Identity recognition on POS machine

1. **Background**:

Disadvantages of face recognition:

Currently, face recognition technology is mainly applied in three categories. The first one is to prove the information of the person and the certificate is unified, which is mainly used for real-name verification. This is called 1 to 1 recognition. The second is 1 to N certification, which is to judge whether a person is a member of a specific group, used for personnel access management. Third, vivo testing to ensure that a real person is operating the business, and then grant account licensing or authorize.

Apparently, in public life, the related biotechnology are mainly the first and third, while the second is mainly used for criminal identification and counter-terrorism. Despite the advantages of face recognition such as efficiency, speed and non-invasive, the disadvantages of face recognition are obvious. For example, facial recognition technology may not work well for twins, before and after cosmetic surgery, sudden thinness and fatness, and changes in appearance as people age. What's more, criminals can easily forge fake face to deceive facial recognition technology.

Face recognition system mainly consists of several parts such as face image acquisition and detection, face image feature extraction and matching and recognition. As it stands, there could be bugs in all parts above. As long as a person to provide photos, even the most simple pictures, criminals can make a 3D model with key feature of faces from picture. This 3D model can ‘fool’ the face recognition machine. It will bring great harm to the safety of people.

ATM machine and POS machine is our daily used tool and now the problem is that the machine cannot figure out whether the person in front of the machine is the owner of the credit card. If we lose our credit card, and suppose the card is picked up by others and then it will be used by others. Currently, we most POS machine does not ask pin number and it is not safe. In spite of it, we can prevent this occur by install face recognition software, but this technology has flaw and we cannot totally rely on it.

New solution:

Now we have solved this problem. Our new technology uses deep neural network called GAN to avoid users use fake face to ‘fool’ the face recognition machine. The trained GAN model will be coded into our new software and deployed to credit card POS machine. When customers try to use credit card, they will be asked to smile or turn face left or right to make sure the customer is the owner of the credit card. The progress is slow but it is safe enough, and customers will not lose money any more.

The solution is Artificial intelligence, which is popular recently, and it will perform well in this case. Credit card bank will gain more customers and get more benefits.

2. Aims:

The aim of this project is identity recognition. It means using a system to recognize if the person who is using ATM or credit card is the owner of the card.

To implement this project, there are 3 steps as follows:
1. Collect human face images. This project need to use deep neural network to implement, therefore sample data set is important to the performance of the system. Human face images should include different expression such as smile, angry, left side, right side and so on. When there are more status of a person’s face, the more powerful the system will be. The data resource can be download from the Internet or collect from real world. The recommend is to collect from real world. Our project team will hire volunteers to collect their face images. After that, these images will be stored in our database as important data of this project.

2. Train model and optimize

This is the most important part of this project. We will build our GAN model and test if it performs well as our expectation. This phase will take several months and we will make sure the model performs as good as possible. The performance of the model will also be influenced by the training data which are the face images we collected from volunteer. After optimize, we will build our software and hardware with trained model installed.

3. Deploy the model on machine for test

After the development of software and hardware, deploy it on real machine to test performance. Our project test team will test is first in professional way, and then we will hire volunteer to test from the point of view of customers. Then we will give evaluation of this system. After this step, the system is ready to publish.

4. Apply on real world in small range

After testing our system, we will deploy it on real world in small range like only in Sydney. Because if we encounter some error or bugs in our system we can reduce our lost as minimum. After 3 months of using in Sydney, in our plan, we will find a lot of bugs and fix them.

5. Promote the machine to all cities and get benefit

After we fixed a lot of bugs, we can promote the system in all cities in Australia or even outside of Australia.

3. Research project:

Innovation

GAN principle

GAN is much more different than previous neural networks. The thought of GAN is two-player-game. The total benefit of the two players is a constant number. Suppose two players are playing the game, if one player is stronger, he will have more probability to win the game, while the other player will have less probability to win. In GAN, we will introduce two players as generator (G) and discriminator (D), and they have their own work to do in training. Firstly, the G will do the job of generating an output when it get a input. Secondly, the D is binary classifier and its job is to judge whether its input sample is real sample or generated by G.

What we have is samples we collected from real world, and in this project is samples of human images. What we want to get is to get a human image when getting a input, and the image looks like real human face image. In detail, first, D is a neural network and its input a set of image, while the output is a probability number which is used for judge real or fake. The aim of D is to judge whether an image is from real sample or from fake sample. Suppose the input is real image, then the output will be around 1, while if the input is fake sample, then the output will be around 0. Second, G is also a neural network and input is a group of random number while output is an image. Briefly speaking, G's job is generating samples and it aims to make samples which look like real samples and even D cannot figure out.

At last, if G generates samples and send to D, but cannot figure out if it is real or not, this means G is strong enough. In detail, if G generate samples and send to D, while D's output is close to 0.5, this means D cannot judge if it is from real sample set or from generated sample set. Finally, the model meets balance and it is the result we want.

DCGAN principle

Deep Convolutional Generative Adversarial Networks is an extension of GAN. Add CNN into generator to do unsupervised training. Using the strong ability of feature extraction of CNN to improve generator's performance.

There are 4 features in DCGAN:

1. In discriminator, use stride convolutions to substitute pooling, while in generator, use fractional stride convolutions.
2. Except input layer of discriminator, and output layer of generator, use Batch Normalization in other layers.
3. Delete fully connected layer, connect generator's and discriminator's input layer and output layer with convolution layer.
4. Use Tanh function at output of generator while use ReLu in other layers.

How we judge fake user

In this project, we will generate images of customers' smile, left,and right side of face. Then ask customer to do the same face expression, and compare our generated images with real face. If they are similar, then we can confirm that the customer is the owner of this credit card. Otherwise, this is a fake customer.

detail of project progress

1. The data set :

   Collect human face images and save the data in one directory. Set each image in one file with suffix of jpg, and the size of image is 256 * 256 * 3, which is RGB color image. Make sure every image is different. Then load files into program.

2. Construct the neural network:

   We use Deep Convolutional Generative Adversarial Network (DCGAN), and the steps are:

   - Define Generator: input noise, out put generated image.
   - Define discriminator, judge if the input image is real face or not. Input image, output true or false.
   - define function of saving data, draw the generator's result and save it in file
   - define function of training, set the loss function for both G and D, set variance, set optimizer, set epoch and batch.

3. Training:

   After a long time of training, we will get the result of the trained model. The result is a set of images that generated. We can review the images to see the performance.

4. Tuning parameter:

   We can optimize the performance by change some parameters of the neural network.

Time table

2019.10.30 - 2019.12.30	collect human face images
2020.1.1 - 2020.3.1	train model and optimize
2020.3.2 - 2020.6.1	develop software and add trained model into new software
2020.6.2 - 2020.9.30	deploy on machine and test
2020.10.1 - 2020.10.30	deploy in real business machine

Expect outcome

New POS machine with trained model and apply new solution of identity recognition. When customer use credit card and spend large mount of money, the POS machine will ask customer to smile, or turn face to left, or turn face to right. No fake face can fool the machine. Trading is more safe.

4.Budget:

collect human face images	$20,000
train model and optimize	$200,000
develop software and add trained model into new software	$500,000
deploy on machine and test	$20,000
deploy in real business machine	$20,000

Total: $760,000

5.Personnel:

Data scientist * 3: help to collect data, train and optimize model
Software engineer * 5: develop software
QA * 2: test software
Project manager: control progress of project

6.video:

https://youtu.be/Swlbvws-SU8
Or search “uts ML 2019 ZK” on youtube

Reference

Pan, J., Ferrer, C., McGuinness, K., O&#39;Connor, N., Torres, J., Sayrol, E. and Giro-i-Nieto, X. (2019). *SalGAN: Visual Saliency Prediction with Generative Adversarial Networks*.