Dangerous goods identification algorithm based on Generative Adversarial Networks

Chao Wang\textsuperscript{a}, Zhiyuan Li, Lei Huang
Zhengzhou Institute of mechanical and electrical engineering, China
\textsuperscript{a}wlzx@csic713.com.cn
854909839@qq.com

Abstract. With the continuous progress of deep learning, the application has been extended to the identification of dangerous goods in the security inspection system. The quality of the identification algorithm directly determines the quality of the security inspection system. In this paper, a recognition algorithm based on Generative Adversarial Networks is proposed, which can continuously train the generation model and the discrimination model, and collect the image data samples that are blocked or too small, and then generate images with high similarity, so as to achieve the purpose of detecting and tracking the hidden or small dangerous goods. The experimental results show that the algorithm can effectively detect the dangerous goods and greatly improve the tracking effect.

1. Introduction
With the development of big data and AI technology, airport security inspection system is moving towards intelligent and unmanned. Li Jiameng, technical director of Beijing Civil Aviation Security Equipment Corporation, put forward the concept of intelligent security inspection during the 4th China airport safety (Security) conference: smart security inspection is based on high-speed Internet technology, adopts advanced security inspection equipment, has new normalization, diversified and innovative security inspection means and intelligent management security inspection mode. It has six characteristics: integrated operation of network information, integrated transportation system, high-tech automatic security inspection equipment, real-time quality supervision, high efficiency and safety, and low labor input. In the whole security inspection system, the identification of dangerous goods has always been the core process. If we can not monitor any of the dangerous goods, the consequences will be unimaginable.

At present, the mainstream of airport security inspection is X-ray image acquisition. The penetrability of X-ray can make the items in luggage clearly present as images. Wang Huajun \cite{1} and others proposed a detection method based on scale invariant feature transform (SIFT) and implicit shape model (ISM), which collected X-ray images of dangerous goods with different attitudes, labeled the target position, and constructed the training data set; then, extracted the key points of the target through the SIFT algorithm, and constructed the ISM model of the target; In the detection process, the extracted SIFT descriptor is matched with the visual descriptor in ISM model, Voting mechanism is used to judge whether the target is dangerous goods. Although it has certain robustness to the change of target attitude, it is not very good for real-time. AK ó ay s \cite{2} first introduced the deep convolution network \cite{3} \cite{4} into X-ray dangerous goods detection in his work, which applied CNN to the whole process of X-ray image dangerous goods detection, including feature extraction, feature representation
and classification. The transfer learning method [5] is used to fine tune the convolution layer and the full connection layer, so that it can be applied to the field of X-ray image dangerous goods detection. Although the work fully proves the role of deep learning in this field, it does not point out some problems that need to be considered in practical application, such as detection efficiency. The X-ray image dangerous goods detection and tracking algorithm proposed by Lanzhou University [6] is a deep learning detection network based on improved SSD method, which enables the detector to have high detection accuracy under the condition of quasi real-time; on the other hand, the tracker based on the detection results is realized, and the tracking manager is designed to make the detector and tracker work together. However, the detection of small and medium-sized targets in dangerous goods is still not ideal, especially some targets that are seriously squeezed after being adjusted.

2. Generative Adversarial Networks mathematical model

2.1. GANs basic principles
There are two important parts in Gans[7]: 1. Generator: generate data (mostly images) by machine, in order to "cheat" discriminator; 2. Discriminator: judge whether the image is real or machine-generated, the purpose is to find out the "false data" made by the generator.

The training process can be summarized as follows:
1. The first stage: fixed discriminator D, training generator G
   First, we use a discriminator that satisfies the basic function, and let a "generator g" continuously generate "false data", and then give the "discriminator D" to judge. At first, "generator g" was still weak, so it was easy to find out. However, with the continuous training, "generator g" skills continue to improve, and eventually deceive "discriminator D". At this point, "discriminator D" is basically in the state of guessing, and the probability of judging whether the data is false is 50%.
2. The second stage: fixed generator g, training discriminator D
   When the first stage is passed, there is no point in continuing to train generator G. At this point, we fix "generator g" and start training "discriminator D". Through continuous training, "discriminator D" improves his discrimination ability, and finally he can accurately judge all false pictures. By this time, "generator g" can no longer cheat "discriminator D".
3. Cycle phase 1 and phase 2
   Through continuous cycles, both generator g and discriminator D are becoming more and more powerful. Finally, we get a very good generator g, and we can use it to generate the images we want.

The advantage of Gans[8] is that they can better model data distribution (sharper and clearer images) in the first place; in theory, Gans can train any kind of generator network. Other frameworks require the generator network to have some specific function forms, such as the output layer is Gaussian; there is no need to use Markov chain to repeatedly sample, do not need to infer in the learning process, and there is no complex variational lower bound, so as to avoid the difficult problem of approximate calculation of probability.

2.2. Gans algorithm flow
Initializes the parameters of the discriminator $\theta_d$ and initializes the parameters of the generator $\theta_g$.

In each iteration:
1. M sample points $\{X_1, X_2, \ldots, X_m\}$ are listed from the data set $P_{data(x)}$, which is also a super parameter. Considering the data convergence and computer complexity, M is taken as 50 in this paper;
2. List m vectors $\{Z_1, Z_2, \ldots, Z_m\}$ from a normal distribution;
3. Taking Z in step 2 as input, m generated data $\{X'_1, X'_2, \ldots, X'_m\}$ are obtained.
4. Update the parameters $\theta_d$ of the discriminator to maximize $V$. We want to make $V$ the bigger the better. In the following formula, we should make $D(x^i)$ the smaller the better. That is, to lower the score of the generator, we will find that the discriminator is actually a binary classifier:

$$\text{Maximize}(V = \frac{1}{m} \sum_{i=1}^{m} \log D(x^i) + \frac{1}{m} \sum_{i=1}^{m} \log(1 - D(x^i)))$$

$$\theta_d \leftarrow \theta_d + \eta \nabla V(\theta_d) \quad (\eta \text{ is also a super parameter. In this paper, we take } 0.8) \quad (2)$$

Steps 1-4 are used to train the discriminator. Usually, the parameters of the discriminator can be updated more than 20 times;

5. List $m$ vectors $\{z^1, z^2, \ldots, z^m\}$ from a distribution. Note that the enumeration does not need to be consistent with step 2;

6. Update the parameters $\theta_g$ of the generator to minimize:

$$V = \frac{1}{m} \sum_{i=1}^{m} \log(1 - D(G(z^i)))$$

$$\theta_g \leftarrow \theta_g - \eta \nabla V(\theta_g) \quad (4)$$

Step 5-6 is in the training generator. Generally, in the process of training the generator, the parameters of the generator should not change too much, and it can be updated a few times.

3. Experimental results and analysis

3.1. Experimental platform configuration

In this paper, keras open-source framework[9] and tensorflow open-source framework[10] are used as the back-end for convolutional neural network training. Based on win10 professional operating system, simulation software uses anaconda, and the experimental environment is configured as Intel i7-8700, main frequency 3.20 GHz, 32 G memory, graphics card GTX 1600.

3.2. Data collection and sample training

The np-st204 security inspection intelligent analyzer of Hikvision is used to collect and mark dangerous goods. The product adopts embedded design, friendly interactive interface and embedded deep learning algorithm to realize docking with the third-party security inspection machine. It can complete the intelligent transformation of traditional security inspection, realize the network connection of security inspection machine, structure the security inspection image, and carry out intelligent classification of prohibited goods, which integrates video monitoring and docking with Haikang Platform, personnel channel and other business in one.

In this paper, the video containing knives, lighters, small electronic products and bottles of dangerous goods is a 5-hour video. The video is taken every 5 seconds and the sampled image sample is saved. The sample image is shown in Figure 1.
The np-st204 software was used to mark the dangerous goods, and a data set was generated. A total of 1000 images were included, including 750 images as training images and 250 as test images. 75 images were randomly selected as validation set in the training set. The data set is put into the model of generating countermeasure network for training, and the value of map is tested.

3.3. Comparative experiment and analysis

In this section, we test the proposed generated countermeasure network detector. In target detection, the bounding box and confidence of the detection results will be output. The commonly used evaluation criteria are: precision, recall, AP, map, FPS. Firstly, two groups of images with different sizes, 320×320 and 640×640, were set to verify the accuracy and recall rate of knives, lighters, small electronic products and bottles. As shown in figures 2 (a) and (b).

![Image](image1.png)

Fig.2 Sample Precision

![Image](image2.png)

Table 1 performance comparison of testing framework

| Detection framework | FPS | mAP | Tool | Lighter | Small electronic products | Bottles |
|---------------------|-----|-----|------|---------|--------------------------|---------|
| Faster-RCNN         | 16  | 70.12 | 95.12 | 85.67   | 84.56                    | 94.89   |
| YOLO-V3             | 15  | 82.36 | 96.45 | 93.12   | 94.34                    | 95.34   |
| SSD300              | 10.5| 81.45 | 93.78 | 90.15   | 90.19                    | 94.19   |
| GANs                | 10  | 79.89 | 96.35 | 94.89   | 92.28                    | 96.98   |

It can be seen from the table that the average accuracy rate of detectors of Gans, yolo-v3 and ssd300 is roughly the same, which is significantly higher than that of fast RCNN. In terms of detection...
speed, ssd300 and Gans can meet the requirements of real-time detection; for AP indicators of knives and bottles, the four inspection frameworks are basically the same; for lighter and small electronic products, yolo-v3 and Gans showed high accuracy.

4. Conclusion
In the airport dangerous goods detection, the generated countermeasure network algorithm is used to identify the dangerous goods. While ensuring the real-time performance, the map index is kept at a high standard. In the detection of small dangerous goods such as lighters, the accuracy rate is better than other algorithms, which can meet the requirements of airport miniaturization inspection. In the future, the generation countermeasure network will be improved so that it can adaptively meet the real-time requirements and detect all dangerous goods.

References
[1] Wang Hua Jun, Hui Jing. X-ray image dangerous goods detection method based on SIFT features and ISM [J]. Computer measurement and control, 2018,26(01):31-33+37(in Chinese).
[2] Akçay S, Kundegorski M E, Devereux M, et al. Transfer learning using convolutional neural networks for object classification within x-ray baggage security imagery[C]/Image Processing (ICIP), 2016 IEEE International Conference on. IEEE, 2016: 1057-1061.
[3] Krizhevsky A, Sutskever I, Hinton G E. Imagenet classification with deep convolutional neural networks[C]/Advances in neural information processing systems. 2012: 1097-1105.
[4] Szegedy C, Liu W, Jia Y, et al. Going deeper with convolutions[C]. Cvpr, 2015.
[5] Oquab M, Bottou L, Laptev I, et al. Learning and transferring mid-level image representations using convolutional neural networks[C]/Computer Vision and Pattern Recognition (CVPR), 2014 IEEE Conference on. IEEE, 2014: 1717-1724.
[6] Han Ning. Research on X-ray image dangerous goods detection and tracking algorithm based on deep learning [D]. Lanzhou University, 2018(in Chinese).
[7] Khaldi Y, Benzaoui A. A new framework for grayscale ear images recognition using generative adversarial networks under unconstrained conditions[J]. Evolving Systems, 2020(19).
[8] Ma T, Ma J, Yu K, et al. Multispectral Remote Sensing Image Matching via Image Transfer by Regularized Conditional Generative Adversarial Networks and Local Feature[J]. IEEE Geoscience and Remote Sensing Letters, 2020, PP(99):1-5.
[9] Jin H, Song Q, Hu X. Auto-Keras: An Efficient Neural Architecture Search System[J]. 2018.
[10] Alzantot M, Wang Y, Ren Z. RSTensorFlow: GPU Enabled TensorFlow for Deep Learning on Commodity Android Devices[J]. Mobisys, 2017, 2017:7-12.