Face Identification Lock

SP18 ECE 445

Team #69: Kaiji Lu, Zan Chen, Zekun Hu

TA: Jacob Bryan

Feb. 18th, 2018

Introduction

A. Objective and Background

1. Objective

It is quite annoying when we are at the front door of our houses with hands full of things from the supermarket, but we can not enter in since we still have to take out the key from our packet to unlock the door. Keys, just like pin numbers for our phones, can be more and more replaceable now. A face-identification lock is one solution to the problem of finding keys and losing keys. Instead of putting things on the ground and then use our free hand to get the key and unlock the door, we can easily stand in front of a camera and then the door will automatically unlock after it identify us.

The project we propose seizes the achievement of turning a cheap camera into an intelligent guard. Nowadays, face identification has been an active area with many deep learning methods. Specifically, a neural network approach is good to tackle the face detection to maintain a high accuracy. [1] Even though the system does not necessarily seem more secure than a regular lock, it does provide us a much more convenient way to open the door when our hands are full while the tradeoff of security is in an acceptable level.

2. Background

At present, people are paying increasing attentions to home securities. The market of home security products will possibly reach 12 billion USD by 2025. In particular, the image processing technology has made more and more security solutions possible such as smart monitor systems or motion triggered cameras. [2] As an alternative to traditional security systems that use passwords, cards, or keys, face recognition lock is one of the image processing technology that both offers users great convenience of hands free operation and ensures the sensitive area to be monitored and controlled.[3] However, we have to agree that face identification is a hard to formally describe coding problem, which there would be no such formula or rule to define one person's face. So, we choose machine learning to approach such problem. We let the computer to learn from the experience by feeding with input and hand-designed features or multiple layers of features depend on the algorithm we choose. By mapping from those features, the computer is able to provide us the output.

Our project only requires old cameras, so it is cost effective and reliable compared to the average price of 400 USD of existing products in the market.

B. High-level Requirements List

1. The face identification accuracy must be at least 85%.
2. The entire operation cycle must be within 8 seconds.
3. The system must be able to control the lock so that it remains locked all the time expect when face is identified.

Design

A. Block Diagram

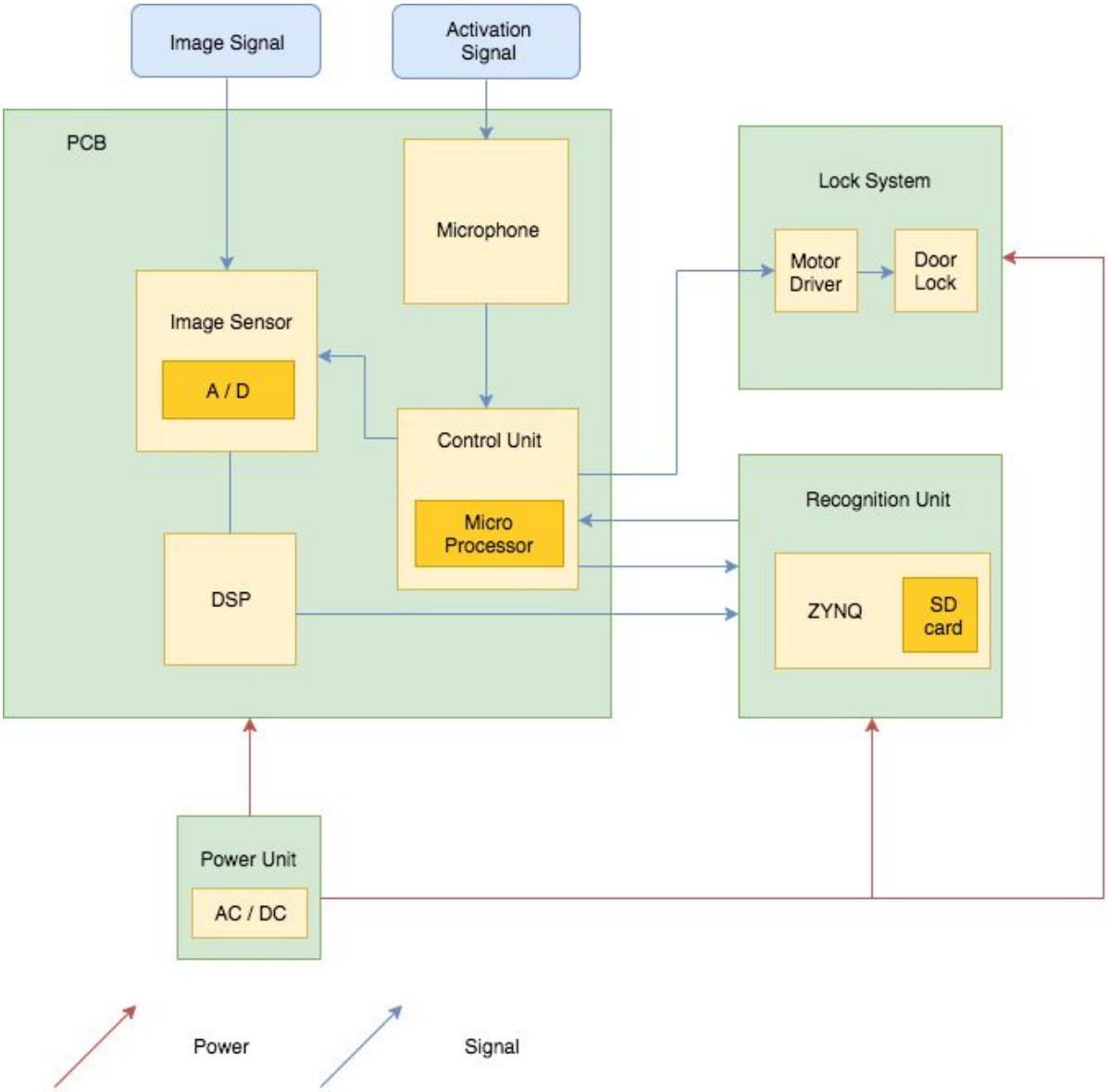

Figure 1. Block Diagram of the System

B. Block Descriptions

1. PCB

Description:

The PCB contains the following subunits:

- Image sensor: We plan to use OV7725 CMOS sensor which outputs image of 640x480 pixels at a maximum rate of 60 fps.
- Sound sensor: We plan to use Sparkfun SEN-12642 sound detector.

- Microprocessor & DSC: We plan to use PIC33E MCU that controls the operation of the whole system. For example, the activation of image sampling, and the control of motor driver.

Requirement:

- Power requirement for our PCB is roughly 15V.

2. **Lock System**

Description:

The lock system includes the following subunits:

- Motor Driver: The motor driver receives an PWM signal sent by aforementioned microprocessor. Then it sends an unlock signal to the door lock.
- Door Lock: We plan to use FC MXBB DC door lock. Upon receiving the unlock signal, it rotates to unlock the door. It will remain unlocked for a short amount of time and tries to relock the door.

Requirement:

- Input: PWM signal sent by the control unit.
- Voltage requirement for the lock system is 12V, power requirement is 9.6W.

3. **Power Unit**

Description:

Power unit supplies DC power to all the other units. It is connected to a AC wall plug, with a AC to DC converter. We also need to design a regulator that stabilizes the circuit.

Requirement:

- All of the input voltage to the chips and units should be strictly controlled within limit range.

4. **Recognition Unit**

Description:

Face identification runs on a ZYNQ FPGA board. Its input is the pre-processed image from the DSP chip. The input test image should be tested by the pre-trained neural network, and the recognition unit should be able to output identification result that is either true or false. The output signal will go back to the control unit.

The recognition unit includes the following subunits:

- PYNQ: FPGA board based on ZYNQ chip with BNN framework[6] supported.
- SD card: SD card can be used as memory once formatted.

Requirement:

- The recognition process should be done very fast within a second.
- It should output unambiguous decision, either lock or unlock.

C. Risk Analysis

We could have both hardware difficulty and software difficulty. Since OV7725 outputs 640x480 rgb pixels, it would require the DSP chip to have enough RAM for processing. Our main concern in hardware is that if the DSP chip can output correct processed data expected by the neural network. Also, the communication of every unit, transmission of data and the consistency of the system can cause troubles. On the software

side, we do not know if the input data from hardware needs to be realigned and there could be difficulties implementing neural network and SoC.

Since our project is a security device, lowering the error rate is extremely essential. There are two types of error: a false negative and a false positive. A false negative will lock the user from entering the door, but could be simply solved by a key. Just like the face id system of iPhone 10: a negative result of recognition would prompt the password option. A false positive, however, is way more dangerous. It would allow intruders to use this glitch to unlock the door.

With our current algorithm and design, the estimation of the total error rate is less than 15%. False negative rate is estimated around 10%, therefore the false positive rate should be less than 5%. We will try to improve our facial recognition algorithm to reduce false positive rate.

Ethics and Safety

There are some ethical concerns with our project. As our project includes a facial identification, we inevitably need to process people's photos. We here promise that all the information through our technology is confidential as we should not go against the IEEE code of Ethics. As #1 and #9 mentions, we have to "disclose promptly factors that might endanger the public or the environment " and "avoid injury other's property." [4]

Since our project relates to a door lock , we have to try our best to improve the accuracy of our algorithm. As following the IEEE code of Ethics #7 , we humbly accept helpful advices or criticisms from all sources and we ensure that we credit these contributions properly. Besides, according to the IEEE code of Ethics #3, even if our final project does not come to be as accurate as we expect initially, we promise to report the true result and give justified claims. [4]

The safety of our physical design is relatively high. We may have potential overheat for several chips and a motor which controls the lock. However, we do need to pay attention to our data safety when we use convolutional neural network to accomplish the goal of face identification. We have to watch out whether the data are going somewhere else when we did not intend. That's a big safety concern and an ethical issue as we talked before. All cloud services based on the US, the UK, France and other jurisdictions known to be tolerant of NSA-style snooping, which means the data we store on the cloud services all have potential danger of being accessed by others. [7] Thus, it is important for us to protect these identifiable information that we collect during our trials. One potential way to keep our data safe is to encryption and avoid storing too much data on the cloud services.

Finally, we aim to create good, safe and convenient intelligence system for others. To meet ACM Code of Ethics and Professional Conduct #1.1 , we dedicate to create a "safe social environment" as well as a "safe natural environment." [5] That's why our product aims to be lower cost than a surveillance camera but also high-accuracy promised intelligence system.

References

[1], Y.An *CNNs for Face Detection and Recognition*, 2017 [Online]. Available http://cs231n.stanford.edu/reports/2017/pdfs/222.pdf [Accessed: 07-Feb-2018]

[2]prnewswire.com(2018), "Global Home Security Products and Solutions Market to Reach US$ 12 Bn by 2025". [Online]. Available: "https://www.prnewswire.com/news-releases/global-home-security-products-and-solutions-market-to-reach-us-12-bn-by-2025-640292763.html)
[Accessed: 08-Feb-2018]

[3] H.Htlar Lwin , "Automatic Door Access System Using Face Recognition" "http://www.ijstr.org/final-print/june2015/Automatic-Door-Access-System-Using-Face-Recognition.pdf")

[4] "IEEE Code of Ethics", ieee.org, 2017. [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 07-Feb-2018]

[5] Acm.org. (1992). ACM Code of Ethics and Professional Conduct. [online] Available at: https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct [Accessed 07-Feb-2018].

[6] R. Zhao, W. Song, W. Zhang, T. Xing, J. Lin, M. Srivastava, R. Gupta, Z. Zhang, "Accelerating Binarized Convolutional Neural Networks with Software-Programmable FPGAs"[Online] Available "http://www.csl.cornell.edu/~zhiruz/pdfs/bnn-fpga2017.pdf"

[7] J.Naughton (2013), "Internet security: 10 ways to keep your personal data safe from online snoopers" [Online]. Available: https://www.theguardian.com/technology/2013/sep/16/10-ways-keep-personal-data-safe