crf',
    ↪  '22', '-map', '0', '-segment_time', time, '-reset_timestamps', '1', '-g', '30',
    ↪  '-sc_threshold', '0', '-force_key_frames', 'expr:gte(t,n_forced*'+str(time)+')'
    ↪ , '-f', 'segment', directory[:-1]+'-2sec/' + file + '%05d.mp4'])
```

This script allows to have two seconds of video clips of the vehicles. We can then annotate the dataset.

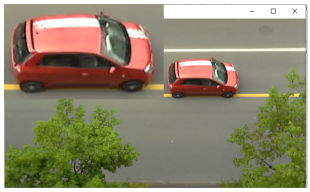
4.2.1 Dataset annotation

A good practice when creating a dataset to classify it is to put the files in folders. Each folder represents a class. In our case, we use the classes defined in section 3.1.2:

- *left_to_right*: Key: **D** The vehicle goes from the left to the right of the microphone.
- *right_to_left*: Key: **A** The vehicle goes from the right to the left of the microphone.
- *no_cars*: Key: **S** No vehicles pass by the microphone.
- *multiple_cars*: Key: **W** Multiple vehicles pass by the microphone.

Each class has its folder. We can then annotate the dataset by moving the files to the correct folder. We developed a tool to annotate the dataset. The tool is an application that shows a 2-second video from the recordings. The user can then press a key in the application to automatically move the video to the class folder. The user can also press a "cancel" key to remove the last annotated video if the user makes a mistake. Figure 4.10 (a) shows an example of the tool. We can see multiple vehicles in this video. The user can press the **W** key. In Figure 4.10 (b), we see only one vehicle going from right to left. The user can then press the **D** key to save the file in the correct folder.

(a) Multiple car



(b) Left to right

Figure 4.10: Dataset annotation tool

Since the videos only show vehicles moving on a road, we don't need to play the video at real speed. The tool plays the video accelerated to gain time when annotating the dataset.

4.2.2 Dataset

The annotation was done for 2037 videos and defined our baseline dataset for the project. The dataset contains 2037 videos of two seconds each. We split the dataset into four classes. The statistics for the classes are the following:

```
classes:  ['left_to_right', 'multiple_cars', 'no_car', 'right_to_left']
total files:  2037
total files for class left_to_right:  513
total files for class multiple_cars:  234
total files for class no_car:  582
total files for class right_to_left:  708
```

We represent the statistics as a table in Table 4.1.

Class	Number of files
left_to_right	513
multiple_cars	234
no_car	582
right_to_left	708

Table 4.1: Dataset statistics

We made a script to shuffle the dataset and split it into training and test sets. The script's parameter defines the proportion of data in the train and test set. We use the training set to train the neural network and the test set to evaluate the neural network. The script output the number of files in each set. For example, when we run the script with a 70% train and a 30% test, the script gives us the following output:

```
classes:  ['left_to_right', 'multiple_cars', 'no_car', 'right_to_left']
files in train set:  1426
files in test set:  611
total files:  2037
ratio:  0.29995090819833087
```

The script calculates the ratio to ensure that the proportion of data in the train and test set is correct.

4.2.3 Dataset annotation from audio

Since the project aims to use audio to annotate the dataset, we also create a dataset from the audio. We can use the same tool to annotate the dataset. The tool plays the audio of the video instead of the video. The user can then press the same keys to annotate the dataset. Since we use two microphones, we can play the audio in a stereo headset to have all audio channels listenable during the annotation. We can then compare the results of the dataset annotated from the audio only with the results of the neural network trained on the dataset annotated from the video.

4.3 Neural Network for Sound Source Localization

For the neural network implementation, we use Python. Python is a popular programming language for machine learning. It is easy to use and has a lot of libraries for machine learning. The machine learning

library we use is *PyTorch* [11]. We use it because it is popular, open-source, and free. It also has a lot of documentation. Pytorch allows us to create neural networks in Python. It helps us create the neural network architecture, load the data, train the neural network, and test it. It uses the concept of tensor to represent the data. A tensor is a multidimensional array. To manage the arrays on the Python side, we use the *numpy* [12] library. We also use the *matplotlib* [13] library to plot the results.

The shape of a tensor is a representation of the size of each of their dimension and their sizes.

4.3.1 Data loading

Once we have annotated the dataset, we can load the train set in as a matrix. The matrix contains a dimension for each sample, a dimension for each channel, and a dimension for each time step. In parallel, we keep an array with every label for each sample. We then convert the matrix to a tensor with shape ([1422, 2, 88200]). The first dimension is the number of samples in the train set (here, 1418). The second dimension is the number of channels (here, two since we recorded with two microphones). The third dimension is the number of samples (here 88200, which is two times the used sampling rate since we recorded for two seconds).

4.3.2 Data preparation

Since we want to input spectrograms into our network, we need to convert the audio samples to spectrograms. We use the *torchaudio* [14] spectrogram implementation to convert each sample to a spectrogram. The spectrogram function has the following parameters:

- **n_fft**: the number of Fourier bins. We use 1000 bins.
- **win_length**: the length of the window to use to compute the spectrogram. We use a window of 1000 samples.
- **hop_length**: the length of the hop to use to compute the spectrogram. We use a hop of 1280 samples.
- **window**: the window to compute the spectrogram. We use a Hann window of 1000 samples.
- **normalized**: whether to normalize the spectrogram. We use a normalized spectrogram.

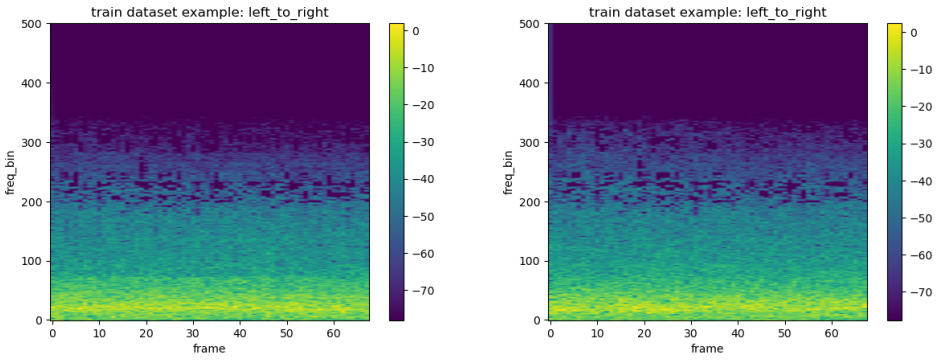
The spectrogram function returns a tensor with the shape [1422, 2, 501, 69]. The first two dimensions are the number of samples and channels. The third dimension is the number of frequency bins (here, 501). The fourth dimension is the number of time steps (here, 68). These parameters are the result of the spectrogram function parameters. The number of frequency bins is the number of Fourier bins divided by two plus one. The number of time steps is the number of samples minus the window length divided by the hop length plus one.

$$\text{number of frequency bins} = \frac{\text{number of Fourier bins}}{2} + 1 = \frac{1000}{2} + 1 = 501 \tag{4.1}$$

$$\text{number of time steps} = \frac{\text{number of samples} - \text{window length}}{\text{hop length}} + 1 = \frac{88200 - 1000}{1280} + 1 = 69 \tag{4.2}$$

[11] https://pytorch.org/
[12] https://numpy.org/
[13] https://matplotlib.org/
[14] https://pytorch.org/audio/stable/generated/torchaudio.transforms.Spectrogram.html

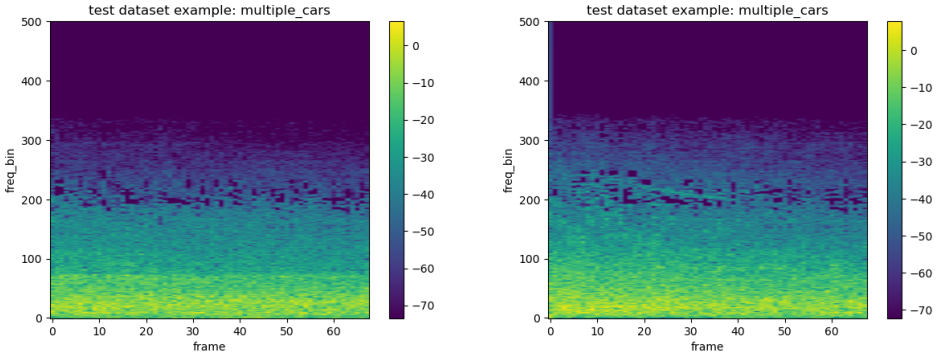
After the spectrogram process, we can visualize some spectrograms. Figure 4.11 shows some spectrograms from the train set.



(a) Channel 0 (b) Channel 1

Figure 4.11: Spectrograms for each channel from the train set

And Figure 4.12 shows some spectrograms from the test set.



(a) Channel 0 (b) Channel 1

Figure 4.12: Spectrograms for each channel from the test set

It is hard to tell the difference between the spectrograms even when they are in two different classes. That's why we use a neural network to classify them.

4.3.3 Convolutional Neural Network architecture

We use the architecture defined in section 3.2. Based on the input dimension, it gives the architecture in Figure 4.13. We generate this by using the *sumarry* function of library *torchsumarry*[15]. The *sumarry* function takes a neural network as input and returns the architecture of the network.

[15] `https://pypi.org/project/torchsummary/`

```
==========================================================================================
Layer (type:depth-idx)                   Output Shape              Param #
==========================================================================================
├─Sequential: 1-1                        [-1, 8, 100, 13]          --
|    └─Conv2d: 2-1                       [-1, 8, 501, 68]          408
|    └─ReLU: 2-2                         [-1, 8, 501, 68]          --
|    └─MaxPool2d: 2-3                    [-1, 8, 100, 13]          --
├─Sequential: 1-2                        [-1, 16, 33, 4]           --
|    └─Conv2d: 2-4                       [-1, 16, 100, 13]         3,216
|    └─ReLU: 2-5                         [-1, 16, 100, 13]         --
|    └─MaxPool2d: 2-6                    [-1, 16, 33, 4]           --
├─Sequential: 1-3                        [-1, 32, 16, 2]           --
|    └─Conv2d: 2-7                       [-1, 32, 33, 4]           12,832
|    └─ReLU: 2-8                         [-1, 32, 33, 4]           --
|    └─MaxPool2d: 2-9                    [-1, 32, 16, 2]           --
├─Linear: 1-4                            [-1, 4]                   4,100
==========================================================================================
Total params: 20,556
Trainable params: 20,556
Non-trainable params: 0
Total mult-adds (M): 19.50
==========================================================================================
Input size (MB): 0.26
Forward/backward pass size (MB): 2.27
Params size (MB): 0.08
Estimated Total Size (MB): 2.61
==========================================================================================
```

Figure 4.13: Convolutional Neural Network architecture from Torchsumarry

We can better visualize the network architecture with Figure 4.14. It shows us the different layers that we apply to the network.

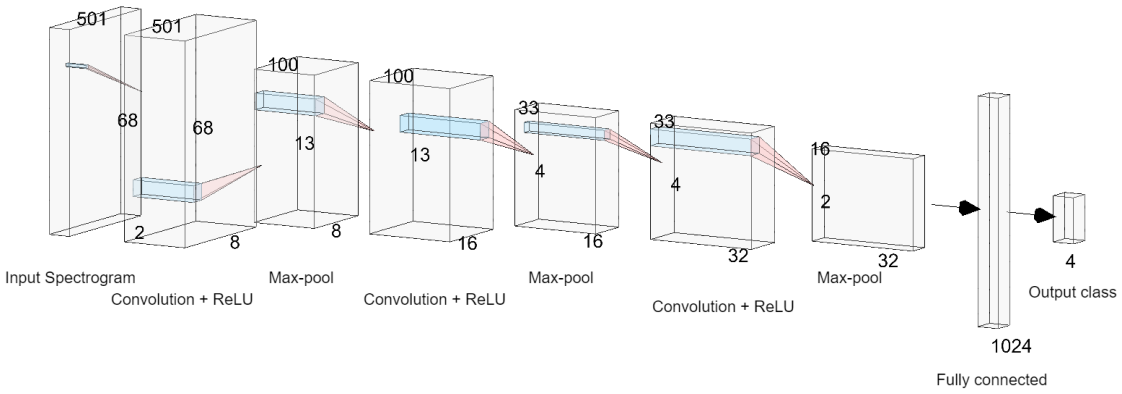


Figure 4.14: Convolutional Neural Network architecture

We added a dropout layer between the last layer and the output. It will help to prevent overfitting.

Our dataset is unbalanced, so we use the weighted cross-entropy loss function. We use the pytorch implementation of the weighted cross-entropy loss function[16].

We use the Adam optimizer with a learning rate of 0.001 by using the PyTorch implementation of the Adam optimizer[17].

We also use a scheduler to reduce the learning rate when the loss function stops decreasing. We use the PyTorch implementation of the ReduceLROnPlateau scheduler[18]. This will change the rate at which the optimizer will change the weights of the neural network.

4.3.4 Training

When training, we have to define some more parameters for the training. We use the following parameters:

[16] https://pytorch.org/docs/stable/generated/torch.nn.CrossEntropyLoss.html

[17] https://pytorch.org/docs/stable/generated/torch.optim.Adam.html

[18] https://pytorch.org/docs/stable/generated/torch.optim.lr_scheduler.ReduceLROnPlateau.html

- **batch_size**: the number of samples to use in one batch. We use a batch size of 32.
- **patience**: the number of epochs to wait before reducing the learning rate. We use a patience of 3 epochs.
- **weight_decay**: the weight decay. We use a weight decay of 1e-3.

We don't use the epochs count to stop the training. We use the ReduceLROnPlateau scheduler to stop the training when the learning rate is less than 1e-7. Which means that the model is nearly not learning anymore.

4.3.5 Training hardware

We used a computer with the following specifications to train the neural network:

- **CPU**: Intel Core i7-10700K
- **GPU**: NVIDIA GeForce RTX 4070 Ti
- **RAM**: 32 GB

The important part of the hardware is the GPU. Since machine learning comprises many parallelizable operations, it is much faster on GPU. We use CUDA[19] to use the GPU. CUDA is a parallel computing platform and application programming interface model created by Nvidia. It allows us to use the GPU to train the neural network. The Pytorch library does the CUDA integration. To use the GPU, we have to tell Pytorch to move the model and the data on the GPU by using the *.to('cuda')* function.

This hardware helps us to train the neural network faster. We can train the neural network in 2 minutes on this hardware. If we don't use the GPU, the training time is multiplied by 40. The short training time allows us to train the neural network multiple times and to try different parameters.

Once we train the network, we can use it to classify the data by giving new input data to the network. After each training, we save the model to be able to use it later.

4.3.6 Training visualization

We use *Tensorboard*[20] to visualize the training. Tensorboard is a visualization toolkit for machine learning experimentation. Figure 4.15 shows the Tensorboard interface.

[19] https://developer.nvidia.com/cuda-toolkit
[20] `https://www.tensorflow.org/tensorboard`

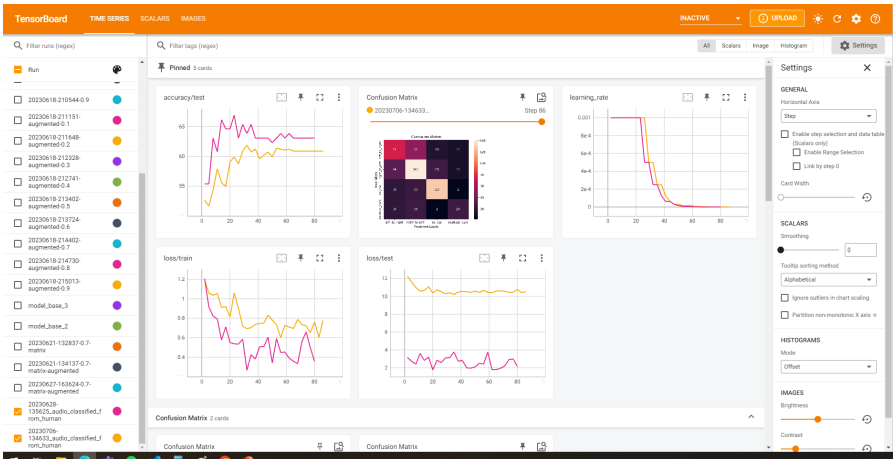


Figure 4.15: Tensorboard interface

It allows us to visualize the training loss and accuracy during the learning process. It helps to understand if we choose good hyperparameters for the training or if the neural network is learning. It also helps to compare the results between training.

4.4 Simulation model creation

To create a dataset in simulation, we use Unity combined with the *Microsoft Project Acoustic*[21] plugin. The combination of the two allows us to create a simulation of a street with vehicles passing by and to record the sound of the vehicles. We can then use the recorded sound to create a dataset. We can then use the dataset to train a neural network.

The simulation is also faster than recording the data from real life. We can generate a lot of data in a short time. The simulation is also cheaper than data recording since we only need a computer. The simulation is also more flexible than recording the data. We can change the position and comportment of every object in the simulation at any time.

4.4.1 Unity

We reproduced a street in Unity. We used the Unity Asset Store[22] to get the assets to create the street. Figure 4.16 shows the street in Unity.

[21] https://learn.microsoft.com/en-us/gaming/acoustics/what-is-acoustics
[22] `https://assetstore.unity.com/`

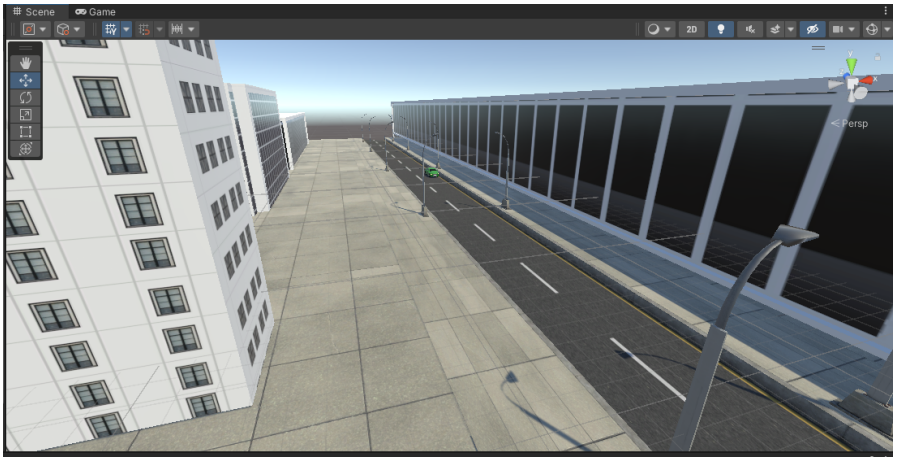


Figure 4.16: Street in Unity

4.4.2 Microsoft Project Acoustic plugin

The Microsoft Project Acoustic plugin allows us to simulate sound propagation in the scene. We can add it in Unity's plugin tab by following Microsoft's guide[23]. Once we add it, we need to voxelize the scene to define which 3D surface the sound will bounce. Voxelization is the process of averaging a 3D model with squares. The plugin does the voxelization and takes a short time to complete. Figure 4.17 shows the voxelization of the scene. Each green square represents a voxel.

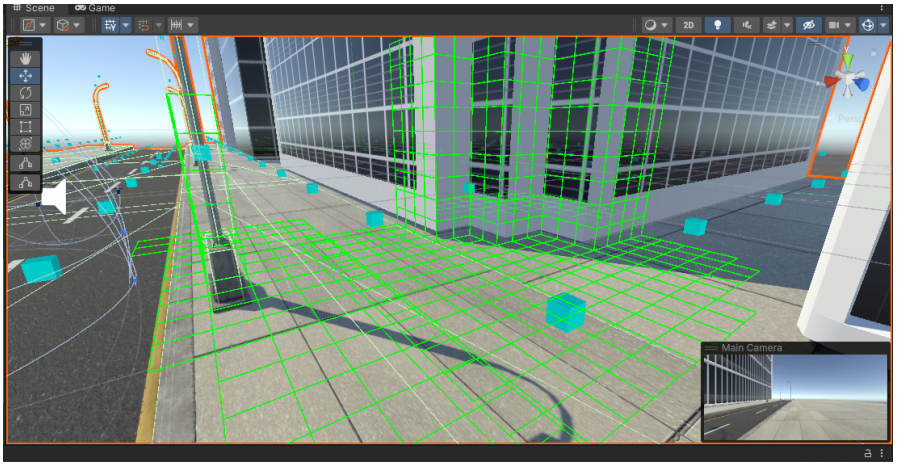


Figure 4.17: Voxelization of the scene

Once we finish the voxelization, we can bake the scene. Although Microsoft proposes using their Azure cloud service[24] to bake the scene, we can also bake it locally. The baking process uses docker[25] to set up the environment. The baking process takes a lot of time to complete. It took us around 2 hours to

[23] https://learn.microsoft.com/en-us/gaming/acoustics/unity-integration
[24] https://azure.microsoft.com/fr-fr
[25] https://www.docker.com/

bake the scene. If we had to bake the scene multiple times, we could use the Azure cloud service to bake the scene faster.

Multiple channel recording in Unity In unity, by design, only one audio listener can be active at a time [26]. This design means that we can only record one channel at a time. To record multiple channels, we have to record each channel separately. We solve this issue by creating a script that will record each channel separately by moving the audio listener to the microphone's predetermined positions and recording the sound. We then merge the channels to create a multi-channel audio file.

4.4.3 Managing sound in game engine

In game engines, sounds travel instantly. This concept means that if we play a sound, we will hear it instantly. In real life, sound travels at 343 m/s, so we will hear it after the time it takes for the sound to travel the distance separating us from the sound origin. We have to take this into account when we create the simulation. We have to play the sound at the right time. We have to calculate the time it takes for the sound to reach the microphone. We can calculate the time with the following formula:

$$t = \frac{d}{v} \tag{4.3}$$

Where t is the time, d is the distance between the sound source and the microphone, and v is the speed of sound. The speed of sound is 343 m/s. We can then play the sound after the calculated time.

Since we record each channel separately, the time difference between each channel depends on the microphone's position. We show an example of this effect in figure 4.18 with a large distance between each microphone.

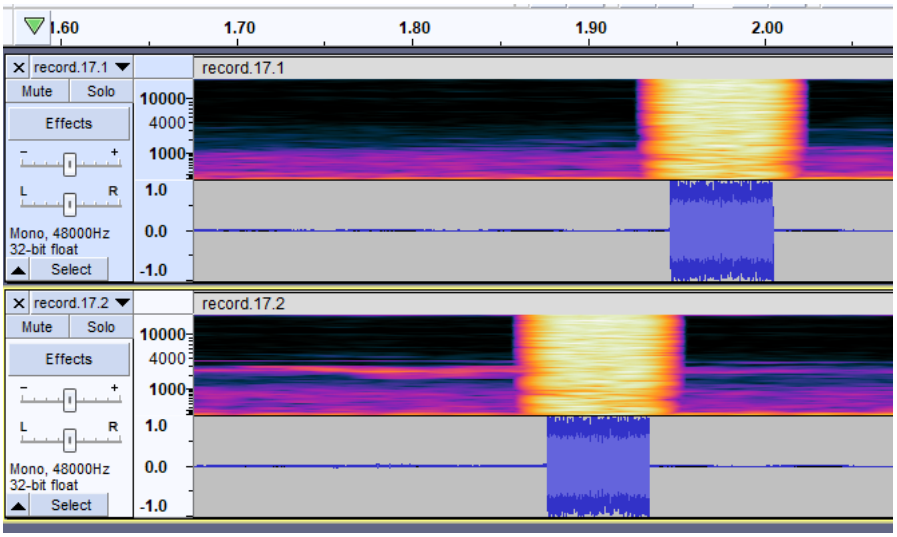


Figure 4.18: Time difference between channels

Recording the sound To record the sound, we use the *AudioListener* component of Unity and gather each sample of the sound. We then save the samples in a wav file. We use *SavWav.cs* script created by

[26] https://docs.unity3d.com/Manual/class-AudioListener.html

darktable [27] to create the file and save data in it.

4.4.4 Creating the dataset

We can create a folder corresponding to the class based on each class defined in section 3.3. When the simulation runs, it saves the audio file in the correct folder. Since the simulation always knows the state of the objects, we can use this information to define in which folder we need to save the audio file. This process allows us to create a dataset based on the same design as the one created with real-life data.

Once we create the dataset, we can extend the training dataset created with real-life data to improve the neural network's performance. We achieve the extension of the real-life dataset by loading the dataset the same way as the real-life dataset (in section 4.3.1) and extending the matrix containing the real-life dataset. We then train the model with the extended dataset by following the procedure described in section 4.3.4. We generated 1267 audio files with the simulation. We then added them to the training dataset.

We detail the results of this process in section 5.4.3.

4.5 Adversarial Attack

To realize the adversarial attack, we needed to have a trained model. We used the model trained on the dataset created with real-life data. We used the *Fast Gradient Signed Method* (FGSM) defined in section 3.4 as the adversarial attack design. Since we saved the model at the end of the training, we can load it and use it to create the adversarial attack.

4.5.1 Adversarial example generation

To generate adversarial examples, we need to do the equivalent of one pass of the training. The goal is to find the gradient direction that maximizes the loss. To find the sign, we can do as follow:

```
loss = criterion(model(input_tensor), label)
loss.backward()
perturbed_input_tensor = input_tensor + epsilon * input_tensor.grad.sign()
```

The $model(input_tensor)$ gives us the model prediction. The $label$ is the true class of the $input_tensor$. The $criterion$ is the loss function. We calculate the loss value when we call $backward()$. Once we find the loss, we can find the gradient direction by taking its sign. Once we have the direction of the gradient, we can multiply our $epsilon$ by the direction to find an image modified to maximize the loss, hence maximizing the miss-classification of the image.

The point of the FGSM on images is to get a modified image undetectable by the human eye. We have to get the smallest $epsilon$ possible to stay undetected. To find the smallest possible $epsilon$, we can run the FGSM multiple times with an increasing $epsilon$ until we find the most efficient value of $epsilon$. This value will show the level of resistance of the model to adversarial attacks.

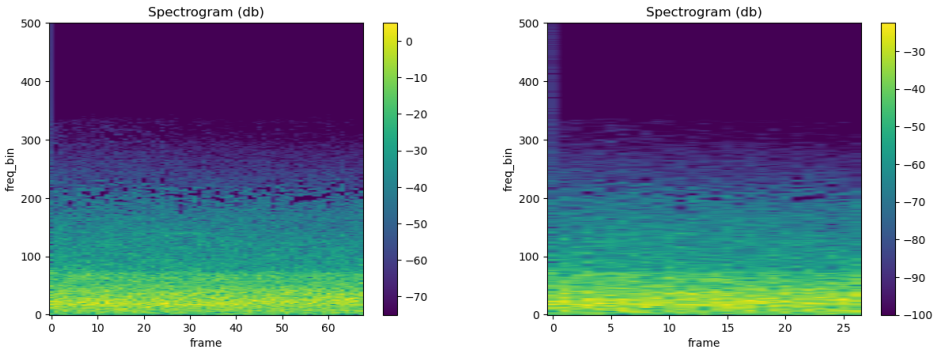
Once we have the $perturbed_input_tensor$, we can save it as an adversarial example.

4.5.2 Audio signal reconstruction

Since we use spectrograms, but our system records audio directly from a microphone, we need to convert the adversarial example to an audio file to attack our system. We use the *friggin-lim* algorithm from *pytorch* to reconstruct the audio signal from the spectrogram. Since going through a spectrogram and back to an audio signal uses multiple approximations, the reconstructed audio signal will differ from the original

[27] https://gist.github.com/darktable/2317063

audio signal. We can see that the signal loses some of its information and has a smaller definition in figure 4.19.



(a) Audio signal before reconstruction

(b) Audio signal after reconstruction

Figure 4.19: Spectrograms before and after the reconstruction

5 Results

This chapter presents the results of the realizations conducted in the previous chapter. It proposes an analysis of the next steps that someone in the future could take to improve the system.

5.1 Objectives fullfilement

5.1.1 Recording system

Once we installed the recording system on the HEIA-FR building, it allowed us to record the street at any time and generate large amounts of data. The system was reliable, always available, and thanks to the script to run it, it was also easy to use.

Problems encountered We first tried streaming the data directly from the raspberry pi to the storage server with the Real-time Transport Protocol (RTP) [1]. By default, the RTP protocol did not encrypt the streamed data. The *FFMPEG* encoding buffer was regularly full, which caused the loss of some frames and some artifacts in the audio, and the streaming technique gave us a bad image quality due to the real-time encoding of the video.

We solved all these problems by using the SFTP protocol. We solved the image quality by mounting the storage server's folder on the raspberry pi as a network driver. Since FFMPEG no longer used the RTP, it could take his time to encode the video in good quality and save it. The SFTP use also solved the buffer issue. Finally, the SFTP protocol allowed us to encrypt the data since it's a secure protocol by default. An example of the difference between the two method's quality can be seen in the figure 5.1.

[1] `https://fr.wikipedia.org/wiki/Real-time_Transport_Protocol`

(a) Frame quality with RTP

(b) Frame quality with SFTP

Figure 5.1: Comparison of the frame quality between the two streaming methods

Even if the quality difference is not considerable, getting a better quality by using the SFTP protocol was a nice side effect of changing the streaming method.

5.2 Definition of the baseline

With the analysis and design parts of the report (section 2.1 and 3.1), we defined the baseline as a set of steps to follow to achieve the goal of this project. The baseline described in this report is accurate and complete enough to be followed by someone else in the future. The definition achieves the first objective of creating a baseline in section 1.1.1.

5.3 Real-life dataset

With the recording system in place, we built a dataset for this project comprising 2028 dual-channel audio and video files of 2 seconds classified into four classes. The realization of this dataset achieves the goal defined in section 1.1.1 of having a dataset that follows the baseline to train our model. The dataset is complete and follows the baseline. It is also large enough to train a model with it. The dataset's creation solves the problem of the lack of a dataset for this project. We can consider the objective defined in section 1.1.1 as achieved.

Although the dataset is created and follows the baseline, we challenge it in the next section ()5.4).

5.4 Neural Network model results

We trained the neural network multiple times and tested it on the test set. The results were not as good as expected. The model could not classify the *no_car* and the *multiple_cars* classes well. The model could not accurately classify the *right_to_left* and *left_to_right*. We trained the model with different percentages of the dataset in the train set. First with 60%, then with 70%, and finally with 80%. The results are presented in the table 5.1.

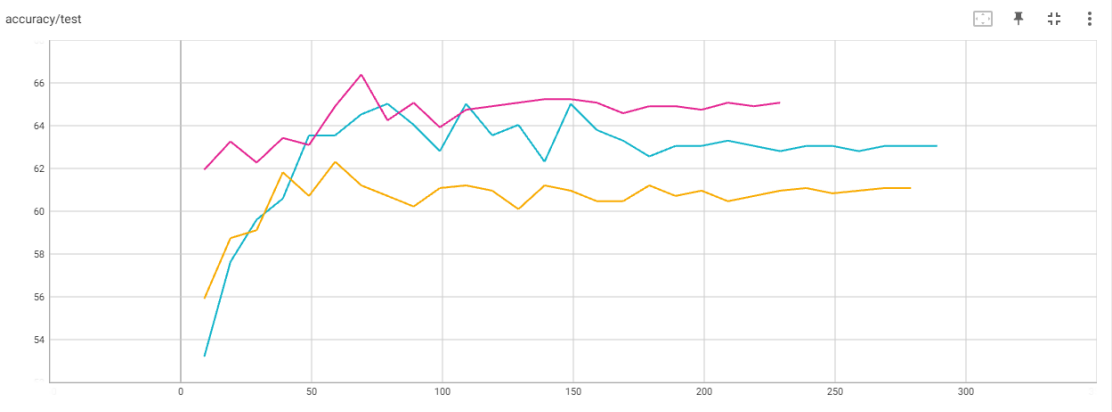


Figure 5.2: Accuracy of the neural network model for each train set proportion. Orange is 60%, purple is 70%, and pink is 80%. X axis is the number of epochs.

We can see that the model trained with 70% of the dataset in the train set is the one that has the best accuracy. It might mean that using the 80% dataset in the train set is too much, and the model overfits the data. If we look at the loss graph (figure 5.3), we can see that the model trained with 60% of the dataset in the train set has a higher loss than the two others.

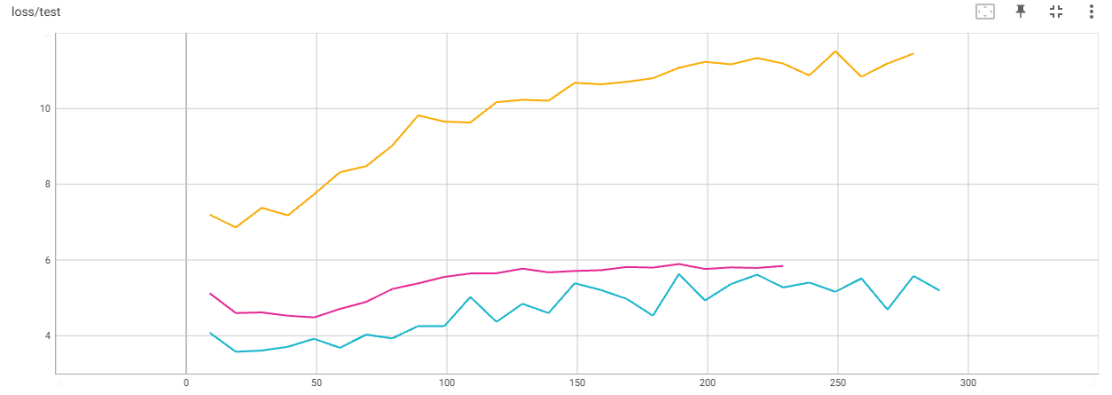


Figure 5.3: Loss of the neural network model each train set proportion. Orange is 60%, purple is 70%, and pink is 80%. X axis is the number of epochs.

Here we see that both the validation loss and the accuracy are increasing. This double increase can happen because the loss function is not always directly related to accuracy. The loss function measures how well the model can predict the correct output. The model may make more confident incorrect predictions, increasing both loss and accuracy.

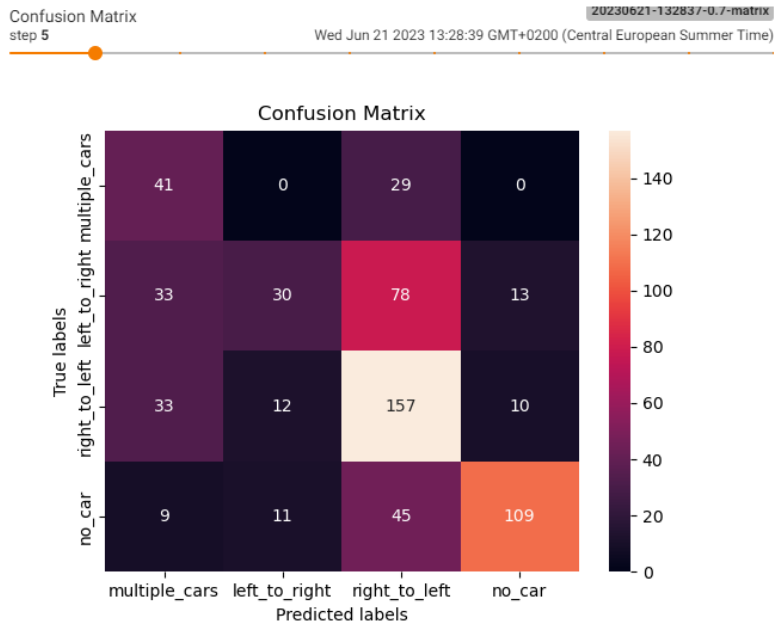
We present the accuracy and loss of the models in Table 5.1. We added the runs with the 40%, 50%, and 90% of the dataset in the train set to the table to show that the model's accuracy and loss are not better with these percentages.

Train set	Test set	Test set accuracy	Test set loss
40%	60%	0.60	21.3
50%	50%	0.61	9.5
60%	40%	0.63	11.4
70%	30%	0.65	5,84
80%	20%	0.61	5.1
90%	10%	0.50	6.3

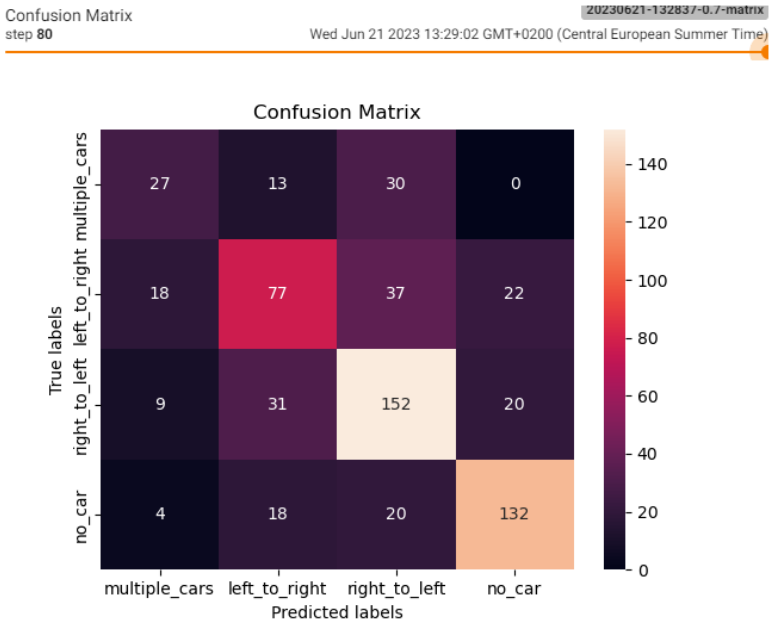
Table 5.1: Accuracy and loss of the neural network model for each train set percentage

We can see in the table 5.1 that the model trained with 70% of the dataset in the train set has the best accuracy and loss. We can also see that the 90% one has the worst accuracy and loss. We can see that the loss with the small train set is big, so the model cannot generalize well. This observation concludes that we need a bigger dataset to train the model.

To better understand with which classes the model is not performing well, we can look at the confusion matrix of the model trained with 70% of the dataset in the train set (figure 5.4).



(a) Epoch 5 (start of the training)



(b) Epoch 80 (end of the training)

Figure 5.4: Confusion matrix of the model trained with 70% of the dataset in the train set

We can see that the model can classify well on the first epochs between the *no_car* and the *multiple_car* class. We can see it by looking at the four corners of the confusion matrix. The corners on the top-left and bottom-right have a high number, while the ones in the bottom left and the top right have a small number.

On the last epoch, the model better predicts the two classes *left_to_right* and *right_to_left*. We can see it by looking at the center of the last epoch of the confusion matrix. Overall, we might have a case of overfitting. To solve this problem, we have multiple possibilities.

- We can do an early stopping of the training. We can stop the training when the loss on the test set starts to increase.
- We also can construct a bigger dataset. Since we could train the model on more data, it would generalize better and be less likely to overfit.

We also have a dataset that is hard to tell when a vehicle is coming from the left or the right. This problem seems to be hard. We could train the model with more data to predict these classes better. We tried to train the model with more parameters to see if it could get better accuracy. We added more convolutional layers and more neurons in the fully connected layers, but the results were not better than this model. To not make the model too big, we decided to keep this model.

5.4.1 Human accuracy

We annotated the test set with only the audio to compare the human and model performance. At this task, the human did only 30.3% accuracy. This accuracy is just slightly better than average. We can see on the confusion matrix (figure 5.5) that the human has difficulty telling when there is a vehicle. He predicted more than 50% of the classes as *no_car*.

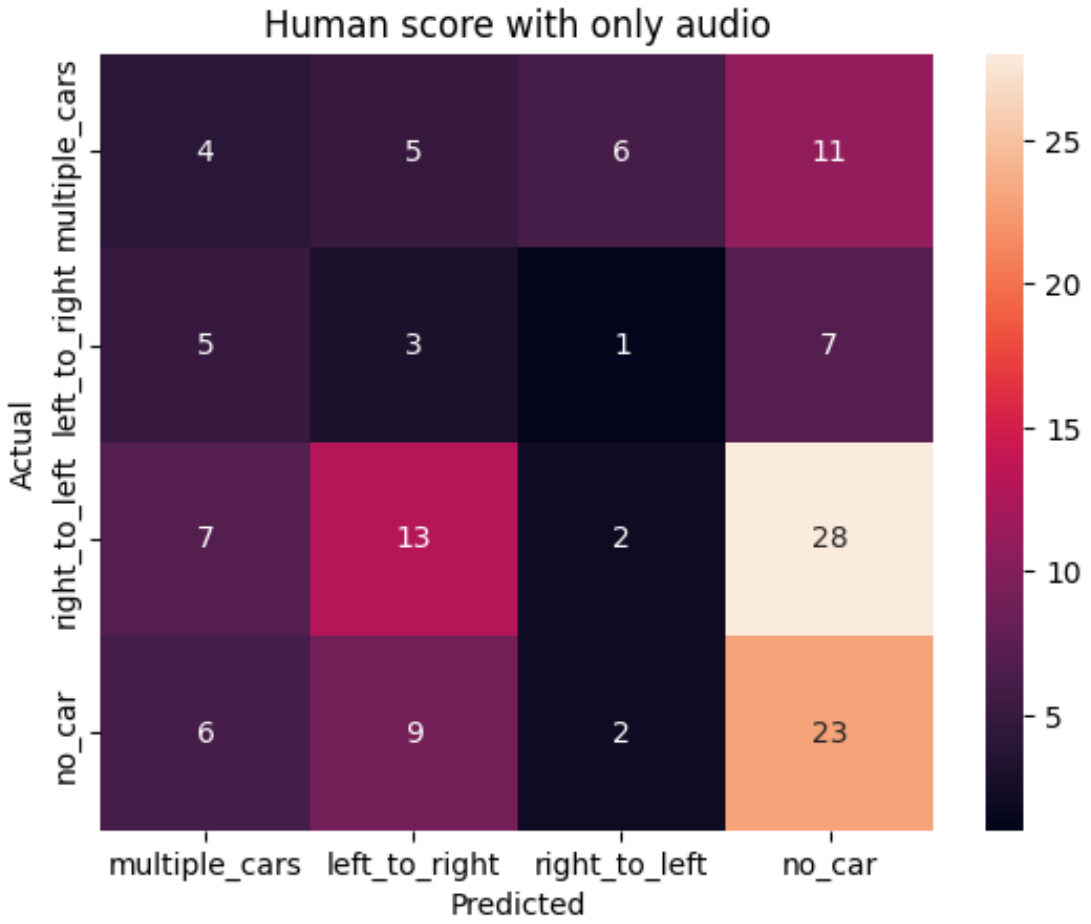


Figure 5.5: confusion matrix of the human on the audio classified set

To have a fair comparison, we tested the model on the same dataset used to confront the human. The model achieved a score of 63.08% with the following confusion matrix (figure 5.6):

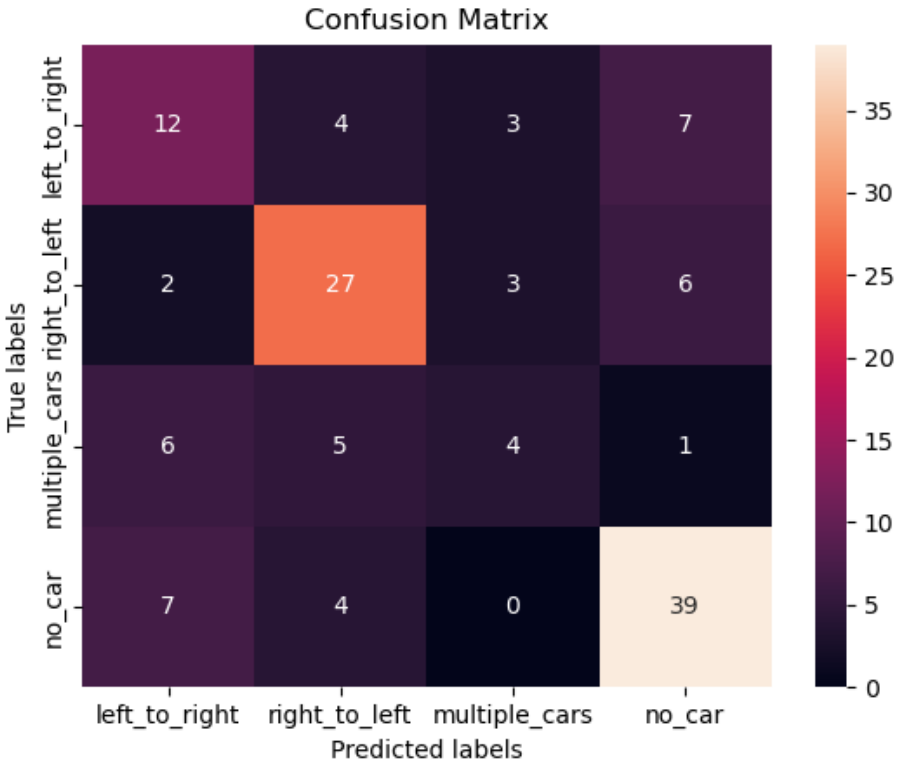


Figure 5.6: confusion matrix of the model on the test set

We can see that the model performs way better than the human.

With this result, we can tell that the objective 1.1.1 is achieved. The model is better than humans at predicting the vehicle's direction with only the audio input. Still, the model could be way better. Achieving 63.08%

5.4.2 Dataset quality

With the results from the convolutional neural network, it's hard to tell if the dataset is well labeled or not. We can see that the model can classify the *no_car* and the *multiple_cars* classes very well. The model could not accurately classify the *right_to_left* and *left_to_right*. This accuracy could mean that the dataset is not well labeled.

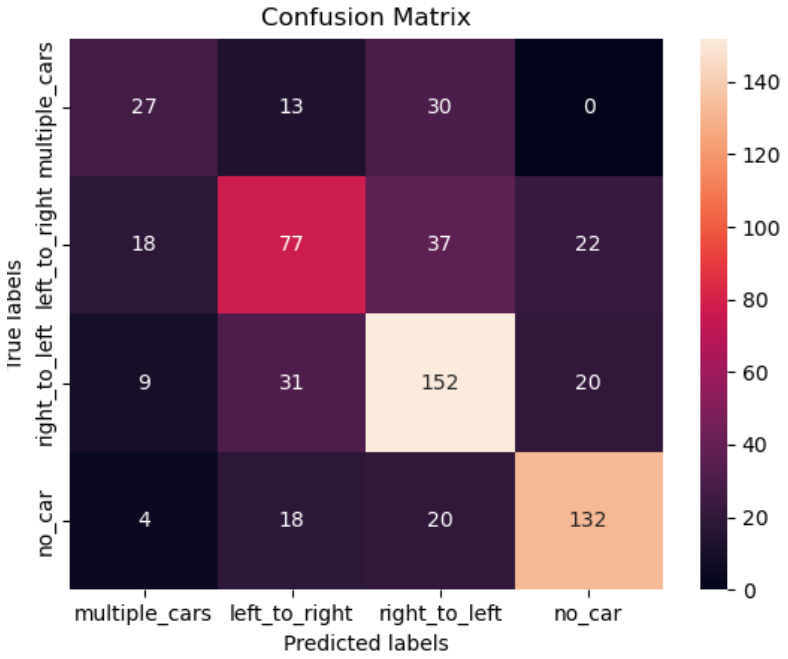
5.4.3 Dataset Augmentation with the Simulation

By adding the simulated data to the real-life dataset, we hoped to see better accuracy for the model. We will call it the augmented dataset. The augmented dataset keeps the same number of real-life samples in the train and test sets. We augment the train with the simulation data. We can see in the table 5.2 that the model trained with 70% of the dataset in the train set has the best accuracy and loss. We can also see that the 90% one has the worst accuracy and loss. We can see that the loss with the small train set is big, so the model cannot generalize well. This observation concludes that we need a bigger dataset to train the model.

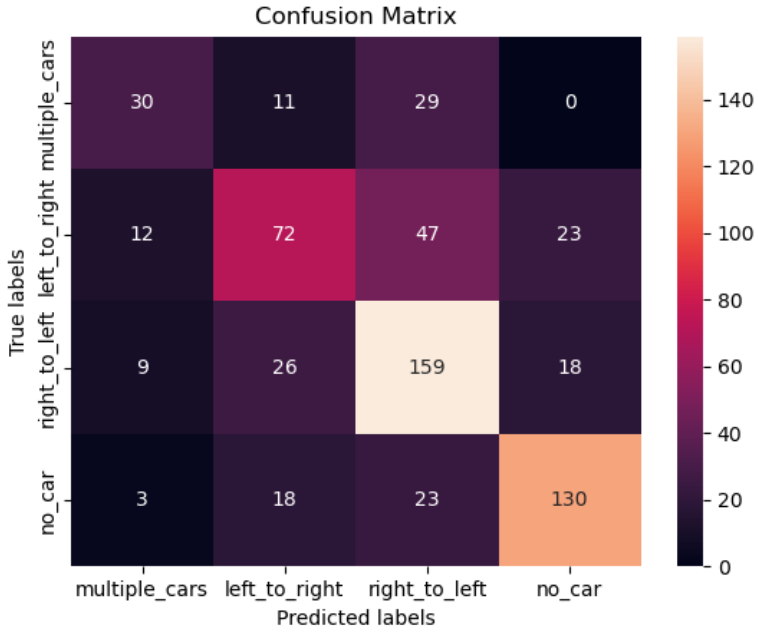
Train set	Real-Life	Augmented
40%	61.71	59.06
50%	61.2	61.22
60%	61.08	61.62
70%	63.77	64.1
80%	63.05	60.64
90%	59.5	59.31

Table 5.2: Accuracy comparisons between the real-life and the augmented dataset for each train set percentage

We can see in the table 5.2 that the augmented dataset does not improve the model's accuracy. We can see that the model trained with 70% of the dataset in the train set has the best accuracy and loss. We can also compare the confusion matrix of both models (figure 5.7). We can see that the augmented dataset does not change a lot the confusion matrix.



(a) Real-life dataset



(b) Augmented dataset

Figure 5.7: Confusion matrix of the model trained with 70% of the dataset in the train set

We can deduce that the simulated data does not help the model. The reason might be that the simulated data is unrealistic, so the models ignore it. It might happen because there are errors in the simulation, and

the generated data contains them.

The objective 1.1.1 was to augment the dataset with the simulation. We only partially fulfilled this objective. We have created a dataset in a simulation, but it does not help the model.

5.5 Adversarial Attack results

We realized the adversarial attacks on the best model of the convolutional neural network. We use the model that uses 70% of the dataset (Table 5.1).

We took every input from the test set that is classified correctly by the convolutional neural network. We try the FGSM with the following $epsilons$: 1e-08, 1e-07, 1e-06, 1e-05, 0.0001, 0.001, 0.01, 0.1, 1.0, 10.0. For each epsilon, we modify the input we chose previously and use it to predict again on the model. This attack gives us the following graph (Figure 5.8).

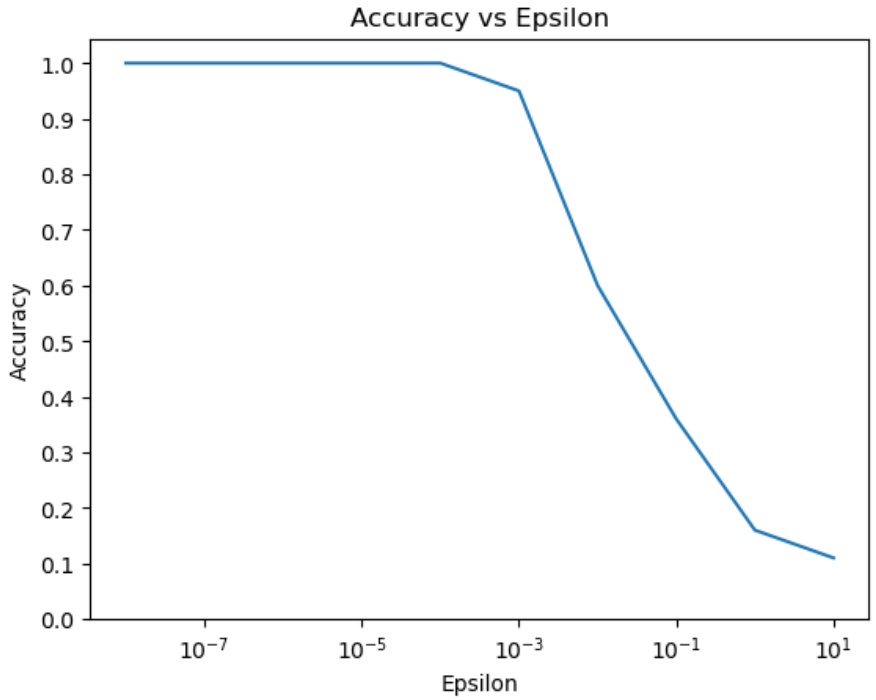


Figure 5.8: Accuracy of the model for each epsilon value with the FGSM attack

We can see that the accuracy is dropping around 10^-3 and 10^-1. We can visualize what happens to the input with the following images (Figure 5.9).

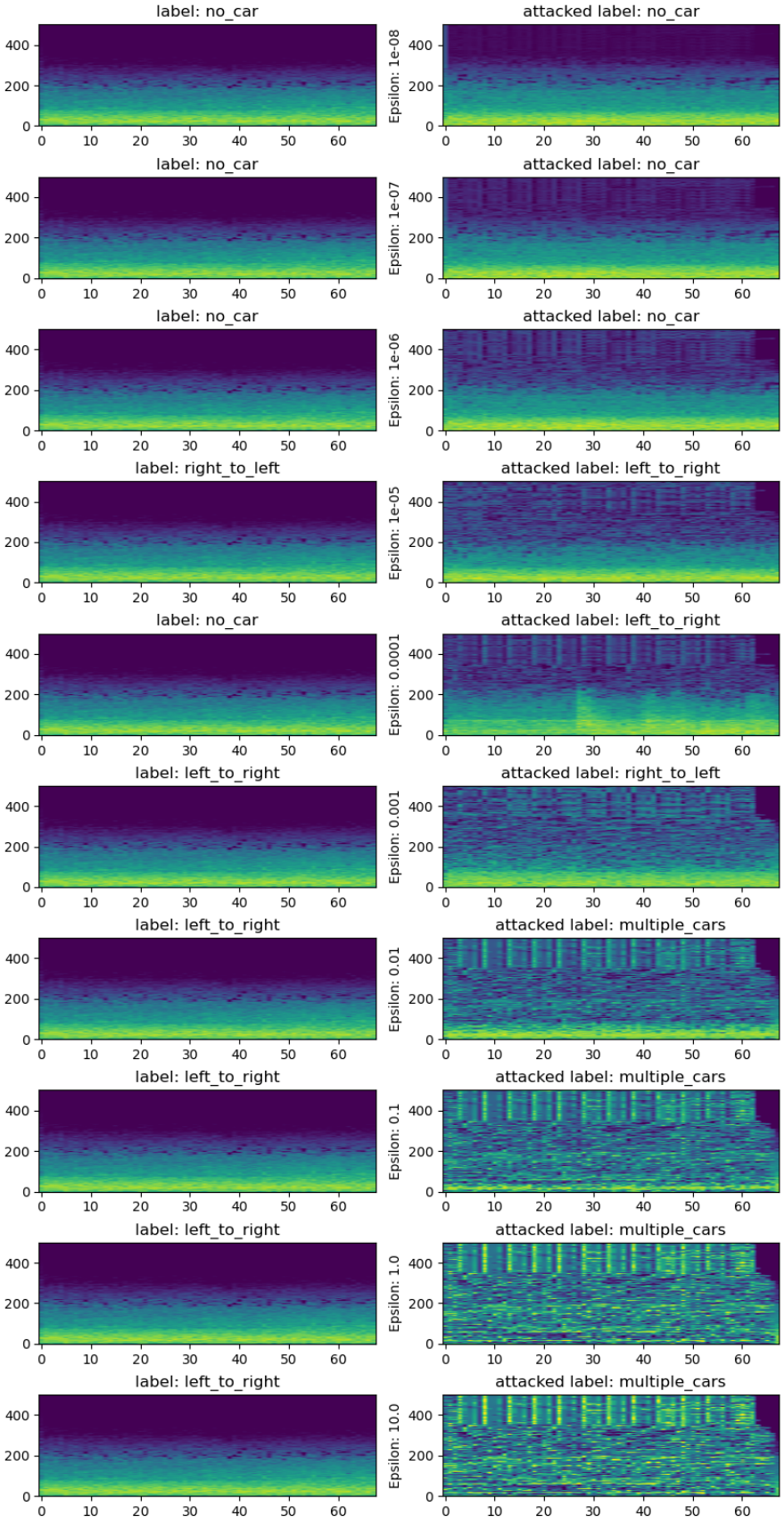


Figure 5.9: Adversarial attack results

We can see that our attack only works when the spectrogram is heavily modified. After reconstructing the audio from the spectrogram, we can hear that the audio is not understandable anymore. It's mainly noise. This attack is not useful for our case because we need audio to produce the exact spectrogram we modified with the attack.

5.5.1 Adversarial Attack mitigation

We can conclude that a CNN that classifies sounds is safer by design than one that classifies images when attacked with the FGSM. The loss of information during the griffin-lim and the Fourier transform makes the model more robust to adversarial attacks.

Even if we managed to attack with a small $epsilon$, the attack would need to play the sound through a speaker. The speaker would not be able to reproduce every small noise that we added to the spectrogram. So the attack would not work in real life without having a considerably different sound. By referring to the objective 1.1.1, we can conclude that we have partially fulfilled it. We have shown that an adversarial attack is possible but useless in a real-life case. We must find an attack that works differently to fulfill this objective completely.

Suppose the attack is possible in a real-life case. In that case, we can mitigate it by following the proposed strategy in [Adversarial Attack Mitigation Strategy for Machine Learning-Based Network Attack Detection Model in Power System][31].

6 Conclusions and Future Work

6.1 Objectives fullfillment

Based on the chapter 5, objectives 1, 2, 3, and 5 are fulfilled. Objective 4 is partially fulfilled.

6.2 Future Work

We created the project for the master's thesis. We were not sure where it would lead us. After the results obtention, we can assume that we set the baseline, and other projects can use it to improve the results. A bachelor's thesis has already begun based on the baseline defined in this project.

6.2.1 Adding more microphones to the recording system

Two microphones might not be enough for a machine learning algorithm to differentiate a sound from the left or the right. The next could be to improve the recording system by adding more microphones. This improvement would modify the dataset by adding dimensions. The current system is limited to two microphones. The system should be able to record four or more microphones. By adding channels to the audio signal, we augment the input dimension of the convolutional neural network, and we can better train it, thus improving the results.

6.2.2 Labelization of more data

Currently, the dataset only comprises a bit more than 2000 samples. By labeling more data, we can compare the results and see if the results are improving. If they improve, we can assume that the dataset needs to be way bigger for the machine learning algorithm to generalize the problem.

6.2.3 Adding more classes

The current baseline is only able to differentiate between four classes. The next step is to add more classes to the dataset. The classes could be more zones that the model would have to discern. Adding classes

would also increase the problem's complexity and require more data to train the model. But it could provide a better tool to build a product we could use in real situations.

6.2.4 Sound Propagation Simulation

The sound propagation simulation was an important part of the project and is not performing well enough. The next part of improving the simulation is the implementation of a real sound propagation that simulates the time needed for the sound to reach the microphone directly into the engine and allows the use of multiple microphones at the same time while managing effects like Doppler occurring when the sound source is moving relatively to each microphone.

Not generating data for the *no_car* and the *multiple_cars* could have been an error.

6.2.5 Sound Propagation Simulation bachelor's thesis

A thesis named *SimSound3D* has started in the HEIA-FR. The goal of this thesis is to improve the sound propagation simulation. They will base their thesis on the work done in this project. At the moment, they have chosen to try to use the Unreal Engine to simulate sound propagation. The student claims to be able to record from multiple positions simultaneously. If the thesis succeeds, it could greatly improve the project.

6.2.6 Advanced adversarial attack

The current adversarial attack is a simple, inefficient attack in our situation. The next step is to improve the attack by using more advanced attacks. The patch attacks presented in [Generative Dynamic Patch Attack][32] could change a zone in the image, thus, making it easier to transform it back to an audio signal without adding lots of noise on the whole spectrogram. This process could improve the attack's efficiency and make it more realistic.

6.2.7 Dataset publication

Since we created a dataset containing more than 2000 labeled samples, we could publish it. Other researchers could use the dataset for their projects. The machine learning community could also use the dataset to improve the project results.

6.3 Specification self-assessment

At the beginning of the project, the specification was going more toward emergency vehicle detection. During the project, we modified the project's objectives to a more generic sound source localization and distance estimation. We adapted the specification to the new objectives.

The planning was designed with three epic deadlines during the project to represent a cyclic workflow. Although the three epic deadlines did not represent three different project realization cycles, they were still useful for providing a global view during the project. The tasks defined in the planning were well followed.

The specification file was a good base to start the project and was a good way to have a global view of what we wanted to do.

6.4 Personal conclusion

It is a great opportunity to work on a project that tries to regroup every part of the IT domain, from embedded systems to machine learning. Even if this project was big and sometimes felt like multiple projects at once, it was a great experience to work on it. I learned much about the different domains and technologies, especially adversarial attacks. I also learned how to manage a project. I am happy with the results, and I am looking forward to seeing the next steps of the project.

A
Appendix

A.1 Source code, graphics, images, and dataset

The source code, the graphics, and the images used in the project are available on the HEIA-FR's gitlab [1].

If you want access to the repository and are not part of the HEIA-FR, contact me at . If you want access to the dataset, you can also contact me via email.

A.2 Specification

[1] https://gitlab.forge.hefr.ch/denis.rosset/sound-source-localization-and-distance-estimation-using-simu

Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Travail de Master / 2023

Computer Science - Cybersecurity

Sound Source Localization and Distance Estimation in Open Environment using Simulation and AI

Specification

03.02.2023 – Version 1.0

Denis Rosset

Supervisors: **Michael Mäder**
Beat Wolf

Principal: **ROSAS**

Versions table

Version	Publication Date	Author	Description
0.1	22.02.2023	Denis Rosset	Draft of specifications
0.2	27.02.2023	Denis Rosset	Objectives and task description
0.3	28.02.2023	Denis Rosset	Planning and milestones
0.4	03.03.2023	Denis Rosset	Modification of the tasks and objectives paragraphs to better suit their purpose Rewriting of some paragraphs Modification of the planning + add of the concept of milestones and epics
0.5	13.03.2023	Denis Rosset	Added a use case for the detection of excessively noisy vehicle in the introduction and rewrote some sentences

Table des matières

1 Introduction

Within the framework of the research project "NPR Teleoperation", the engineers of the HEIA-FR have developed the first concept in Switzerland of a remote-controlled automated vehicle. However, teleoperation only makes sense if the vehicle is automated. There can be no teleoperation without automation (economic factors) just as there can be no automation without teleoperation (legal, technical, and social factors). ROSAS then created the Autovete (Automatisation de véhicules téléopérés) project, financed by HEIA-FR, to build up vehicle automation expertise.

For a vehicle to be fully autonomous, the detection of other emergency vehicles is mandatory. To solve this issue, V2V (Vehicle-to-Vehicle) communication can be used but is not yet integrated on emergency vehicles. So, to be able to detect such vehicle, two signals need to be processed: the sound of the emergency siren and the blinking lights of the vehicle. A first use case of this project focusses only on the sound source distance estimation and localization.

Figure 1 Perceptin: An Autonomous Vehicle

To understand if the sound source estimation and localisation could work for the emergency detection, a simpler use case has been created for this project. It is the detection of excessively noisy vehicle on the street. The goal is to measure the sound level of the passing vehicles and compare it with the legal limits. If a vehicle exceeds the limit, the system can record its license plate and report it to the authorities. This way, the system can help reduce noise pollution and improve road safety.

To implement this use case, the system requires a microphone array, a camera, and a processing unit. The microphone array captures the sound signals from different directions and sends them to the processing unit. The processing unit applies a sound source localization algorithm to estimate the direction and distance of the sound source. The camera captures the image of the vehicle and performs license plate recognition.

Big improvements in sound source localization with the help machine learning are being made1 and can be used to reliably localize the origin of a sound using one or more microphone array (multiple microphones operating in tandem).

A non-negligible problem is that the number of real-world datasets with moving sources in open environment is limited. A solution is to create the datasets in realistic sound propagation simulation.

To validate and use the model, it should also be tested to see how it react against adversarial attacks, understand how it can be used in a real environment and limit the attack vector.

2 Actors

The following actors are part of the project:

- Denis Rosset, Computer Science student, MSE
- Michael Mäder, Professor in Computer Science at HEIA-FR, Supervisor
- Beat Wolf, Professor in Computer Science at HEIA-FR, Supervisor

[1] A SURVEY OF SOUND SOURCE LOCALIZATION WITH DEEP LEARNING METHODS (https://arxiv.org/pdf/2109.03465.pdf)

3 Objectives

3.1 Objective n°1 Dataset according to the baseline

The first objective is to have a dataset constructed. It needs to be coherent with the baseline of the project and should help to create and understand the problem. The dataset should contain the target variable, the features, and the necessary pre-processing steps, such as missing data imputation, data normalization, feature engineering, etc.

3.2 Objective n°2 Model for better sound source localization and distance estimation

The project should use a neural network model to detect the origin of a sound using a microphone array. The neural network should be trained using the dataset created and should be able to accurately localize the sound source. The trained neural network model should be evaluated to see how it performs in a real environment. The model should also be evaluated to see how dependable it is in localizing sound sources and how it can be improved.

3.3 Objective n°3 The model should resist to attacks

The trained neural network model needs to be evaluated to see how it reacts to adversarial attacks. This should be done by testing the model on data that has been modified in some way, such as by adding or removing noise, or by modifying the sound source. The model could also be tested against various types of attacks, such as masking, time-warping, and frequency-shifting. The model should be able to accurately localize the sound source even when it is attacked. The model should also be as robust as possible to come back to a normal operating state once the attack is over.

4 Tasks

The tasks are divided in three main categories. Dataset generation, model creation and model validation.

4.1 Dataset generation

Since no datasets with sound of a vehicle and its relative position in open environment exists, the dataset needs to be created. The dataset of sounds and relative position can then be used to train a neural network. The dataset needs to have a real-life use case so it can be compared later in the project. To achieve that, a baseline needs to be established (i.e. siren sensor, sound recordings) to compare results. Sound spatialization simulation software can be used to generate data in 3D environment. The subtasks are:

- Definition of the baseline
- Create 3D models of different environments
- Generate the dataset using the sound spatialization software
- Evaluate the dataset and make sure it is suitable for training

4.2 Model creation

Creating a model to predict the position of the source of a sound is the second part of the project. The architecture of the model needs to be based on state-of-the-art solution to try getting the most out of the dataset. The dataset needs to be split into multiple smaller datasets (test, train, validate, etc.) to help understanding how the model perform after its training. The subtasks are:

- Research and study of existing models
- Design and implementation of the model
- Train the model on the generated dataset
- Evaluate the model and compare its accuracy

4.3 Model validation

Evaluating the model in a real-world environment is the third part of the project. With the help of microphone arrays, the model should be tested with real-world data to see how it performs in real-world conditions. The results can then be compared to the baseline to see if the model is performing as expected. To ensure the robustness of the system, an analysis of the potential of adversarial attacks against it needs to be done. Propositions of improvements of the model to make it better and more secure should be put down. It should also be tested to see how it reacts to environmental changes (i.e. more open environment, more echo in the street, difference in sound propagation). The subtasks are:

- Evaluate the model against real-world data
- Evaluate the model against environmental changes
- Compare the results against the baseline
- Research and study of adversarial attack that could be applied to this project
- Test the model against the adversarial attack (and how it reacts after the attack)
- Find ways to improve the model and limit attack vector

4.4 Documentation

Task: Write a report that summarize the work done and present the results

- Write a report that summarize the work done
- Presentation of the results

5 Key dates

- 20.02.2023 (SP1) Start of the Master Thesis
- 15.03.2023 (SP4) **Milestone 1** Baseline definition
- 22.03.2023 (SP5) **Milestone 2** Dataset review
- 29.03.2023 (SP6) **Milestone 3** Model review
- 07.04.2023 (SP7) **EPIC 1 + Milestone 4** project review + model validation against baseline
- 28.04.2023 (SP9) **Milestone 5** Dataset review
- 05.05.2023 (SP11) **Milestone 6** Model review (SP 11)
- 17.05.2023 (SP12) **Milestone 7** Validation review
- 26.05.2023 (SP13) **EPIC 2 + Milestone 8** project review + adversarial attack potential
- 09.06.2023 (SP15) **Milestone 9** Dataset review
- 14.06.2023 (SP17) **Milestone 10** Model review
- 23.06.2023 (SP18) **Milestone 11** Model validation + adversarial resistance
- 07.07.2023 (SP19) **EPIC 3** Report deposit
- 14-25.08.2023 Presentation

6 Planning

Week	1	2	3	4	5	6	7		8	9	10	11	12	13	14	15	16	17	18	19
Documentation																				
Specification and planning realization																				
Report																				FR
Dataset Generation																				
Research of existing methods of sound localization																				
Definition of the baseline				1. WE																
Research and creation of baseline datasets and sound simulation software																				
Creation 3D models of different environments																				
Generate a dataset using the sound spatialization software																				
Evaluate the dataset and make sure it is suitable for training					2. WE					5. FR						9 . FR				
Model Creation																				
Research and study of existing models																				
Design and implementation of the model																				
Train the model on the generated dataset																				
Evaluate the model and compare its accuracy						3. WE						6. FR						10. WE		
Model validation																				
Test the model against real-world data																				
Evaluate the model against environmental changes													7. WE							
Compare the results against the baseline							4. FR													
Research and study of adversarial attack that could be applied to this project																				
Test the model against the adversarial attack																				
Find ways to improve the model and limit attack vector														8. FR					11. FR	

EASTER HOLIDAYS

List of Tables

List of Figures

Bibliography

[1] Pierre-Amaury Grumiaux, Srdjan Kitic, Laurent Girin, and Alexandre Guerin. A survey of sound source localization with deep learning methods. *The Journal of the Acoustical Society of America*, 152(1):107–151, jul 2022.

[2] H. S. Black and J. O. Edson. Pulse code modulation. *Transactions of the American Institute of Electrical Engineers*, 66(1):895–899, 1947.

[3] Jort F. Gemmeke, Daniel P. W. Ellis, Dylan Freedman, Aren Jansen, Wade Lawrence, R. Channing Moore, Manoj Plakal, and Marvin Ritter. Audio set: An ontology and human-labeled dataset for audio events. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 776–780, 2017.

[4] Shlomo E. Chazan, Hodaya Hammer, Gershon Hazan, Jacob Goldberger, and Sharon Gannot. Multi-microphone speaker separation based on deep doa estimation. In *2019 27th European Signal Processing Conference (EUSIPCO)*, pages 1–5, 2019.

[5] Xiaofei Li, Laurent Girin, Fabien Badeig, and Radu Horaud. Reverberant sound localization with a robot head based on direct-path relative transfer function. In *2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, oct 2016.

[6] Amengual Garamp. Spatial analysis and auralization of room acoustics using a tetrahedral microphone, Apr 2017.

[7] E. O. Brigham and R. E. Morrow. The fast fourier transform. *IEEE Spectrum*, 4(12):63–70, 1967.

[8] Nathanaël Perraudin, Peter Balazs, and Peter L. Søndergaard. A fast griffin-lim algorithm. In *2013 IEEE Workshop on Applications of Signal Processing to Audio and Acoustics*, pages 1–4, 2013.

[9] Carlos Fernández Scola and María Dolores Bolaños Ortega. Direction of arrival estimation : A two microphones approach. In *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2010.

[10] Ruoyu Sun. Optimization for deep learning: theory and algorithms, 2019.

[11] Jiawei Zhang. Gradient descent based optimization algorithms for deep learning models training, 2019.

[12] Shiv Ram Dubey, Satish Kumar Singh, and Bidyut Baran Chaudhuri. Activation functions in deep learning: A comprehensive survey and benchmark, 2022.

[13] Sarit Khirirat, Hamid Reza Feyzmahdavian, and Mikael Johansson. Mini-batch gradient descent: Faster convergence under data sparsity. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 2880–2887, 2017.

[14] Ch Sekhar and P Meghana. A study on backpropagation in artificial neural networks. *Asia-Pacific Journal of Neural Networks and Its Applications*, 4:21–28, 08 2020.

[15] Tong Yu and Hong Zhu. Hyper-parameter optimization: A review of algorithms and applications, 2020.

[16] Zhiyong Hao, Yixuan Jiang, Huihua Yu, and Hsiao-Dong Chiang. Adaptive learning rate and momentum for training deep neural networks, 2021.

[17] Jürgen Schmidhuber. Deep learning in neural networks: An overview. *Neural Networks*, 61:85–117, jan 2015.

[18] Weibo Liu, Zidong Wang, Xiaohui Liu, Nianyin Zeng, Yurong Liu, and Fuad E. Alsaadi. A survey of deep neural network architectures and their applications. *Neurocomputing*, 234:11–26, 2017.

[19] Keiron O'Shea and Ryan Nash. An introduction to convolutional neural networks, 2015.

[20] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, and Illia Polosukhin. Attention is all you need, 2017.

[21] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.

[22] Mariam Yiwere and Eun Joo Rhee. Sound source distance estimation using deep learning: An image classification approach. *Sensors*, 20(1), 2020.

[23] Geoffrey E. Hinton, Nitish Srivastava, Alex Krizhevsky, Ilya Sutskever, and Ruslan R. Salakhutdinov. Improving neural networks by preventing co-adaptation of feature detectors, 2012.

[24] Sharath Adavanne, Archontis Politis, and Tuomas Virtanen. A multi-room reverberant dataset for sound event localization and detection. In *Proceedings of the Detection and Classification of Acoustic Scenes and Events 2019 Workshop (DCASE2019)*, pages 10–14, New York University, NY, USA, October 2019.

[25] Archontis Politis, Sharath Adavanne, and Tuomas Virtanen. A dataset of reverberant spatial sound scenes with moving sources for sound event localization and detection. In *Proceedings of the Detection and Classification of Acoustic Scenes and Events 2020 Workshop (DCASE2020)*, pages 165–169, Tokyo, Japan, November 2020.

[26] Suorong Yang, Weikang Xiao, Mengcheng Zhang, Suhan Guo, Jian Zhao, and Furao Shen. Image data augmentation for deep learning: A survey, 2022.

[27] Marcelo C. Ghilardi, Leandro Dihl, Estevão Testa, Pedro Braga, João P. Pianta, Isabel H. Manssour, and Soraia R. Musse. Automatic dataset augmentation using virtual human simulation, 2019.

[28] Christopher, Antonia Breuer, Silviu Homoceanu, and Henryk Michalewski. Carla real traffic scenarios – novel training ground and benchmark for autonomous driving. 12 2020.

[29] Matthew Rosen, Keith Godin, and Nikunj Raghuvanshi. Interactive sound propagation for dynamic scenes using 2d wave simulation. *Computer Graphics Forum (Symposium on Computer Animation)*, 39(8), September 2020.

[30] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples, 2015.

[31] Rong Huang and Yuancheng Li. Adversarial attack mitigation strategy for machine learning-based network attack detection model in power system. *IEEE Transactions on Smart Grid*, 14(3):2367–2376, 2023.

[32] Xiang Li and Shihao Ji. Generative dynamic patch attack, 2021.