# Secure Multiparty Computation Meets Deep Learning

Yoshi234

2024-01-30

# Table of contents

# Preface

This is a Quarto book. To learn more about Quarto books visit https://quarto.org/docs/books.

## Contents

The quarto book contains an organized structure of notes on a variety of secure multiparty computation protocols, implementation details, and a discussion of v2x applications and relevant deep learning models. The authors hope that any readers find these resources useful.

## Resources

The matcha editor is used to construct some of the mathematical diagrams shown in this book. In order to export a matcha diagram, you need to enter the full-screen mode for the diagram, and click on the "export" drop-down which becomes available. This will allow you to save the math diagram as a png image. We will make liberal use of these throughout the book, especially for explaining complex security primitives such as beaver's triples and homomorphic encryption.

# 1 Red Light Violation Detection

## 1.1 Motivation

Secure Red Light Violation detection is an important application of secure machine learning protocols. Oftentimes, these systems will require the use of image segmentation and object recognition protocols. The images used for this task expose often-times sensitive data about individual users.

In the practical setting of interest, this means exposing license-plate information, associated vehicles, and location information available from the images themselves.

## 1.2 V2I Algorithms for RLR Detection

> The authors of this paper have constructed V2I mechanisms for red light running (RLR) detection, wrong way entry (WWE), and an array of other import tasks in the context of V2X. See the citation Dokur and Katkoori (2022)

### 1.2.1 Red Light Violation Detection Algorithm

The proposed system utilizes the following logic to detect whether a car will violate a red light. A car which is approaching an intersection is connected to road-side units (RSUs) which are installed at traffic lights in an intersection.

Each light is said to be located at points $B(x_2, y_2, z_2)$, $C(x_3, y_3, z_3)$, $D(x_4, y_4, z_4)$ and $E(x_5, y_5, z_5)$ respectively.

Unlike image-based systems, this system assumes V2I communication between the traffic lights and the vehicle in question. This means that the traffic state does not need to be determined by an image classifier. Rather, we already have this information by default.

## 1.3 Thao et.al on Traffic Violation Detection

The paper proposed by L. Thao (2022) introduces a mechanism for detecting red light violations automatically. There paper is titled: *Automatic Traffic Red-Light Violation Detection Using AI*

### 1.3.1 Problem Setting

The reason AI technologies (image classification and detection) systems are better suited than standard sensor technologies is that they are able to operate more consistently, even when the number of vehicles in the setting increases dramatically.

### 1.3.2 System Design and Solution Approach

Separate the task into three parts:

1. vehicle violation detection
2. red signal change monitoring
3. vehicle recognition

**Vehicle Violation Detection**

The YOLOv5s pretrained model (COCO dataset) is used for detecting violating vehicles. After detecting violation, following frames are used to try and determine the license plate (identfy vehicle).

Below, a picture of the overall system flow is presented:

- **vehicle tracking** - performed every 5 frames
  - if IOU (intersection over union) of bounding box is close to one from a previous frame, then the car is assumed to be the same one from that frame.
- **violation line detection**
  - image processing is used to determine traffic lines
  - boundary lines are drawn onto frames captured by the camera later
- **traffic state detection**
  - color filters and image processing used to detect changes in the state of the traffic light

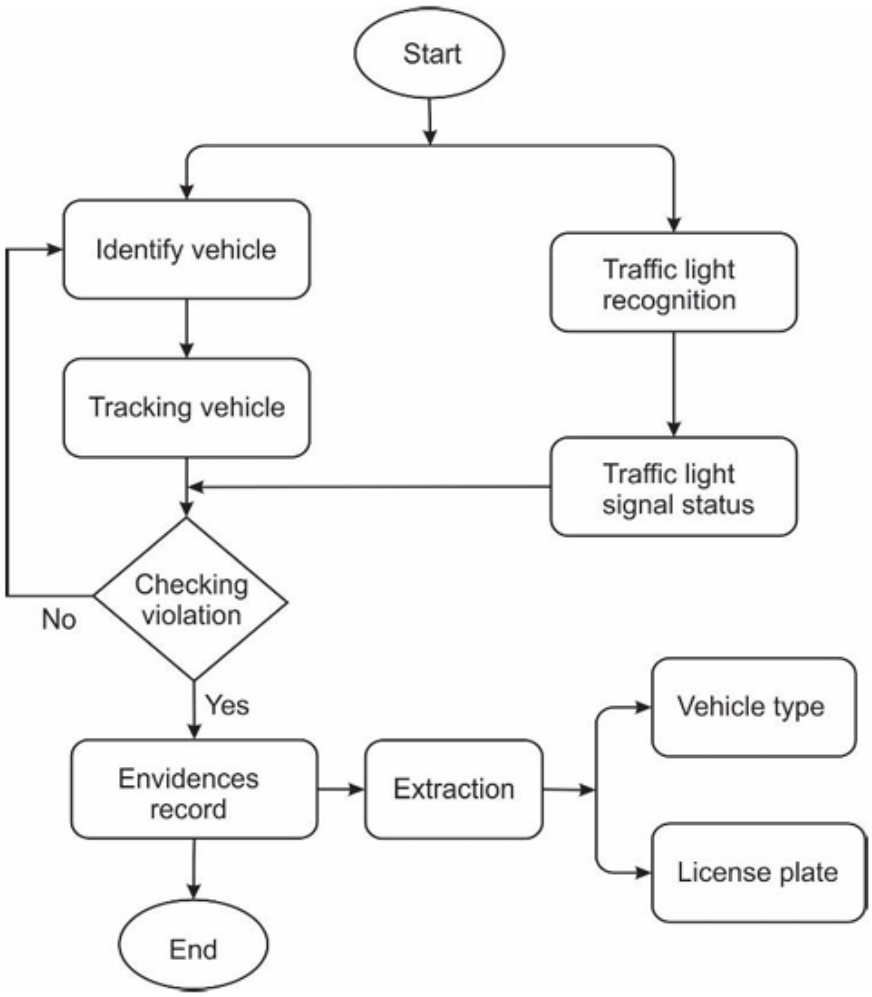


**Figure 2.** Algorithm of violation detection

Figure 1.1: system flow

### 1.3.3 Primary Contributions

1. Implementation of modified *YOLOv5s* model
    1. used parameter changes from original model
    2. achieved following accuracy results:
        1. 82% - vehicle identification
        2. 90% - traffic signal status change
        3. 86% - violation detection
2. Best Performing Architecture given below (v3 / v4)

**Figure 9.** YOLOV5S_v2 remove y3 block

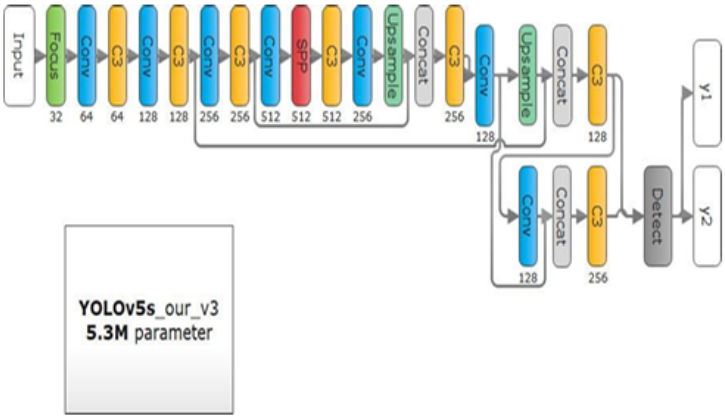


**Figure 10.** YOLOV5S_v3 reduce ½ filter in Conv, remove y3 block

Figure 1.2: modified Yolo architecture

# 2 Traffic Flow Forecasting

## 2.1 Attention Based Spatial-Temporal Graph Convolutional Networks for Traffic Flow Forecasting

In this paper, S. Guo (2019) proposed a method for traffic flow prediction which utilized an **attention based spatial-temporal graph convolutional network**. They aimed to model several time-dependencies: (1) recent, (2) daily-periodic, and (3) weekly-periodic dependencies. The *attention mechanism* captures spatial-temporal patterns in the traffic data and the *spatial-temporal convolution* is used to capture spatial patterns while *standard convolutions* describe temporal features.

### 2.1.1 Core Contributions of ASTGCN

Difficulties of the traffic forecasting problem

1. it is difficult to handle unstable and nonlinear data
2. prediction performance of models require extensive feature engineering
    1. domain expertise is necessary
3. cnn - spatial feature extraction from grid-based data, gcn - describe spatial correlation of grid based data
    1. fails to simultaneously model spatial temporal features and dynamic correlations of traffic data

Addressing these issues:

1. develop a *spatial-temporal attention mechanism*
    1. learns dynamic spatial-temporal correlations of traffic data
    2. temporal attention is applied to capture dynamic temporal correlations for different times
2. Design of *spatial-temporal convolution module*
    1. has graph convolution for modeling graph structure
    2. has convolution in temporal dimension (kind of like 3-d convolution)

# 3 Summary

In summary, this book has no content whatsoever.

# References

Dokur, O., and S. Katkoori. 2022. "Vehicle-to-Infrastructure Based Algorithms for Traffic Light Detection, Red Light Violation, and Wrong-Way Entry Applications." *IEEE International Symposium on Smart Electronic Systems.*

L. Thao, N. Anh, D. Cuong. 2022. "Automatic Traffic Red-Light Violation Detection Using AI." *International Information and Engineering Technology Association.*

S. Guo, N. Feng, Y. Lin. 2019. "Attention Based Spatial-Temporal Graph Convolutional Networks for Traffic Flow Forecasting." *The Thirty-Third AAAI Conference on Artificial Intelligence.*