


Defense Technology of License Plate Recognition System Based on Regularization and Image Denoising

Haitong Shen ^a

*School of Mechanical, Electrical and Information Engineering, Shandong University,
180 Wenhua West Road, Weihai City, Shandong Province, China*

Keywords: License Plate Recognition, Regularization, Image Denoising, PGD Attack.


Abstract: The license plate recognition (LPR) system plays an important role in modern traffic, but the existing models based on deep learning are difficult to deal with in a series of complex situations, including adversarial example attacks. Based on this, this project deeply studies the defense technology of the LPR system utilizing image processing techniques, aiming to enhance the LPR system's processing ability in the face of complex environments, especially adversarial sample attacks. In terms of research methods, this project is based on a GRU-based sequence model, using regularization and image noise reduction to weaken the sensitivity of the model to specific perturbed data points and enhance the robustness of the model, so that the accuracy of the model to identify adversarial samples is improved from 22% to 68%. The experimental results show that the regularization and image noise reduction method can make the LPR model effectively distinguish the original license plate from the adversarial samples, and can restore the original information in the image adversarial samples. There are still some problems in the model, such as partial errors that may occur when trying to restore the authentic data encoded on the license plate, especially the abbreviation of the province. Further improvement of the character recognition method can be considered in the future.

1 INTRODUCTION

Traditional license plate detection algorithms usually rely on specific features such as color, texture, and shape of the license plate, for example, color feature-based license plate detection algorithms and texture feature-based license plate detection algorithms, their mobility and detection results are poor (Dun, Zhang, Ye, et al., 2015; Kim, Kim, Kim, 1996; Zhang, Jia, He, et al., 2006; Yu, Li, Zhang, et al., 2015).

License plate recognition (LPR) models based on deep learning are an important part of modern transportation systems, which can be utilizable in a multitude of contexts such as illegal capturing, parking lot management, and vehicle trajectory tracking. They have many advantages such as fast recognition speed, high accuracy, and portability. Therefore, it is of great significance to study feasible defense technology of LPR systems and enhance the recognition accuracy of license plate systems in extreme cases to improve the safety of daily travel and traffic conditions.

The deep learning model used in the system makes it difficult to deal with different types of license plates and is vulnerable to adversarial examples. The existing attack methods can interfere with the LPR model by adding carefully designed small adversarial perturbations to the normal samples, and the wrong output will pose a great threat to privacy security and travel safety in the real world. Research by Padmasiri et al. shows that most existing LPR solutions require a large amount of computation and waiting time, and are difficult to cope with the work in complex scenarios such as night (Padmasiri, Shashirangana, Meedeniya, et al., 2022). Deshpande et al. proposed a small object detection algorithm trained using real-time high-resolution data that can detect downsized, slanted, blurred license plate images (Deshpande, Veena, Ferede, 2022). Gao used A local tiled convolutional neural network (LTCNN), and by changing the method of adjusting the weights, the model was able to recognize the make and model of the vehicle with 98% accuracy (Gao, Lee, 2016). However, existing models will find it difficult to

^a <https://orcid.org/0009-0001-8321-6215>

maintain the original high accuracy and confidence when dealing with adversarial samples.

Based on the above investigation and research, this project will develop a set of feasible defense techniques against license plate attacks, using regularization technology to enhance the robustness of the model, and using image denoising technology to weaken the adversarial image. This defense method can enhance the recognition accuracy of the model in extreme cases, and enable the model to detect adversarial samples and restore the original license plate information in the image, to improve the defense performance of the LPR system.

2 RESEARCH METHODS

2.1 Dataset Selection

The data set in this paper is from the open-source Chinese urban license plate dataset CCPD2019. The CCPD2019 dataset was collected by the University of Science and Technology of China. It contains more than 250,000 Chinese urban license plate images, and the recognition results and detection information of the license plate images are annotated in detail to facilitate subsequent training. The license plate photos contained in the dataset involve a variety of complex environments. Different sub-datasets include images affected by different environments, such as rain and snow, fog, tilt, jitter, and blur. This study uses the proportional probability sampling method of different sub-datasets. Considering that the license plate pictures taken in most cases are not affected by extreme weather, this study mainly uses the sub-dataset CCPD-Base under CCPD2019, which contains common license plate pictures under regular conditions.

2.2 LPR Model

HyperLRP is selected as the LPR model in this paper. HyperLRP is a lightweight Chinese LPR model utilizing deep learning techniques, developed by Beijing Zhiyun View Technology Co., LTD. It has the advantages of fast recognition speed and high accuracy and can support the recognition and detection of a variety of license plates. At the same time, HyperLRP is vulnerable to adversarial sample attacks, and it cannot effectively defend against existing attack algorithms. The model uses a sequence model based on Gate Recurrent Unit (GRU) to detect the text in the license plate, which is modified based on the Optical Character Recognition

(OCR) model. The recognition speed is slow, about 20ms, but the recognition effect is good. The final average recognition time of the model is less than 100ms, and the accuracy rate is about 95%-97%.

2.3 Attack Methods

In this paper, the Projected Gradient Descent (PGD) algorithm is used to create adversarial instances to simulate the process of the attacker adding disturbances to the license plate. When running the model, existing license plate image adversarial samples can also be directly input into the model to skip the step of adding disturbances. The PGD algorithm generates adversarial examples by iterating several times along the gradient direction. Compared with other attack methods, the PGD algorithm can constrain the attack into the framework to reduce the disturbance, with the advantages of a good attack effect and less added disturbance. Therefore, the selection of a PGD attack will better reflect the effect of the defense strategy used in this paper.

2.4 Data Preprocessing

Firstly, a cascade classifier based on the Haar feature serves the purpose of identifying all instances of license plates in the image, and then the license plate image is cropped and normalized to ensure that the input image of the model has a uniform size, which is convenient for subsequent recognition and attack.

2.5 Regularization

In this paper, L2 regularization is used to enhance the robustness of the model by incorporating a penalization factor into its loss computation to limit the weight value of the model. On the one hand, it reduces the fitting degree of the model to the training samples, which makes the model more difficult to attack. On the other hand, it reduces the sensitivity of the model to small perturbations. Adversarial examples will make it difficult to attack the image recognition model by adding small perturbations to the original image. The attacker has to increase the degree of perturbation so that the naked eye can recognize the adversarial sample, to achieve the purpose of defense.

2.6 Image Denoising

Use a median filter for noise reduction. By sorting each pixel in an image and its neighborhood and replacing the value of that pixel with the median

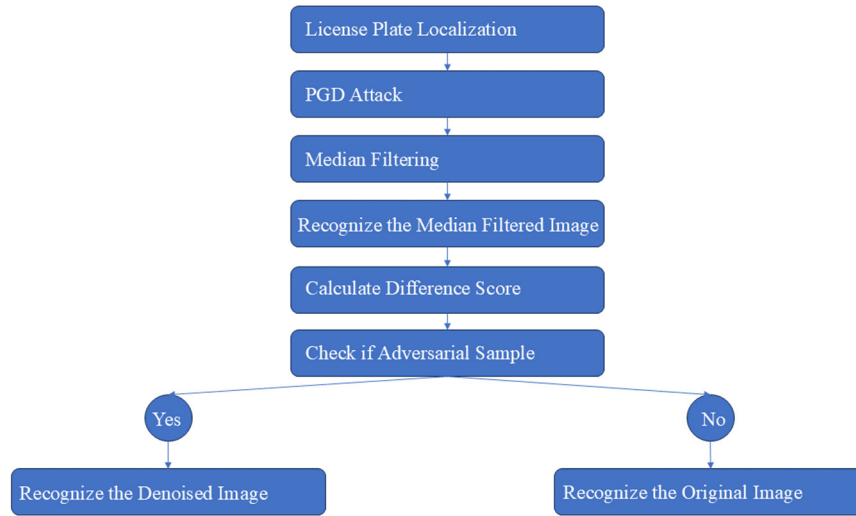


Figure 1: The flow of image recognition algorithm after adding defense (Photo/Picture credit: Original).

value, the median filter can mask out small changes to some pixels in the image. Compared with noise reduction methods such as mean filtering and Gaussian filtering, median filtering is more resistant to noise, which can significantly reduce the influence of adversarial samples on the model, and at the same time better retain the edges and some details of the image, reducing the difficulty of subsequent recognition of the original image and the restored adversarial samples.

3 ALGORITHM DESIGN

The CCPD2019 dataset was used to train the model. The model's loss function is augmented with L2 regularization to penalize large weights, thereby simplifying the model and mitigating the risk of overfitting. The parameters of the model as well as the regularization coefficient λ are updated by gradient descent. Finally, the model parameters are saved.

As shown in Figure 1, firstly, rough positioning is performed after reading the license plate image to find out all the license plates in the image. Then fine positioning is carried out, the license plate is cropped along the contour and normalized to divide the license plate into individual characters, which is convenient for character recognition later.

If the license plate image is the original image, to simulate the adversarial sample attack, a PGD attack should be performed on the cropped license plate, and

then the perturbed image should be pasted to the corresponding position of the original image and the above steps of license plate location should be repeated to obtain the cropped license plate image.

If the input image is an adversarial sample, the step of adding disturbance here can be skipped.

Then, the median value of each point in the 3*3 neighborhood matrix of each sorted point is taken as the actual pixel value of the point, to ignore the small changes in some pixels in the image and enhance the robustness of the model.

The adversarial samples before and after the median filtering are sent to the LPR model respectively, and the output tensor of the model is obtained, where the element is the probability matrix output by the license plate for each character. According to this, whether the image has been subjected to adversarial attacks is determined.

The Euclidean distance between the model and the probability matrix of each character in the license plate before and after the median filtering is calculated, and it is added as the difference degree of the two tensors. For each character in the license plate, if the recognition results of the model are inconsistent before and after the median filtering, an additional weight μ is added to the above dissimilarity.

In Formula (1), D is the degree of difference between probability matrices, that is, the possibility of the image being attacked. $E(x, y)$ returns the Euclidean distance between two matrices x and y . $p1$ is the model's outputted probability matrix for the

original image, $p2$ is the model's outputted probability matrix for the image after median filtering, and the elements in $p1$ and $p2$ are the model's outputted probability matrix for the characters in the license plate (for example, $p1[0]$ is the probability matrix output by the model when recognizing the abbreviation of the province). μ is the contribution of error recognition to matrix dissimilarity, which is set to 0.5 in this paper. $e(x, y)$ determines whether two arguments are equal and returns 0 if they are identical or 1 if they are different. $a(x)$ returns the maximum value of the matrix x , and $a(p[n])$ is the recognition result of a character.

$$D = \sum E(p1[n], p2[n]) + \mu \sum e(a(p1[n]), a(p2[n])) \quad (1)$$

Finally, according to the size of the threshold and the above difference value, whether the image is an adversarial sample was determined. If it is, the output of the model for the median filtered image will be used as the final recognition result. If not, the output of the model for the original image is used as the final recognition result.

4 EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Experimental Results

As shown in Table 1, after adding defense, the accuracy of the model in recognizing the original image is improved, from 77% to 82%, and the accuracy of recognizing the adversarial sample is greatly improved, from 22% to 68%. In addition, the accuracy of the model to determine whether the image is under attack is 73%, and the recall rate is 69%.

Table 1. Performance Improvement comparison

Metrics	Before adding defenses	After adding defenses
Original image accuracy (%)	77	82
Adversarial sample accuracy (%)	22	68
Model judgment attack accuracy (%)	-	73
Model-judged attack recall (%)	-	69

4.2 Experimental Analysis

According to the experimental results, the accuracy of identifying adversarial samples is greatly improved after adding defense, because the regularization reduces the sensitivity of the model to the change of pixels in the image, and the median filtering weakens the adversarial messages in the image. Therefore, for those adversarial samples that try to complete the attack with small disturbances, the model will be able to restore the license plate's original information. The recognition rate of the original image is slightly improved because the regularization improves the robustness of the model.

There are still some problems in the model, it is difficult for the model to restore some information in the license plate, especially the abbreviation of the province and some similar letters. Moussaoui et al. showed that light intensity and excessive noise can affect character extraction algorithms, making it difficult to accurately identify characters (Moussaoui, Akkad, Benslimane, et al., 2024).

For some images that are difficult to recognize, especially those affected by the environment, the model may classify them as adversarial samples; Similarly, for some adversarial examples with poor attack effects, the model may think that they have not been attacked. This may lead to improvements from the following facts.

According to the study of Liu et al., for some extreme license plate images, such as the deformation of the license plate caused by lateral photography, the image should be corrected before segmentation, such as the polynomial distortion method and interpolation method (Liu, Liu, 2000).

Su's research shows that YOLO-based license plate detection methods have higher accuracy than HyperLPR and perform better when faced with adversarial samples (Su, 2021).

In addition, the model used in this paper is based on a single image, while the LPR scene in practical applications is often based on video. In the future, video-like datasets can be considered, such as the video-based license plate dataset LSV-LP constructed by wang et al. (Wang, Lu, Zhang, et al., 2023).

The main province of license plate in the CCPD2019 dataset is "Anhui", resulting in the limited transfer capability of the model and the difficulty in defending against some adversarial samples with strong adversarial resistance.

5 CONCLUSION

In this paper, a sequence model based on GRU is used to recognize adversarial license plate samples. By adding regularization and using image noise reduction technology, the recognition accuracy is improved from 22% to 68%.

The study shows the feasibility of regularization and image noise reduction in the field of LPR, but some errors may occur when trying to restore the license plate's original information, especially the abbreviation of the province or municipality. A possible explanation for this can be obtained from the following facts.

Firstly, the robustness of the model can be improved by using the L2 penalty term in the loss function to limit the range of the parameters and make them smoother. Gradient regularization on input pictures that may be adversarial examples can reduce the sensitivity of the model to some small perturbations. Image denoising can weaken the perturbation information in the image adversarial examples, and preserve the original information in the image while removing the noise. Secondly, the adversarial sample may add weak perturbations at multiple places on the license plate instead of adding strong perturbations at a small number of pixels, which cannot be effectively processed by the model.

In the future, it may be considered to correct extreme images before cropping images, adopt more effective license plate detection methods, and use videos as the data set for model training to facilitate the in-depth study of this issue.

REFERENCES

- Deshpande, M., Veena, M.B. and Ferde, A.W., 2022. Auditory Speech Based Alerting System for Detecting Dummy Number Plate via Video Processing Data sets. *Computational Intelligence and Neuroscience*, 2022, 4423744.
- Dun, J., Zhang, S.Y., Ye, X. and Zhang, Y., 2015. Chinese License Plate Localization in Multi-Lane with Complex Background Based on Concomitant Colors. *IEEE Intelligent Transportation Systems Magazine*, 7, pp. 51-61.
- Gao, Y. and Lee, H.J., 2016. Local Tiled Deep Networks for Recognition of Vehicle Make and Model. *Sensors*, 16(2), pp. 226.
- Kim, S., Kim, D.W. and Kim, H., 1996. A recognition of vehicle license plate using a genetic algorithm based segmentation. *Proceedings of the 3rd IEEE International Conference on Image Processing*, 2, pp. 661-664.
- Liu, Z.Y. and Liu, Y.J., 2000. Image extraction and segmentation in license plate recognition (LPR). *Journal of Chinese Information Technology*, 14(4), pp. 29-34.
- Moussaoui, H., Akkad, N.E., Benslimane, M., El-Shafai, W., Baihan, A., Hewage, C. and Rathore, R.S., 2024. Enhancing automated vehicle identification by integrating YOLO v8 and OCR techniques for high-precision license plate detection and recognition. *Scientific Reports*, 14(1), 14389.
- Padmasiri, H., Shashirangana, J., Meedeniya, D., Rana, O. and Perera, C., 2022. Automated License Plate Recognition for Resource-Constrained Environments. *Sensors*, 22(4), pp. 1434.
- Su, Y., 2021. Research and implementation of neural network attack and defense technology for license plate recognition. (Doctoral dissertation, Guangzhou University).
- Wang, Q., Lu, X., Zhang, C., Yuan, Y. and Li, X., 2023. LSV-LP: Large-Scale Video-Based License Plate Detection and Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(1), pp. 752-767.
- Yu, S., Li, B., Zhang, Q., Liu, C. and Meng, M.Q., 2015. A novel license plate location method based on wavelet transform and EMD analysis. *Pattern Recognition*, 48, pp. 114-125.
- Zhang, H., Jia, W., He, X. and Wu, Q., 2006. Learning-Based License Plate Detection Using Global and Local Features. *18th International Conference on Pattern Recognition (ICPR'06)*, 2, pp. 1102-1105.