Neural network verification investigation on image manipulating research

Jinliu Peng
Australian National University, Canberra, Australia
u6996728@anu.edu.au

Abstract. In order to study in CaldWell's paper on eye tracking, whether the interviewees judge whether the pictures have been manipulated with through their own recognition, this paper uses a single hidden layer neural network to verify a case.(This paper uses for assignment.)

Keywords: verification, accuracy

1 Introduction

This article selects 5 pictures from the CaldWell study and data from interviewees for verification. The results show that within the framework of a neural network under a single hidden layer, it is able for interviewees to effectively determine that experiment participants are looking at a manipulated or unmanipulated image based on how the participants use their eyegaze to look at the image and experiment participants will vote (another output set, verbally saying whether the image is manipulated or unmanipulated) based on how the participant uses their eyegaze to look at the image.

1.1 Data Inspection

This paper use the first version of dataset. There 372 observations in the dataset and there are 4 inputs(features). I shuffled the dataset and took 80% as the training data and 20% as the testing data.

1.2 Method

I build a neural network with one hidden layer to calculate the possibilities that the experiment participants accuracy of identifying whether the images are manipulated. If the accuracy is higher than 70%, I will consider the participants are capable of identifying images. If the accuracy is lower than 70% but higher than 50%, I will consider the participants have equivocal senses to identify images. If the accuracy is

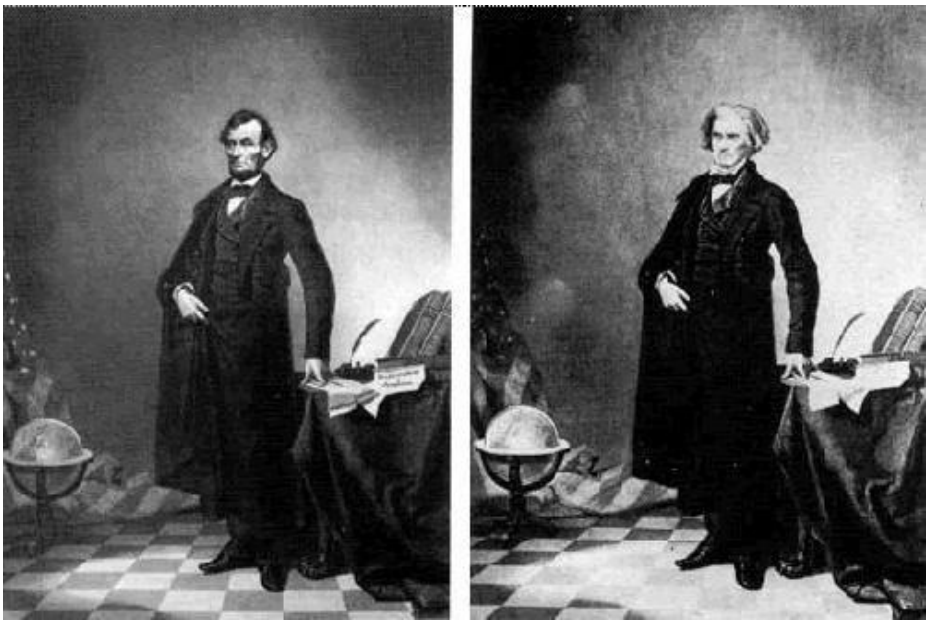
lower than 50%, then I will consider the participants are unable to identify manipulated images and were fooled by image manipulation techniques.

2 Discussion of recent research

When it comes to image tampering, the paper <Learning Rich Features for Image Manipulation Detection> published on CVPR2018 is inseparable. This article introduced some common image manipulating methods and techniques for detecting manipulating and also guides the direction of image detection.

The first false image in history appeared in 1860. The picture of Lincoln on the left in Figure 1 was actually obtained by replacing Senator John Calhoun's head on the right with Lincoln's head.

Figure 1.



The propaganda pictures used in the 2004 election of Bush Jr. were actually obtained by transplanting Bush's photos onto other photos. The false images interfered with the decision-making of the people during the election and also had a considerable impact on the results of the election.

Figure 2.

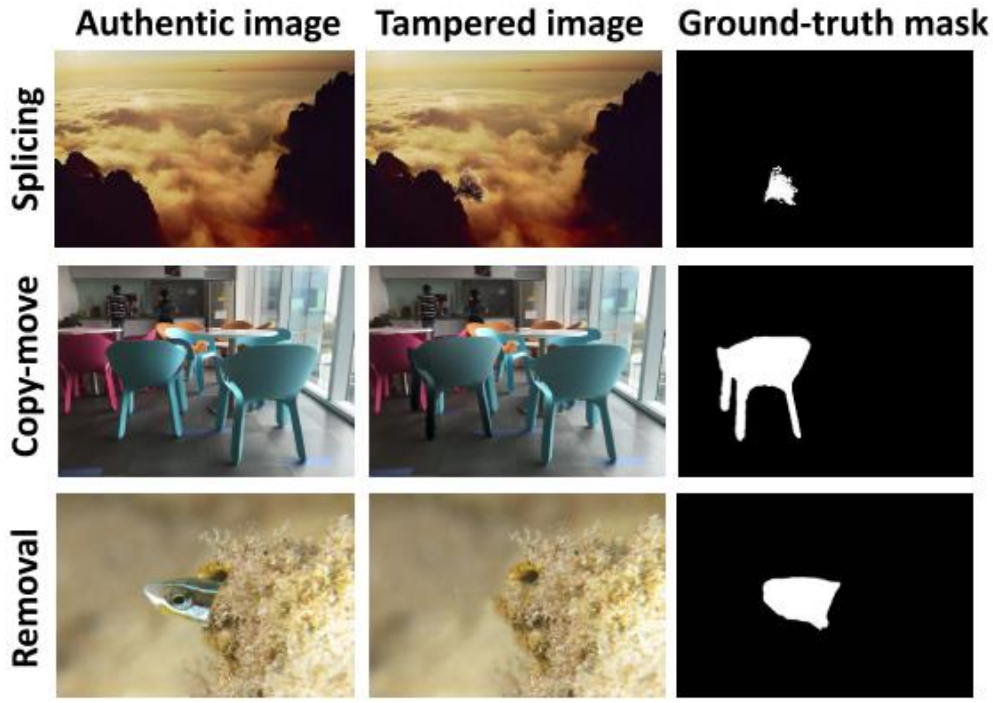
The examples listed above reflect the research background and significance of image traceability and forensics from the side. With the frequent occurrence of various digital image fraud incidents, people have serious doubts about the authenticity of digital images. Such behavior may not only have a huge impact on personal reputation and interests, but also indirectly have a negative impact on social stability and unity, and may even have a huge impact on national security. Therefore, some important digital image application fields.

For example, national security agencies, government agencies, and commercial agencies should strengthen the detection of image authenticity to ensure the authenticity and originality of digital images.

According to the CaldWell [2015] survey, we learned that the effect of eye tracking to determine whether an image is tampered with is poor. In recent years, with the continuous development of deep learning technology, especially the excellent performance of Convolutional Neural Network (CNN) represented by AlexNet in feature extraction, coupled with its excellent performance in image classification, semantic segmentation, and object recognition and other computer vision tasks have achieved considerable results. Some researchers have tried to use deep learning technology to solve the problem of tampering detection of digital images.

The tamper detection technology based on convolutional neural network uses the multi-layer structure of the deep learning network and powerful feature learning capabilities to achieve tamper detection that does not depend on the single attribute of the image, which makes up for the lack of applicability of traditional image tamper detection technology based on feature extraction Shortcomings. The tamper detection technology based on convolutional neural network can not only locate the tampered area, but also give the corresponding type of tampering. In the existing experiments on public data sets used for digital image forensics, the tampering detection based on convolutional neural network The algorithm effect is better than the traditional image tampering detection algorithm, and shows better robustness.

Figure 3.



3 Discussion of my research

The core of this article is the two-classification problem of neural networks. Through 4 input features, the experiment participant is looking at a manipulated or unmanipulated image based on how the participant uses their eye-gaze to look at the image.

After processing the eye-gaze data set, I obtained the accuracy of question 1 and question 2.

In my neural network, I use SGD as the optimizer, learning rate as 0.01, epoch = 5000, hidden neurons are 5(inputs feature plus 1).

And the accuracy of answering whether the image the participant views is the manipulated or unmanipulated is between 65.44% and 66.78%. The accuracy of answering the verbal opinion of the participant as to whether the image is manipulated or unmanipulated is between 68.3% and 69.1%. These two accuracy is very closed to 70% however, they are still not high enough to say that participants are capable of identifying manipulated and unmanipulated images.

4 Conclusion

In the Eye-gaze dataset, I build a neural network with one hidden layer to verify CaldWell's results. The accuracy of two questions are about 65.8% and 68.6% respectively. The accuracy are not convincing evidences to prove these participants are qualified to identify image manipulation by human eyes. But it is undeniable that the accuracy rate of more than 50% which means participants do have some senses or knowledge or technique to distinguish the tiny difference in different images.

5 References

1. Zhou, P. , et al. "Learning Rich Features for Image Manipulation Detection." , in 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2018).
2. Kaur A, Mustafa A, Mehta L, et al. Prediction and localization of student engagement in the wild[C]//2018 Digital Image Computing: Techniques and Applications (DICTA). IEEE, 2018: P1-8.
3. Ghosh S, Dhall A, Sebe N, et al. Predicting group cohesiveness in images[C]//2019 International Joint Conference on Neural Networks (IJCNN). IEEE, 2019: P1-8.
4. Dhall A, Joshi J, Sikka K, et al. The more the merrier: Analysing the affect of a group of people in images[C]//2015 11th IEEE international conference and workshops on automatic face and gesture recognition (FG). IEEE, 2015, P1-8.