Research on High-Speed Face Authentication Algorithm for IoT Devices

Naoya Shinozaki[a,*], Lifeng Zhang[a]

[a]1-1sensui-cho Tobataku, Kitakyushu city, Fukuoka Japan 804-8550
Kyushu Institute of Technology

*Corresponding Author: shinozaki.naoya223@mail.kyutech.jp

Abstract

Face authentication has been widely recognized as one of biometric authentication techniques and has been put into practical use in various situations. But faces changes, and it is still affected by changes in facial expressions and face orientation. There are also many technical difficulties. Also, face authentication requires both compatibility of accuracy and speed, but it is difficult to implement complicated calculations with ineffective devices.

In this study, we show that we simplified the face authentication algorithm for IOT devices, and that a certain level of face authentication accuracy and high speed operation can be achieved at the same time..

Keywords: face authentication, high-speed, IoT device

1. Introduction

1.1 Face Authentication

A With the recent informationization, the importance of identity authentication is becoming more and more important. In the case of using ATM of a bank, even at the time of returning home, there is a case where people are authenticated, and these cases will increase in the future.

There are several methods for identity authentication, such as possessed object authentication, intellectual authentication, biometric authentication, etc. Among them, it is difficult for a person to spoof the biometric authentication that utilizes the physical features of the person. We thought that biometric authentication is the most needed in the future society. In addition, face authentication is widely recognized in biometrics authentication.

A face authentication system is a system for identifying a person from an input image. It is necessary to register and make a judgment as to whether the input face is registered or not. And the task of the face authentication system is the speed and accuracy of authentication. If making the algorithm complicated to improve accuracy, complicated calculation will be done, and as a result, the authentication speed is down. In addition, we cannot do complicated calculations with inactive devices which have less processing capability. You cannot do complicated calculations or it will take a very long time

Therefore, we tried to reduce computational complexity by simplifying algorithms and try to achieve both high speed and some degree of authentication precision even for ineffective devices.

1.2 IoT Devices

IoT is an abbreviation for Internet of Things. By connecting various other things to the Internet like a personal computer, it becomes possible to know the state of a remote thing and operate it. This idea will be able to improve our lives. The reason why attention to IoT is increasing is that the number of devices connected to the Internet is increasing.

Now the IoT devices continue to increase year by year. It is expected to exceed 50 billion units by 2020.

However, not all IoT devices are highly functional, there are many devices with poor performance such as low computing power. In such a device, it is difficult to implement a complicated algorithm for face authentication, and even if it is implemented, problems will arise in terms of speed and accuracy. Therefore, I thought that the algorithm for such ineffective devices is necessary.

As shown in Figure 1, the number of IoT devices continues to increase year by year. It is expected to exceed 50 billion by 2020.

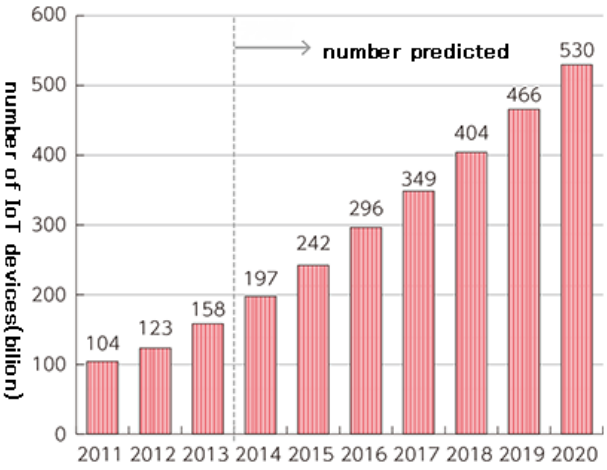


Fig. 1. Number of IoT Devices

1.3 Purpose

For the implementation on IoT devices, we develop a simple algorithm that performs face authentication only with the sign of DCT coefficients using DCT, and investigate the performance of face authentication.

Specifically, we examine how the authentication rate varies depending on the number of points of DCT coefficients we take, and how the rate changes by the points of DCT coefficients when we gradually shift from the larger amplitude to the smaller amplitude. We investigate Self-refusal rate, others acceptance rate, etc.

2. Principle

2.1 System prerequisites

As explained in the previous section, the face authentication system is one of the biometrics authentication, it is an application which can distinguish a person from the image. The face is photographed in front of the camera, and from the part considered to be face, identification is done by comparing with the information registered in advance.

As described above, the face authentication system assumes that the face is not moved so much toward the front, and cannot cope with the case where it is not directed to the front, so the same assumption is made in this system. It is not supposed to shake extremely up, down, left and right. Also, because of the nature of discrimination using only the sign of the DCT coefficients, it is difficult to discriminate too many people.

2.2 Face Detection

Face detection is a technique for determining where a face is in a given image. First of all, we get an image from the camera and convert it to grayscale. After that, face detection is performed and only the face area is cut out from the original image using the position coordinates of the face. After cutting out the face area, resize the face area of original image to a size of 128 × 128 pixels.

Fig. 2. Face Detection

2.3 DCT(Discrete Cosine Transform)

After performing face detection, DCT is performed to achieve both face recognition accuracy and speed compatibility. DCT is a method of converting a discrete signal to a frequency domain. By sampling the image and converting it to a discrete signal, performing DCT and encoding, it is possible to reduce the data capacity without damaging the majority of the original signal.

The DCT is closely related to the discrete Fourier transform. DCT is one of the separable linear transformations. Therefore, the two-dimensional transformation corresponds to executing one-dimensional DCT along one dimension and then executing one-dimensional DCT in another dimension. The definition of two-dimensional DCT for input image A and output image B is as follows.

$$B_{pq} = \alpha_{p\alpha}\alpha_q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} A_{mn} cos\frac{\pi(2m+1)p}{2M} cos\frac{\pi(2n+1)p}{2N}$$

$$0 \le p \le M-1$$

$$0 \le q \le N-1$$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases}$$

M and N are the row size and the column size of A. DCT has the feature that the converted frequency component concentrates in the low frequency region.

In face image recognition by DCT, we use the fact that the DCT coefficients are greatly different among individuals. In this study, slicing DCT coefficients with a certain threshold value, sorting in descending order of values, retrieving important information, and discarding other information as low importance. As a result, data capacity can be reduced and high-speed operation will be expected.

The image of DCT is shown in Fig.3

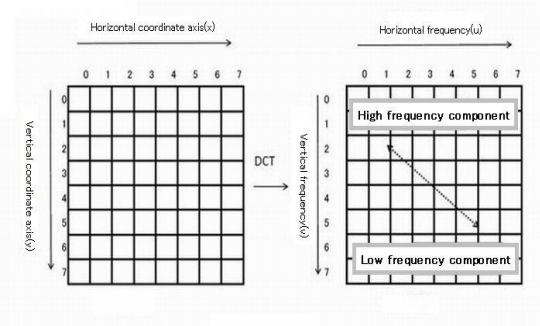


Fig. 3. Image of DCT

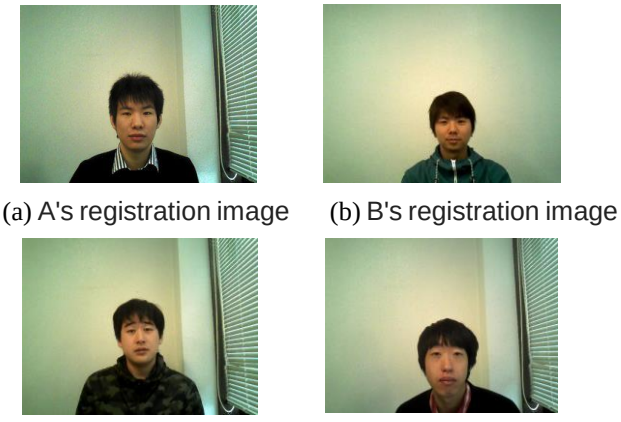
3. Experimental Method

The face image in this experiment is actually photographed with a web camera, and it is assumed that one image for registration and 100 images for authentication are input. Also, 100 images of the same person who registered and 300 images of different three people were prepared for authentication images. The input image satisfies the following conditions

- A human face exists in the image
- Color image
- A person do not face extremely sideways to the camera or face up and down
- A person is not approaching or getting too far from the camera

We developed a face authentication system that operates at high speed with the contents described in the previous section, and actually verified it. However, the size of the input image is 640 × 480 pixels, and after cutting out the face area, resize it to 128 × 128 pixels and make other input image all the same size. In addition, the DCT coefficients are examined for two patterns, a pattern to extract 64 points in the low frequency region and a pattern to extract 32 points. It is checked what percentage of the extracted points coincide with each other.

In this case, since face authentication is performed only by whether or not the plus and minus signs match, it is considered that about 50% coincidentally coincides. Therefore, it is dangerous to declare that the same person is the same even if, for example, 80% signs coincide. In this experiment, we judged that it is the same person when the signs match 90% or more. We also shifted by 5 points in descending order of the DCT coefficients, and examined how the performance of face recognition changes depending on how DCT coefficients are taken. After sorting in descending order of the DCT coefficients, experiments are performed by changing the point used for authentication such that the first to the 64th are extracted, then the sixth to the 69th are extracted. Shift of the points to be used like this is done five times. However, the image for registration has its face facing the front of the camera so that there is no change in facial expression. The image for authentication is moving the face a little or changing the expression so that only the same image will be input. The images used for registering persons A, B, C and D are shown in Fig.4.



(a) A's registration image (b) B's registration image

(c) C's registration image (d) D's registration image

Fig. 4. Each registration image

4. Results

4.1 Authentication Speed

Throughout the experiment, the authentication speed was on average of 30 milliseconds per image. Assuming that the maximum frame rate of the camera is 30 fps, it is possible to perform face authentication for almost all frames.

4.2 Authentication Rate

(1) In case taking 64 DCT coefficients

We took 64 DCT coefficients and shift the 64 points five times by 5 points. We investigated how many images are certified per 100 images.

The number of facial images authenticated per 100 is shown in Table 1.

Table 1. Number of facial images authenticated per 100(using 64 points for authentication)

Position of the point	Acceptance number of principals	Acceptance number of others
1-64	36.00	1.250
6-69	28.75	0.500
11-74	23.25	0
16-79	18.75	0
21-84	18.00	0
26-89	15.75	0

Table 2. Number of facial images authenticated per 100(using 32 points for authentication)

Position of the point	Acceptance number of principals	Acceptance number of others
1-32	54.50	19.92
6-37	43.50	13.50
11-42	38.25	7.583
16-47	32.00	2.750
21-52	26.00	1.167
26-57	25.25	0.6667

(2) In case taking 32 DCT coefficients

We took 32 DCT coefficients and shift the 32 points five times by 5 points. We investigated how many images are certified per 100 images.

The number of facial images authenticated per 100 is show in Table 2

5. Conclusion

In this Study, we performed face authentication using only the sign of DCT coefficients, and examined how the performance changes by the number of points to be taken and the position of the points to be used. As for the authentication speed, it can be said that it is sufficient speed, about 30 milliseconds per facial image. Next, regarding the authentication rate, it can be seen that it varies greatly depending on the number and order of DCT coefficients. When 64 DCT coefficients were taken, the number of certified images increased more than when 32 points were taken. And as we shift the points which we take, we can see that the number of certified images will decrease, both of person himself and others.

As a result, it was found that it is possible to distinguish only by the sign of the DCT coefficient. We thought that it is possible to realize a simple face authentication system which can work at high speed on IoT devices by using this method.

However, there are still many points that can be improved, speed and authentication rate are expected to be improved more than now, devising how to select feature value and how to calculate. For example, if the computer automatically decides how many DCT coefficients to take and which position to take by machine learning, the acceptance rate of other people will decline, and it is considered that it will be considerably evolved and will be more useful as a face authentication system. Based on the results obtained in this study, we will raise the quality of the face authentication system with a simple algorithm, but the number and the position of points best suited for authentication are not clear yet, we have to investigate it.

References

(1) Koichi Sakai: “Introduction to image processing and pattern recognition: from the basics until project creation by VC # / VC ++. NET”, pp. 101-112, 2006

(2) Hiroshi Nagahashi : “Image analysis theory(3)”, http://www.isl.titech.ac.jp/ nagahashilab/member/longb/imageanalysis/LectureNotes/ImageAnalysis03.pdf
(3) “OpenCV-1.0 Reference Manual(Japanese translation)”, http://opencv.jp/opencv-1.0.0/document/index.html