CryptoCam

(Cryptograph Camera)

Team 17 – Jihoon Lee, Sameeth Gosike, and Sang Baek Han
ECE 445 Project Proposal – Spring 2017
TA: Jose Sanchez Vicarte

1 Introduction

1.1 Objective

Taking the photograph using a camera has become such an easy task nowadays. As the technology improved, more people use smartphones to take the photograph rather than carrying extra device that can only take the photograph. As for the smartphone, they do have the encrypted software available freely and reliably. However, the professional camera used by photojournalists and anyone related to that field still do not have access to any type of encryption. The encryption is necessary for the professional camera so that it provides the immediate protection from unexpected damage, lost, or robbery of camera [1].

Our solution to this problem is to use the additional hardware components between camera data bus and memory storage so that when the photo is taken, the photo will immediately get encrypted and then stored. Only the authorized user who has the access to this additional hardware with the right key can see the decrypted image.

1.2 Background

Last year December, Freedom of the Press Foundation had published an open letter to the world-leading camera manufacturers such as Nikon, Sony, Canon, Olympus, and Fuji to build a camera with the encryption features for the sake of filmmakers and photojournalists. Those filmmakers and photojournalists are occasionally exposed to dangerous subjects which lead to the threat from the authoritarian governments or criminals. With their camera full of unencrypted images, they have no way to protect themselves from such risk [1].

1.3 High-Level Requirements

- Timing requirements – For benchmarking, an experiment reported average time of 0.38-0.40 second to encrypt 512x512 image that are 24-bits each, using a computer with Pentium 4 processor (x86) [2]. The resolution is very close to ones we are planning to use (640x480). Considering the operating frequency of Pentium 4 processors is typically near 3Ghz, and our microcontrollers would be at 200Mhz max, realistic time achievable by our design would be approximately 15 times of that achieved by the experiment, which would be 6 seconds. This is our current goal.
- Level of Encryption – Success of the encryption relies on how different the encrypted picture is from the original data. Correlation coefficient will be used as a quantitative measure of the difference, which determines the similarity between values of two adjacent pixels. An well encrypted image will have near 0 value.
- Decryption functionality – The result of the decrypted image data should be exactly identical to the original picture. The matching rate will be used as quantitative measure of success, which will be (number of pixels that match / total number of pixels). This will be done using the software.

- Power constraint – Processor and camera both powered by about 3V of voltage. We want the camera to run for about 2 hours at the power-on state with the capability of taking approximately 60 photos. Considering that we favor a battery size close to typical GoPro camera with rechargeability (due to size and similar voltage range to ours), which are rated at 3.8~4.4Wh, we want our average power consumption around 1.9~2.2 Watts. Fortunately, our camera only dissipates 60mW in its active state, which means we need to fit our SRAM and microcontroller into that range.

2 Design

The design makes acquisition of data from camera module and utilizes data processing unit to encrypt the data. The usage of SRAM helps the achievement of timing requirement due to its faster speed compared to other species of memories.

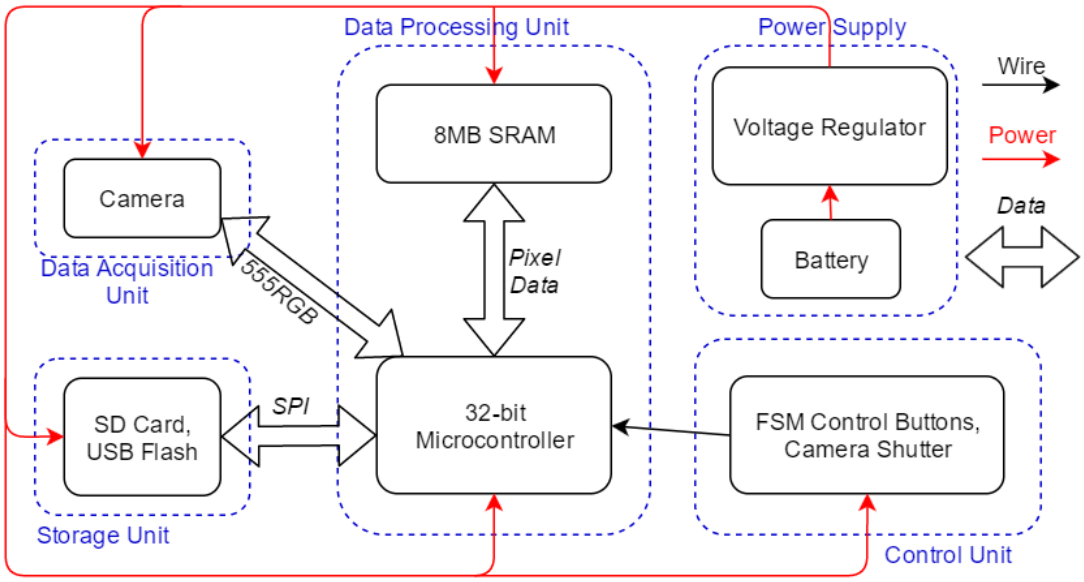

Figure 1 – Block Diagram

2.1 Data acquisition Unit

Data acquisition unit is composed of a single camera (OV7670), which uses light sensitive receptor array to acquire optical input and translate it into RGB data. It is connected to Data Processing unit to encrypt the data.

There is no set of requirement for this unit since it is a commercial camera that our design cannot change. Most improvements are done in other units.

2.2 Data Processing Unit

Data processing unit is centered on a 32-bit microcontroller. 8MB of SRAM is used to store pixel data, which is 600KB (too large for internal RAM), and the variables that are needed to process the whole pixel data. DSP unit will have bidirectional connection with microcontroller to transform data into frequency domain and then pass it back to microcontroller to encrypt it.

The requirement for this unit is to dissipate less than 2.2W of power at fully functional state. (maximum dynamic power) to satisfy power requirement. And we will need to make sure flash memory is big enough in microcontroller (not sure how big at this time) to fit in a

functionality of DSP transform library.

And the I/O pins of Microcontroller should be high in number (at least 82-bits reserved for SRAM(s)) to prepare for case where additional SRAM is used to improve image buffer capacity. SDRAM may be more convenient due to higher capacity (SRAM will be no more than 2MB, while SDRAM may reach up to 16MB) , but SRAM will provide much faster access, helping us to meet timing requirement.

2.3 Control unit

Control unit is responsible for controlling FSM state between key acquisition phase, picturing phase, encryption phase, and reset phase. An additional shutter button will be used to signal the data processing unit to acquire data from acquisition unit.

Control unit should be able to debounce abrupt fluctuations in signals from buttons. Otherwise, processor will be loaded with more instructions to run than needed, affecting our power requirement. We will design an additional RC circuit if problem arises, but we are yet to decide on this.

2.4 Storage Unit

The Storage unit is responsible for the storage of the encrypted images after they are processed by data processing unit. It will consist of a typical USB flash drive to store the encryption key and SD card to store the encrypted image. Both of them share I/O to and from the microcontroller.

The storage capacity will be on the lower side (8Gb) since the main goal of the project does not include storing a large number of pictures. However, in order to read/write to the memory device from and to the microcontroller, a separate USB/SD module will have to be included in between. This will be much more successful than trying to create a protocol in the microcontroller.

2.5 Power Supply Unit

Power supply will comprise of battery and voltage regulator. The maximum voltage allowed for camera is 3.0V while processor may need higher input, which is why we need it. Camera can theoretically operate at 3.0V, but there has been serious malfunctions at this level on one of previous projects, so we will likely operate at fairly low voltage to avoid losing cameras.

Some searches indicate that 32-bit microcontrollers would consume around 1W when active, but its anecdotal at best. SRAM seems to consume a few mW and camera consumes 60mW. This makes total consumption approximately 1.1W, making necessary battery capacity 2.2 Wh to run 2 hours of camera.

If our estimation turns out to be true, we may even use multi-core to separate image reception and encryption in separate processors, but we are yet to estimate actual power consumption.

2.6 Risk Analysis

The biggest risk lies in the interface between data acquisition unit and data processing unit. While input clock to the processors and camera can be synchronized, the output pixel clock of camera may not be precisely synchronized with the input clock. We will be scaling input clock inside camera so that it runs slower than the input clock, and using multiple-cycle instructions to get data.

As final contingency plan, we may use the output pixel clock of camera as clock source of processor, but camera has slow operating speed and this will prevent us from utilizing high operating frequency of processor.

3 Ethics and Safety

There are potential ethical and safety issues regarding to our project. One ethical issue is whether the photo taken does deserve to be encrypted and remained unknown for non-authorized user. As for example, secret photography is the most concern as it can be used for stalking, paparazzi, and hidden camera inside the room. If ever those photographers got caught, then it will be hard to get the evidence out of encrypted image when the access key is broken or purposely damaged.

One way to solve the above issue is to provide the alternative method to decrypt the image. But, at the same time, it raises the issue on the reliability of our encryption and decryption system. The users expect that our decryption is only allowed with one way so they can safely take the photos without being exposed to the risk of getting caught. If there is some way to recover the encrypted image and used as an evidence, then there is no point of using our camera. We will positively assume that this project will be used by modest users, who accept the responsibility as mentioned in #1 of the IEEE Code of Ethics, “to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment” [3].

References

[1] A. Greenberg, "150 Filmmakers Ask Nikon and Canon to Sell Encrypted Cameras," in WIRED, WIRED, 2016. [Online]. Available: https://www.wired.com/2016/12/200-filmmakers-ask-nikon-canon-sell-encrypted-cameras/. Accessed: Feb. 6, 2017.

[2] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, no. 9, pp. 926–934, Sep. 2006.

[3] "IEEE IEEE code of ethics," in IEEE.org, 2017. [Online]. Available: http://www.ieee.org/about/corporate/governance/p7-8.html. Accessed: Feb. 8, 2017.