2019 3rd International Conference on Computer Engineering, Information Science and Internet Technology (CII 2019)

Study of CNN Methods in Signature Verification

Zihan Zeng

Institution of Information Technology, Beijing Normal University, Zhuhai, China

Keywords: Artificial Intelligence, Deep Learning, Computer Vision, Signature.

Abstract: Handwriting identification is an excellent way to identify identities, so people have always used handwritten signatures as their unique features. But with the diversification of counterfeiting methods, people are beginning to need more advanced methods and techniques to verify signatures. This paper proposes a new feature extraction method, combined with a convolutional neural network, to improve the accuracy of signature verification to nearly 80% under the condition of minimizing the amount of computation. This research laid the foundation for further improvement of accuracy and provided a theoretical basis for the establishment of a complete signature verification system.

1. Introduction

Signature as an essential personal feature is widely used in our lives for authentication, such as when signing contracts and issuing checks. In the past, the verification of handwriting was based solely on surface image information, relying on relevant experts in the field of handwriting for manual comparison and identification. However, with the increasing use of signatures, the technology of counterfeiting signatures is continuously improving. The most common reason for falsifying signatures is to swindle money, and such cases have been happening. In 2010, a man in the United States forged a signature of a federal judge to resolve his bill dispute.[1] Also, a British man was recently tried because he forged his partner's signature to withdraw money from his bank account.[2] The technique of falsifying signatures is not only used to defraud property. In October 2019, the Indian Prime Minister's Office claimed that a man had forged the signature of the Prime Minister, but his intention was unknown.[3] Thus, it is extremely urgent to find a valid signature verification method.

Handwriting recognition technology also faces many challenges. In the case of surface images, forged signatures may be merely the same as actual signatures. The internal features of each person's signature are microscopic and difficult to extract. These problems have led to the fact that the accuracy of machine authentication signatures has not been able to rise.

In this article, we propose a new feature extraction method and make improvements on this basis. About these feature extractors, we aim to choose as few features as possible to reduce complexity and achieve better results. Recently, neural networks have developed to the point where they cannot be ignored. Neural networks, especially convolutional neural networks, have significant advantages in characterizing learning. Therefore, we combine the feature extractor with the convolutional neural network, which dramatically improves the accuracy of the machine's recognition in signature verification.

2. Methods

2.1 PSF Features

Path Signature Features (PSF) is first widely used in Handwritten Recognition field which have been demonstrated to improve recognition accuracy dramatically. The PSF features encodes spatial features of digital strokes into a 3D tensor. Each channel of this encoded 3D tensor represents some geometrical property and the order of stroke points information, as shown in Figure 1.

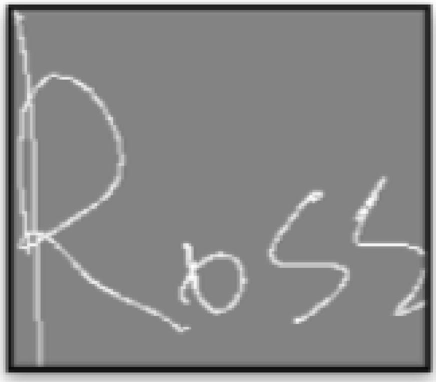


Figure 1. Old PSF Data Example

2.2 Improved PSF Features

In fact, the coordinate features of the points in the stroke are still only the spatial features that characterize the signature. Therefore, we have extended and improved the methods mentioned in the previous section. We considered the time stamp for each point and processed temporal feature.

We believe that the most crucial feature of the time stamp is the time interval between points. Therefore, we set the value of the time stamp of the first point to 0, and the feature value of the following point is set to the time difference from the previous point. In addition, in order to enable the convolutional neural network to extract better and identify features, we have used different algorithms to amplify this feature related to time. As shown in Figure 2, the image processed by this method is very different from the previous one.

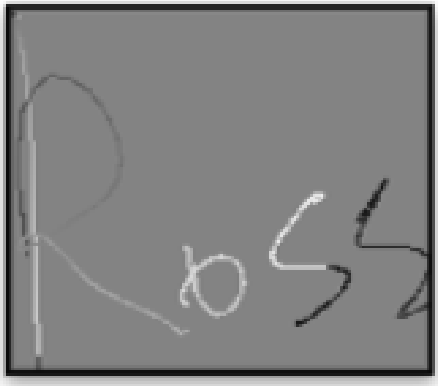


Figure 2. Improved PSF Data Example

We believe this approach can significantly improve the accuracy of recognition and prepare for subsequent work to optimize the structural characteristics of neural networks.

2.3 Neural Network Layer

In order to observe the effect of feature extractor combined with convolutional neural networks in the most efficient way, we chose LeNet, one of the most classical convolutional neural network structures, as the neural network module we used. We believe that if the underlying network structure of LeNet is combined with the feature extractor, the recognition rate can be significantly improved. In later research, a more complex convolutional neural network structure can achieve better results. The trained model can even be used directly.

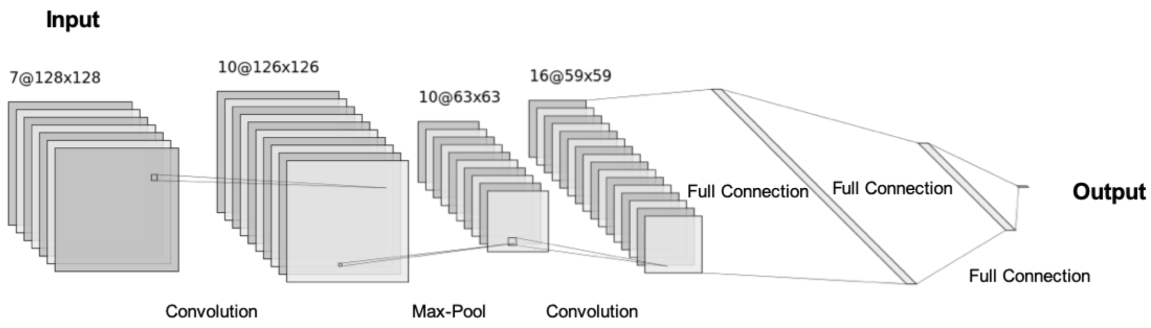


Figure 3. Neural Network Structure

We all know that LeNet's middle layer is divided into two convolutional layers, one pooled layer, and three fully connected layers.[5] After the feature extractor, all of our data is 128x128x7 in size and 128 in length and width. Figure 3 shows the change in size of the data in the neural network module.

3. Experiments

3.1 Dataset

Our experiments are based on a common dataset named SVC2004. Originally, SVC2004 is used in the first international signature verification competition, and it provides a unified standard to determine the effectiveness of a system. With the development of machine learning, we reckon that SVC2004 can be used as a training set and testing set in our experiment regarding neural network. [4]

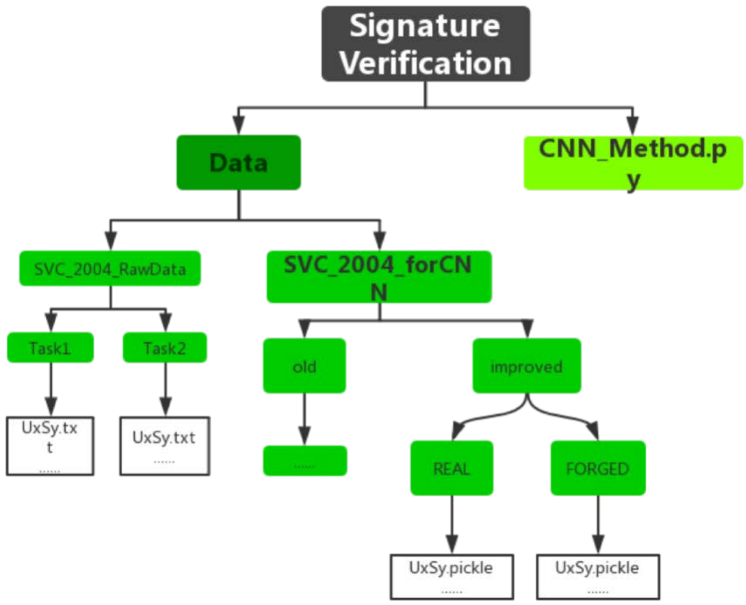


Figure 4. Project Structure

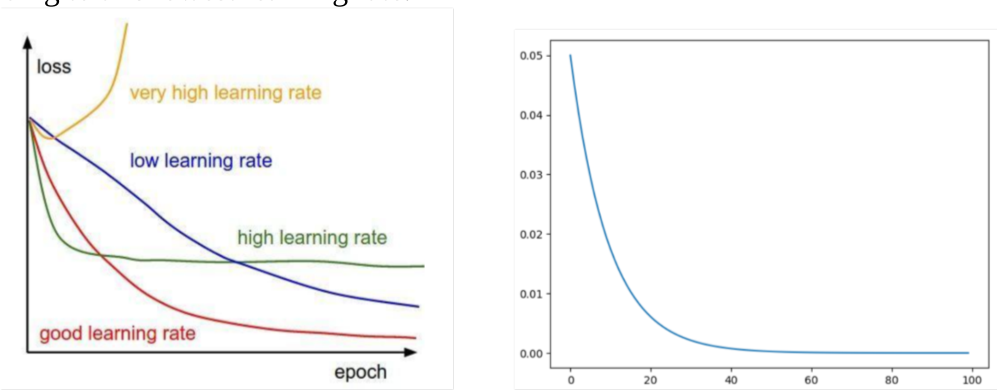
Generally speaking, a signature can be separated into various numbers of strokes, and every stroke can be divided into a series of points. Therefore, the representation of the dataset is also related to this. Each file contains many points with different features. These features are x-coordinate, y-coordinate, time stamp, button status, azimuth, altitude, and pressure. At least 4 features show in each text file.

The naming convention of the files is UxSy, x is the user ID, and y is the signature ID. Real signatures correspond to y values from 1 to 20 and forgeries from 21 to 40. At least 4 people involved the contribution of those forged signatures.[4] There are 80 users in SVC2004 dataset and evenly distributed to Task 1 and Task 2. That's basically the raw dataset.

Hence, we have two solutions to deal with raw data, and we created two new folders to store processed data. We divided each dataset into a training set and testing set randomly, and the testing set accounts for 20% of the total data and does not cross with the training set. Besides, we manually divide the dataset into real and forged signatures according to signature ID, which facilitates neural network classification and testing. Figure 4 has shown the structure of our project structure.

3.2 Settings

The setting of learning rate is critical during the training process. First and foremost, we used the method in the paper Cyclical Learning Rates for Training Neural Networks to find the best initial learning rate. This method is originally to estimate the minimum and maximum learning rate allowed by the network.[6] We did a little change regarding it. The core of this method is to set a small initial learning rate, then increase the learning rate after each batch, and finally find the lowest point of loss by observing the change of loss with the learning rate. Then the best initial learning rate is the value corresponding to this lowest learning rate.



(A) Learning Rate Situation (B) Learning Rate Exponentially Decline

Figure 5. About Learning Rate

After we get the best initial learning rate, we chose to let the learning rate decay exponentially per training epoch because the curve of the exponential decline fits the curve of the loss, as shown in Figure 5.[7] This way tends to get a perfect curve about loss.

To prevent overfitting, firstly, we set a large number of epoch and then set the algorithm to stop the training once the average loss value for this round is less than 0.05.

4. Result

4.1 CNN and Old PSF

It can be seen from Figure 6 that as the number of training iterations increases, the value of loss oscillates aggressively than the initial ones and gradually converges to around 0.692. The decrease in the loss value is minimal and does not change much. Therefore, the combination of CNN and the first PSF feature extractor maybe not a comparable choice for signature verification.

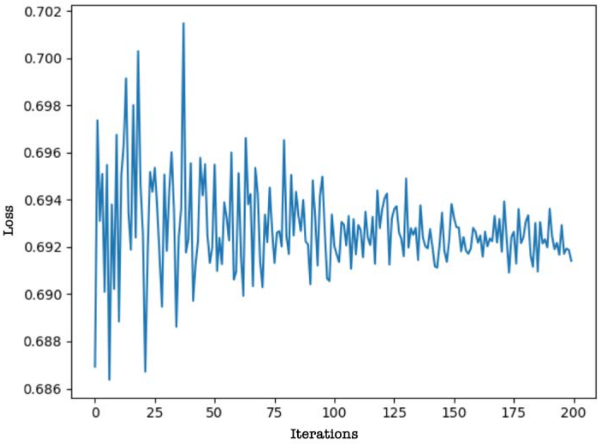


Figure 6. The Loss Image of the First Test

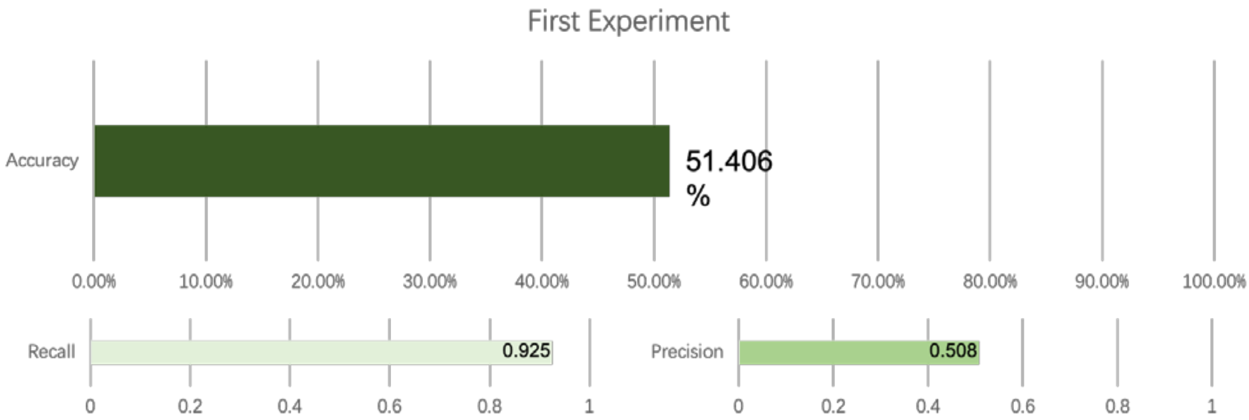


Figure 7. Results of the first experiment

As shown in Figure 7, this experiment shows that the recognition accuracy is only 51.406%, and only 329 of the 640-test data are correct. By analyzing the recall rate and accuracy rate in this experimental result, we found that the algorithm almost found all the positive examples. Since the genuine signature data and the fake signature data are half and half in the test set, it can be analyzed that the machine almost judges all the data to be true. Based on the above, it can be concluded that CNN does not have a good effect on the extraction and learning of the features of the data generated by the first feature extractor, so the algorithm of the first feature extractor needs to be improved.

4.2 CNN and New PSF

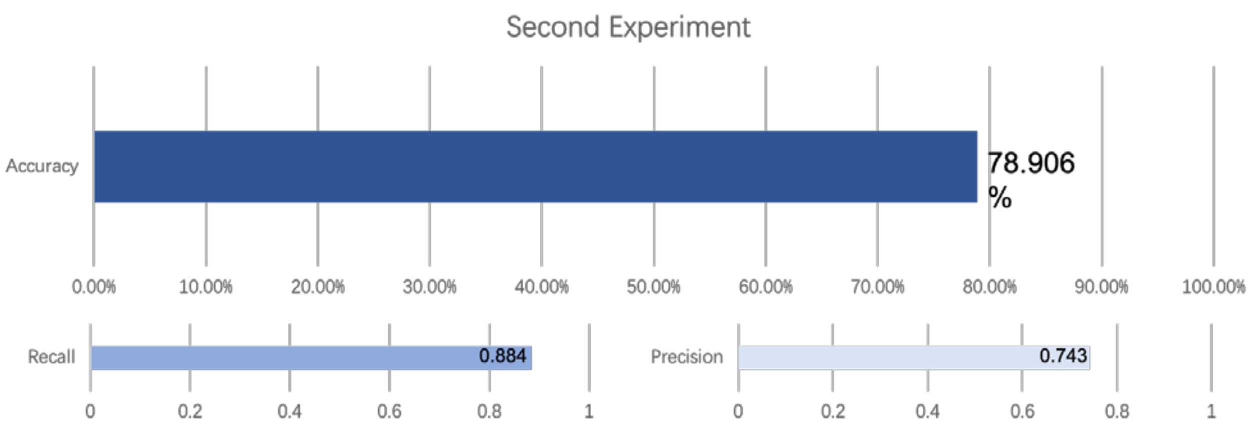


Figure 8. Results of the second experiment

After the data features are amplified, the complexity of the data increases, and the training time and the time of loss convergence also increase. The accuracy of this experiment was 78.906% as well as 505 data in the test set were accurate. Figure 8 shows the accuracy, precision, and recall of this experiment.

4.3 Comparison

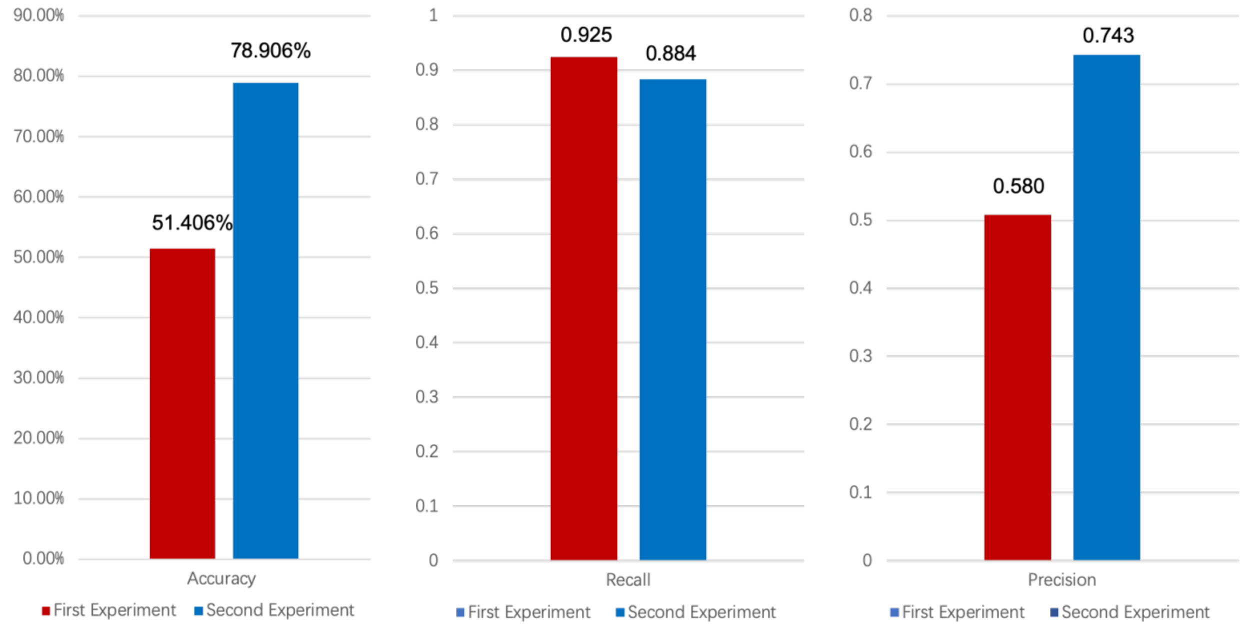


Figure 9. Results Comparison

Comparing the data of the two experiments, we can find that the results of the second experiment are more reasonable than before, and the machine no longer blindly judges the data for the first time. After calculating the F-measure indicator, it was found that the second value was increased by about 30% from the first value. Prove that the second experiment is more effective.

Overall, after the algorithm optimization, the accuracy of the second experiment increased by 27.5%, which proved the necessity and effectiveness of algorithm optimization.

5. Conclusion and Discussion

Handwriting is an essential biological feature is more straightforward to judge in many cases than other features, such as iris, DNA, etc. Signatures as necessary identification identifiers should be protected.

This article shows the application of CNN in signature verification. We show the process of our experiments and the process of continuous improvement and optimization. We not only optimized the feature extraction algorithm but also combined with the convolutional neural network.

We believe that our research has laid a solid foundation for the establishment of a comprehensive real-time signature verification system. Based on our existing research, we still have many prospects.

Although the accuracy rate of 78.906% has improved compared with the previous one, there is still much space for further improvement. In future research, we believe that there are still many ways to explore. Although our goal is to base on as few features as possible to achieve the highest possible accuracy, however, in later studies, in order to obtain higher accuracy, we may consider more features, or continue to perform processing on existing features.

Our experiments have proven that the underlying CNN can play a role in signature verification. So, a more complex and better convolutional neural network combination will certainly be able to verify signatures more accurately.

We believe that, based on our research, a sophisticated real-time signature verification system will be implemented in the near future and used in daily human life.

References

[1] Jake Burns. Man accused of tricking teens also posed as federal agent, forged judge's signature, court docs reveal [EB/OL]. https://wtvr.com/2019/09/25/joshua-c-brady-accused-bribing-teenage-girls-to-file-false-police-reports/. September 25, 2019.

[2] Mercury reporter. Forged signature gained Hakin man £13, 000 [EB/OL]. https:// www. Milford mercury.co.uk/news/17964485.forged-signature-gained-hakin-man-13-000/. October 12, 20 19.

[3] HT Correspondent. Bengaluru-based man booked for 'forging' PM Office letters [EB/OL]. https://www.hindustantimes.com/india-news/bengaluru-based-man-booked-for-forging-pm-office-letters/story-122gZN6rRkDL3POIgSrhVO.html, October 16, 2019.

[4] Yeung D Y, Chang H, Xiong Y M, et al.SVC2004: first international signature verification competition[C]. Proc. of the1st International Conference on Biometric Authentication, 2004:16-22.

[5] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE,1998,86(11):2278-2324.

[6] Smith L N. Cyclical Learning Rates for Training Neural Networks[C]. 2017 IEEE Winter Conference on Applications of Computer Vision (WACV). IEEE, 2017.

[7] CH-Tseng. Kaggle-Digit Recognizer Competition [EB/OL]. https:// chtseng. wordpress. com/ 2017/12/24/kaggle-digit-recognizer-competition/. December 24, 2017.