Computer Security Symposium 2020
26 - 29 October 2020

Thermal Image Human Thermometer and Its Privacy Protection with Raspberry Pi

Yuan Yang[1,a)] Yuta Kodera[1] Takuya Kusaka[1] Yasuyuki Nogami[1]

Abstract: From December 30th, 2019, the novel coronavirus exploded in Wuhan, Hubei Province, China[1]. It is believed that body temperature detection is required for the suspected infectors. However, if one uses a thermometer touching the skin of others, cross infection may occur. In terms of hygiene, it is considered that a non-contact temperature detection is necessary. We tried to use AI technology such as face detection, combined with thermal imaging technology to measuring body temperature, to avoid cross infection through contact equipment. In this study, we developed an attendance record application to detect body temperature within 2 meters which based on Raspberry Pi, infrared sensor MLX90640 and ultrasonic distance sensor HC-SR04. We designed this application for scenarios where do not require identity authentication, such as hotels and event centers. In actual use, we need to record daily measurement information. From a data security perspective, we have to protect the privacy of the detected person. Therefore, we used searchable encryption technology to encrypt the detected person's photo, time, and body temperature. By using searchable encryption technology, we can ensure the security of information in the server, and only the authorized person can search personal information encrypted. As a result, we can detect people's temperature and the measurement error rate is below 1% within 2 meters without a mask. And personal data in the server can also be protected by searchable encryption.

Keywords: Non-contact temperature detection, Raspberry Pi, Thermal imaging, Searchable encryption

1. Background

On December 29, 2019, when one of the unknown pneumonia patients in Wuhan City, Hubei Province, China[1], was sent to Jinyintan Hospital in Wuhan, the novel coronavirus exploded all over the world without limitation from China. The novel coronavirus have an incubation period, and person infected have an unstoppable cough and long-term fever during this period. Critically ill patients are dyspneic and life-threatening[2]. The virus has widespread worldwide since January 30, 2020, when the World Health Organization (WHO) declared an 'Emergency'. As of July 20, there were more than 14 million infected people worldwide[3]. It seemed that vaccine research in each country were progressing at that time, but a perfect vaccine does not yet exist.

For these reasons, it seems that personal protection methods are necessary. There are various ways to protect an individual by putting on a mask, using rubbing alcohol paper and stay away from crowds. However, it is considered to be necessary to examine body temperature in places where there are many people, such as organizations and companies.

At present, there are a contact and a non-contact body temperature test.

The contact type is a device in which the temperature of the skin surface can be recorded when the inspection device comes into contact with human skin. There are electronic thermometers and mercury thermometers on the market, and the price ranges from 800 yen to 1500 yen. From a hygiene perspective, if one use a contact thermometer, it is necessary to to avoid using the equipment other used. Besides, the resistance of the temperature sensor of the electronic thermometer changes with the skin temperature, then the temperature data changes. A mercury thermometer is a device that displays temperature data by the volume of liquid which changes with the temperature. From the above example, it was found that the contact test comes in contact with the human body and has a disadvantage that it takes time to wait for the change of resistance or liquid.

The non-contact test use a device that the temperature of the skin surface can be recorded without the touch of human skin. For example, there is a radiation thermometer and a forehead thermometer, and their prices are both over 7 thousand yen. A non-contact thermometer is a device that measures the temperature of an object by measuring the intensity of infrared rays emitted from the object. It is possible to measure the temperature of an object by measuring the intensity of infrared rays from an infrared sensor and changing the analog signal of intensity to a digital signal of temperature. The non-contact thermometer uses an infrared sensor to measure the intensity of heat radiation from

[1] Graduate School of Natural Science and Technology, Okayama University, Japan
[a)] pmny2wnp@s.okayama-u.ac.jp

the human skin and record the body temperature. Infrared sensors are expensive in the current market, and the price of equipment using infrared sensors is around 20 thousand yen. A thermometer with a monitor is a device that can display a temperature measurement screen. The market price of such a thermometer is about 400 thousand yen, which is too expensive for personal.

Therefore, in this study, we developed a visually non-contact thermometer based on the Raspberry Pi using the infrared sensor MLX90640 and ultrasonic distance sensor HC-SR04. Finally, to protect personal privacy, we tried to use searchable encryption to encrypt the information of the detected person. Through searchable encryption, we can search data while keeping the information encrypted, which can protect the data uploaded to the server from being illegally stolen. As a result, the measurement error within 2 meters is within 1% without a mask. And the proposed system is 33 thousand yen.

2. Thermal imaging

An object whose temperature above absolute zero($-273.15°$C) emits radiation. The wavelength of visible light is 0.4μm to 0.7μm, focusing on infrared rays with a wavelength of 3μm to 14μm. The intensity of infrared rays of this wavelength is directly proportional to the temperature[4]. Therefore, if the intensity of infrared rays can be measured, the temperature can also be calculated.

The infrared sensor used in this study is MLX90640. The sensors on the market have two fields of view, $55° \times 35°$ and $110° \times 75°$, but in this study, $55° \times 35°$ was selected and implemented. The sensor can be measured temperatures from $-40°$C to $85°$C. In addition, the temperature can be searched twice in 1 second with the Raspberry Pi 3 series.

2.1 MLX90640

The specifications of the MLX90640 infrared sensor are shown as figure 1.

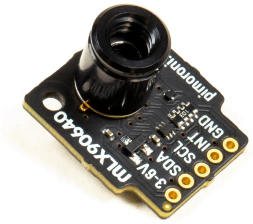

Fig. 1 MLX90640

In this study, we used a sensor with a viewing angle of $55° \times 35°$. The effective distance of this sensor is calculated what is shown formula (1).

$$S = \frac{D}{2 \times tan\alpha}, \tag{1}$$

where S is the distance, D is the size of the object, and α is the viewing angle.

α is the angle between adjacent detection lines. Since the sensor of $55° \times 35°$ can take 32×24 pixels, α here is

$$\alpha = \frac{55°}{32 - 1} \approx 1.8°. \tag{2}$$

In this study, if we substitute D for the size of a person's head of about $0.2m$ and substitute α for $1.8°$ to calculate the temperature of the human face, the effective distance is

$$S = \frac{0.2m}{2 \times \tan 1.8°} \approx 3.3m. \tag{3}$$

The temperature error of MLX90640 is $1°$C, but the decimal point of the temperature can be estimated by the program. The MLX90640 uses I2C to transfer data to Raspberry Pi. The data is processed on Raspberry Pi.

2.2 Image processing

Data from MLX90640 becomes 1 row and 768 columns through I2C communication. In addition, it is necessary to change the shape of the image data in order to visualize these data.

The data of 1 row and 768 columns can be changed to 24 rows and 32 columns. However, this 24×32 matrix cannot directly become an image. A normal image requires RGB(Red, Green, Blue) data. So we used pseudo-color to make an image.

Pseudo-color is a technology that allows you to add color to the data in the matrix to create an image.

The data of the 24×32 matrix is unified to 0 to 255, and changed by specific color. Finally, we could get a colored image. The pseudo color used in this study is the color named JET of OpneCV. Figure 2 shows an example of changing a specific color from an ordinary matrix data.

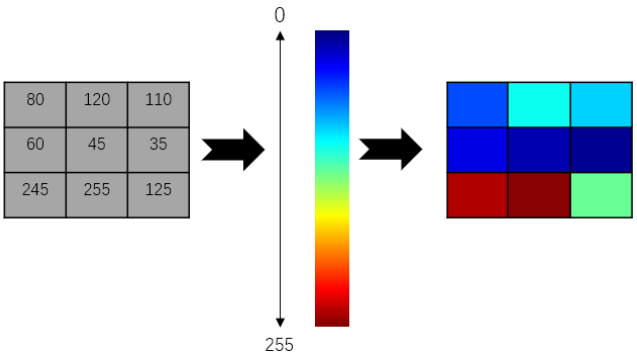

Fig. 2 Pseudo-color

3. Face detection

Nowadays, people have become accustomed to wearing masks when going out. Wearing a mask makes face detection more difficult. Thanks to team AIZOOTech[5], they had made face detection models under some mainstream frameworks, such as TensorFlow and Pytorch. We used their models to make our system to detect masked faces.

We used a common Raspberry Pi camera to detect the position of face, and compared the position information with thermal image to obtain the temperature of the face.

4. Infrared attenuation

When we used the system to measure temperature of people, we found that the temperature error is related to distance. According to Zhou et al. *Influence of Observation Distance and Angle of View on the Detection Accuracy of Infrared Thermal Radiation*, the attenuation of infrared rays is related to measured distance and observation angle [6]. As a result, figure 3 shows the result of the study. In an air environment, infrared intensity is negatively correlated with measuring distance.

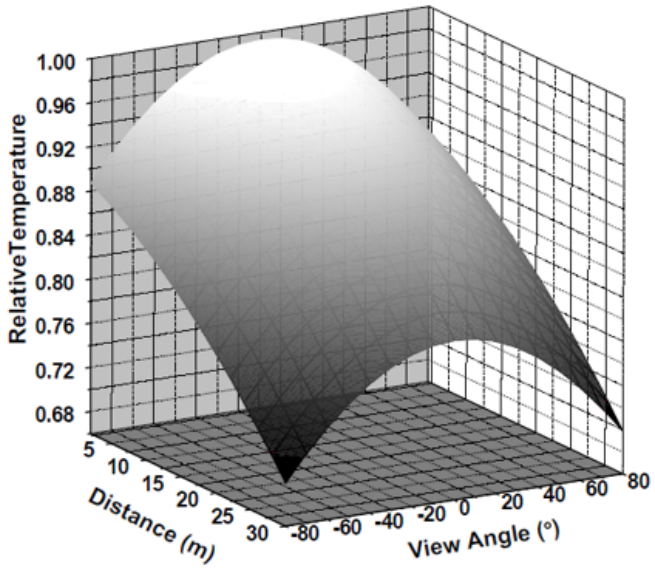

Fig. 3 The attenuation of infrared rays is related to the measured distance and the observation angle

Following this rule, we used an ultrasonic distance sensor to measure the distance between the measured human body and camera, so that we can use the relationship between distance and infrared attenuation to correct measured data.

5. Ultrasonic ranging

The ultrasonic transmitter emits ultrasonic waves in a certain direction and starts timing at the same time as the transmission time. The ultrasonic waves propagate in the air and return immediately when they encounter obstacles on the way. The ultrasonic receiver stops timing immediately after receiving the reflected waves. This method to measure distance called time difference ranging method.

$$s = \frac{346.60 \times t}{2} m. \tag{4}$$

Formula 4 shows the distance calculation method of ultrasonic ranging. The distance s can be calculated by the speed of ultrasonic at room temperature(25°C), $346.60m/s$, and time t means the one round trip time by ultrasonic.

Through ultrasonic ranging, we can obtain the distance between the measured person and the camera, combined with the characteristics of infrared attenuation, thus we can achieve data correction.

6. Log records

In this study, we can save logs about the information for measuring body temperature. We tried two methods of searchable encryption to encrypt our log records. Searchable encryption technology provides a method that can search words while keeping the ciphertext encrypted. By using searchable encryption, we can guarantee the security of the data in the server. Because the server does not know the encryption method or other parameter of encryption, it could not get the plaintext. Through using these methods, we can protect personal privacy of the detected person.

6.1 Application scenario

We designed this system for hotels or event centers, in which places temperature monitoring is required. By using this system which record facial images, name, and temperature information, we can ensure the safety of guests in hotels or event centers.

In order to protect the personal privacy of guests who enter the hotel or center, we use AES encryption to encrypt facial image and use searchable encryption which we talked about in section 6.2 and section 6.3 to encrypt name and temperature information associated with facial image.

When we want to get the information about some guests, we can find the guest's information(just facial image and temperature information) by searching the name label.

In this way, we can ensure that guests have no fever, and use encryption technology to protect guests privacy.

6.2 Public key encryption with keyword search(PEKS)

According to Boneh et al. in paper *Public Key Encryption with Keyword Search*[7], they create a method called public key encryption with keyword search(PEKS). Suppose Bob want to send an encrypted email to Alice using Alice's public key. Bob can use this method to encrypt his email. This method goes through the following 4 steps:

①$KeyGen(s)$: takes a security parameter, s, and generates a public/private key pair A_{pub},A_{priv}.

②$PEKS(A_{pub}, W)$: for a public key A_{pub} and a word W, produces a searchable encryption of W.

③$Trapdoor(A_{priv}, W)$: given Alice's private key and a word W produces a trapdoor T_W.

④$Test(A_{pub}, S, T_W)$: given Alice's public key, a searchable encryption $S = PEKS(A_{pub}, W')$, and a trapdoor $TW = Trapdoor(A_{priv}, W)$, outputs 'yes' if W = W' and 'no' otherwise.

To implement this method, Boneh et al. used a bilinear map, $e : G_1 \times G_1 \rightarrow G_2$, and two hash functions, $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : G_2 \rightarrow \{0,1\}^{logp}$, where G_1, G_2 are two groups of prime order p. The details of the methods as follows:

①$KeyGen$: The input security parameter determines the size, p, of the groups G_1 and G_2. The algorithm picks a random $\alpha \in \mathbb{Z}_p^*$ and a generator g of G_1. It outputs

$Apub = [g, h = g^{\alpha}]$ and $A_{priv} = \alpha$.
②$PEKS(A_{pub}, W)$: First compute $t = e(H_1(W), h^r) \in G_2$ for a random $r \in \mathbb{Z}_p^*$. Output $PEKS(A_{pub}, W) = [g^r, H_2(t)]$.
③$Trapdoor(A_{priv}, W)$: Output $T_W = H_1(W)^{\alpha} \in G_1$.
④$Test(A_{pub}, S, T_W)$: Let $S = [A, B]$. Test if $H_2(e(T_W, A)) = B$. If so, output 'yes'; if not, output 'no'.

We can find that, this method uses finite field operations, such as in $PEKS(A_{pub}, W)$. Finite field operations are very difficult for small CPUs such as Raspberry Pi. When we implement this method to encrypt our log records, we have to stop temperature measurement to calculate the ciphertext from log records.

6.3 Searchable encryption

We also tried the searchable encryption by Song et al. in paper *Practical techniques for searches on encrypted data*[8]. Using this method we can encrypt our log data and upload it to a server safely.

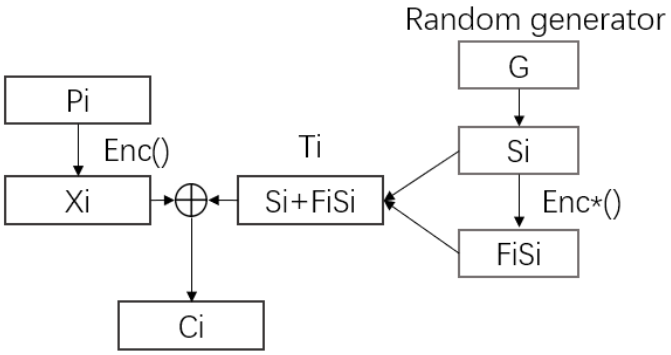

Fig. 4 Encrypt data by searchable encryption

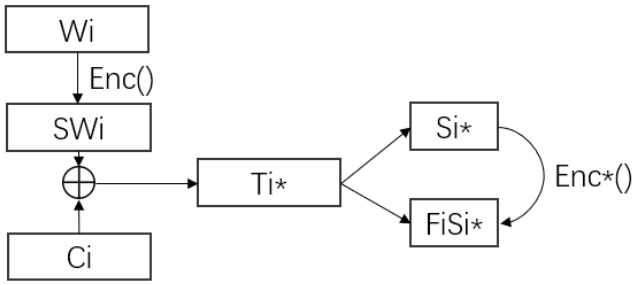

Fig. 5 Search data in encrypted data

Figure 4 shows that we can use this method to encrypt data. Pi is a plaintext that we want to encrypt. $Enc()$ and $Enc*()$ means the difference encryption functions we used. G is a random generator, which can generate random number Si. And if use an encryption function $Enc*()$ we can get $FiSi$, which is the ciphertext of Si. And Ti is composed of Si and $FiSi$. Using XOR operation between Xi which is the ciphertext of Pi and Ti, we get the final ciphertext of Pi called Ci which can be searched by keeping encryption.

When we need to search something we just upload the encrypted word by $Enc()$, like figure 5. If server return the result of $Enc*(Si*) == FiSi$, we can confirm that the data Wi exists.

For example, table 1 shows one of our log records. We can encrypt these data word by word by searchable encryption. If we want to search temperature information about Alice, we can search the keyword 'Alice'. And if we get 'True', which means there are temperature information about Alice. This method is not as safe as the method mentioned above in section 6.2, but we can perform data encryption and temperature measurement at the same time.

Table 1 One example of log information

Photo	Name	Temperature
Photo_1	Alice	36.4
Photo_2	Bob	36.5
Photo_3	Caroline	36.7
Photo_4	Dana	37.5

7. Implementation

In this study, we used Raspberry Pi 3A+ model for data processing. At the same time, we used the MLX90640 infrared sensor and ordinary Raspberry Pi camera for human body temperature measurement. As to the data visualization part, we have two options, the one is to use a 5-inch monitor, the other is to use LCD1602. By using a 5-inch monitor, we can display real-time images. However, using LCD1602 can only display temperature data. HC-SR04 is the ultrasonic ranging sensor. Table 2 lists the equipment and unit price used in this study. It should be noted that the total of 33 thousand yen is used, which is much cheaper than the products(which is about 300 thousand yen) on the current market.

Table 2 Devices and price(yen)

Raspberry Pi 3A+	3,300
AC adapter	1,100
microSD	1,000
PiCamera V2.1	3,200
MLX90640	16,000
5-inch monitor	5,000
LCD1602	300
HC-SR04	200
Other	3,000
Total	33,100

The figure 6 is the overall appearance of the whole system. As you can see, the monitor can show real-time images of people standing in the front of the camera. And LCD1602 can show the temperature data at the meantime.

Fig. 6 The overall appearance of the system

8. System evaluation

In this study, in order to measure the reliability of the system, we recorded data at a distance of 20cm, 50cm, 100cm, 150cm, and 200cm from the camera. Figure 7 shows the

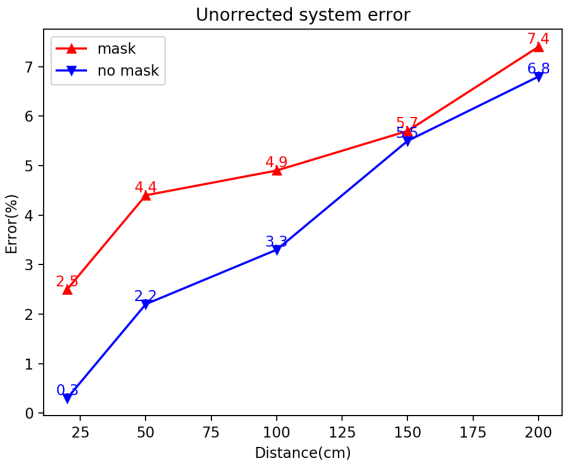

Fig. 7 Uncorrected system error

result of our evaluation without correction. At 20cm we got the minimum error of the system, which means that our system can measure human temperature more accurately at 20cm.

Just like what we talked about infrared attenuation in section 4 above, we concluded that infrared attenuation is related to distance. And, MLX90640 can only get 768 pixels data once, which makes the data far away from the camera insufficient. So, the father distance is, the bigger error is in our system evaluation.

In order to reduce the error, we used ultrasonic distance sensor HC-SR04 to calculate the distance between the camera and the person who was detected. By using the relationship between infrared attenuation and distance, we can reduce system error.

As a result, we got the figure 8. As you can see, we use the distance information to correct the temperature, we can ensure that the error is below 1% in 200cm without a mask.

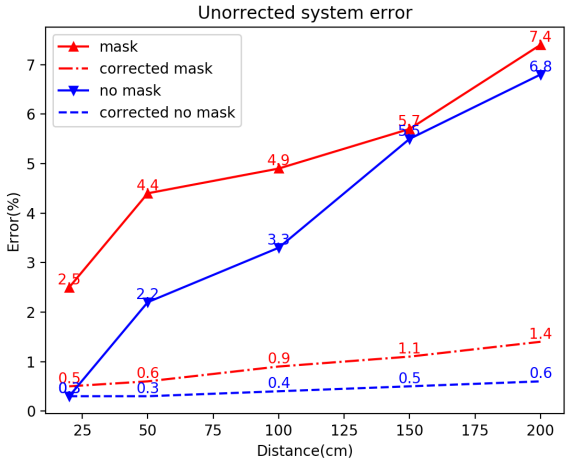

Fig. 8 Corrected system error

9. Conclusion

In this study, we implement a thermal imaging system to measurement people's temperature by using MLX90640 based on Raspberry Pi 3A+. As a result, we got the measurement error within 1% within a 2m without a mask. And the total cost of this system is 33 thousand yen, which is much cheaper than those products on markets. And, we tried two searchable encryptions to protect personal privacy. In the application scenario we designed, we can ensure that the guests entering a venue have no fever, and those with permission can use the search application to search for personal information in encrypted data.

References

[1] Chaolin Huang, et al. 2020. *Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China.* The Lancet, 395(10223), pp.497-506.

[2] Nanshan Chen, et al. 2020. *Epidemiological and clinical characteristics of 99 cases of 2019 novel coronavirus pneumonia in Wuhan, China: a descriptive study.* The Lancet, 395(10223), pp.507-513.

[3] Who.int. 2020. *Coronavirus Disease(COVID-19)–World Health Organization.* Available at: https://www.who.int/emergencies/diseases/novel-coronavirus-2019.

[4] Lloyd, J., 2013. *Thermal Imaging Systems.* Springer Science and Business Media.

[5] GitHub. 2020. *Facemaskdetection.* Available at: https://github.com/AIZOOTech/FaceMaskDetection.

[6] Zhicheng Zhou, et al. 2017. *Influence of Observation Distance and Angle of View on the Detection Accuracy of Infrared Thermal Radiation.* Infrared Technology(39), pp.86-89.

[7] Boneh, D., Di Crescenzo, G., Ostrovsky, R. and Persiano, G., 2004. *Public Key Encryption with Keyword Search.* Advances in Cryptology - EUROCRYPT 2004, pp.506-522.

[8] Song, D., Wagner, D. and Perrig, A., 2000. *Practical techniques for searches on encrypted data.* Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000, pp.44-55.