Biometric Authentication

Topics related to personal identification and verification
using features of the human body
such as fingerprints and facial images

2019-01-11

Toshiaki Saisho
Advanced IT Corporation
toshiaki.saisho@advanced-it.co.jp

Personal Profile

- **Mar. 1970 Graduated from the Department of Engineering, University of Tokyo**
- **Apr. 1970～Dec. 1994 Performed various activities at Information Systems Division of Toshiba Corporation**
  (My role) Promotion of practical use of IT in research and development in the Toshiba G companies
  Instruction and Support for engineers and researchers for advanced use of Computer, Network and various software
- **Jan. 1995～Sep. 2007 moved to Security R&D Divisions of Toshiba Corporation**
  (My role) Leading the research and development of security technology and business support activity
  Leading various research and development projects sponsored by the government
- **Sep. 2007 Retired from Toshiba Corporation**

- **Oct. 2007～ Established Advanced IT Corporation**

Current business of my company is
consulting on R&D and the business activities
based on the latest Information Technology
and Information Security Technology.

My current positions are as follows.
* President of Advanced IT Corporation
* Executive Advisor of System7 (Los Angeles)
* Advisor of ZenmuTech (Tokyo)
* Researcher of Research Institute, Chuo University

Contents of my lecture

（1）What is Biometric Authentication introductory explanation

（2）Features of Biometric Authentication
compared with other authentication methods

（3）4 major Biometric Authentication methods
fingerprint, face image, iris pattern, vein pattern

（4）Process of Biometric Authentication
process is almost the same for every method

（5）Application examples of Biometric Authentication

（5－1）Immigration Control
USA, UK, UAE, Japan

（5－2）Payment Service
operation phase and experiment phase

（1）

First part of my lecture is

“What is Biometric Authentication”

“Biometric Authentication is personal identification/verification method using human body features.”

Usually, people judge whether a person is someone they are familiar with or not, by the similarity of human body features (face images, voice features, etc.) of a familiar person.

Biometric Authentication uses almost the same method as the one that people usually use.

(1)The human body features of people who want to carry out personal identification/verification are registered beforehand

(2)The human body features of people who are going to be identified/verified are extracted

(3)The two human body features are compared

(4)judges whether the person is a someone they know or not, according to the result of that comparison

Verification steps of PC Owner by Facial Authentication are as follows.

Facial Authentication

http://www.gsd-inc.com/event/index.html

(1)PC stores owner's facial features in advance.
(2)PC gets facial features of the person sitting down in front of PC.
(3)Comparing these two facial features.
(4)Judge whether the person is owner or not based on that comparison result.

You don't need to input user-id and password!

Summary of this part is …

Biometric Authentication is a method using human body features.

Biometric Authentication uses similar methods as those usually used by people.

（2）

Second part of my lecture is

"Features of Biometric Authentication compared with other authentication methods".

 9

Three types of personal authentication methods

（1）Personal authentication by checking the information which only that person knows

➔**Personal authentication by memory**

（2）Personal authentication by the thing which only that person has

➔**Personal authentication by the thing**

（3）Personal authentication by checking the human body features which only that person has

➔**Personal authentication by the human body features**
（**Biometric Authentication**）

 10

Features of personal authentication by the memory

* Simple password memory system that is used every day
* Limits to human memory, and short passwords are used usually
  ➔So, passwords may be guessed easily.
* Many passwords will be required in daily life.
  ➔So, risk of forgetting them is high.
* To prevent forgetting the passwords, people usually take memos
  ➔New risk of memo being stolen is introduced.
* Even if passwords are stolen and abused,
  their owners don't notice it in many cases.
  ➔You must check the date and time of your last login!
  This is a very important thing to consider
  for detecting the abuse of your own password.

 11

Features of personal authentication by the thing

* Authentication by the card, the smart phone, etc. which only the person has, and also which can be identified via network
* You are also using this method in daily life.
* You must always be carrying it.
  ➔There is the risk of loss, breakage, and theft.
* There is the risk of being used by others without permission
  ➔You need to manage the thing firmly.

 12

Features of personal authentication by the human body features (Biometric Authentication)

* Forgery is difficult to make if compared with that of other systems.
* The personal authentication system, which doesn't need any memory nor any thing, can be built by biometric authentication.

  (But, it is used usually combined with other authentication methods.)
* This method sometimes requires a few times of scanning the human body feature.

  (The reason is that the scanned images are often not of good quality. So, your human body features must be scanned again.)

 13

Summary of this part is …

Biometric Authentication is
an authentication method
using human body features.

Biometric Authentication is expected
to be a reliable authentication method.

(13:15)

 14

（3）

Third part of my lecture is

“Introduction of Major Biometric Authentication Methods”

 15

Biometric Authentication methods

＊Fingerprint Authentication

Use the fact that fingerprint images and the presence / positional relationship of feature points are different for each individual

＊Facial Authentication

Use the fact that the positional relationships and shapes of facial images and facial parts are different for each individual

＊Iris Authentication

Use the fact that the iris pattern of the eyes is different for each individual

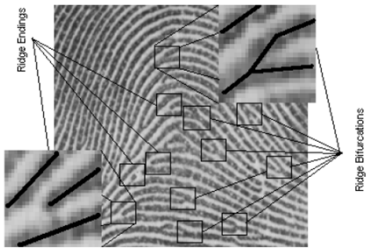
＊Vein Authentication

Use the fact that the route of the venous blood vessels (pattern of blood flow) is different for each individual

 16

Fingerprint（1）

- **Typical comparison method**
  - Typical methods use positions of the peculiar feature called "Minutiae"" in the fingerprint pattern.
  - Typical "Minutiae" are Ridge ending, Ridge bifurcation, Ridge divergence.



- **Accuracy**
  - Accuracy of fingerprint authentication is high in general.

(This is because fingerprint authentication has been used for a long time for criminal investigation purposes.)

 17

Fingerprint（2）

- **Features of usage**
  - Since an input sensor is usually a contact type, it can be miniaturized.
    - ➔ So, it can be embedded in the equipment cheaply.
  - The data of required quality may not be obtained because of the dryness of the skin, perspiration, crack, worn out, etc.

- **Places used**
  - It is used for registration of the candidate of social welfare etc. in the U.S.
  - It is being used without resistance in many situations where authentication is required.

 18

Application to owner verification for personal device

Smartphone

PC

You can use it if the matching result between the scanned fingerprint and the owner's fingerprint registered in advance is good.

 19

Application to authorization check of entering room/house

Server Room

Home

You can enter in it if the matching result between the scanned fingerprint and one of the person's fingerprint registered in advance is good.

 20

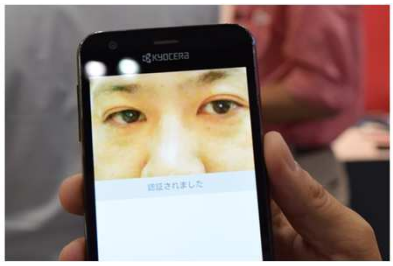
Face(1)

- Typical comparison method
  - Comparing the position of various parts of faces such as the nose and ears from the starting point such as the position of eyes and a mouth in two dimensions
  - The other comparison method compares the three-dimensional structure such as the height of a nose or the shape of a cheek using a certain measuring method
- Accuracy
  - Accuracy of facial authentication is not so high in general.
  - Matching accuracy is influenced by directions, lighting, a hairstyle, sunglass, a mask, etc.
- Features of usage
  - Seeing a face and judging who it is performed by persons usually, and therefore a user's resistance is little.

Face(2)

- Features of usage
  - Usually the face is always exposed, so facial images can be obtained and be compared without the person noticing.
- Places used for authentication
  - Used at places, such as the airport and the bank, where a lot of people go in and out
- Latest trend
  - The personal computer, the mobile phone, the tablet PC and the smart phone are equipped with the camera as standard. So, applications of facial authentication can be easily developed.

Application to owner verification for personal device



Smartphone

PC

You can use it if the matching result between the scanned face image and the owner's face image registered in advance is good.

 23

Application to authorization check when entering and leaving

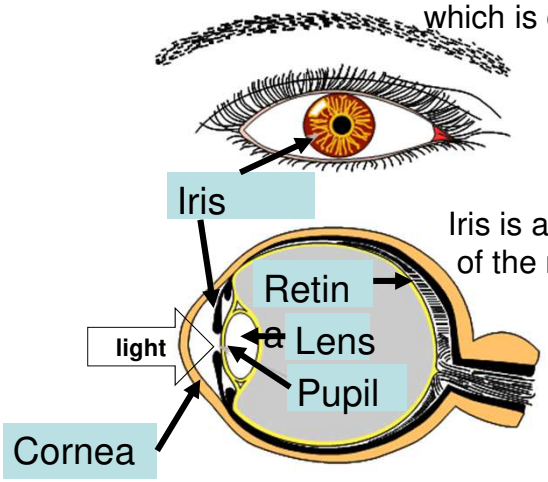
Office

Building

You can enter in it if the matching result between the scanned face image and one of the person's face image registered in advance is good.

Iris (1)

Iris pattern is this colored part which is different in each individual.



Iris is a pattern on the surface of the muscles surrounding a pupil.

The muscles surrounding a pupil help regulate the amount of light entering the eye.

 25

Iris (2)

- **Comparison method**
  - Comparing the iris patterns on the surface of the muscles surrounding a pupil
- **Accuracy**
  - Accuracy of iris authentication is high in general.
  - Iris pattern doesn't change through one's lifetime.
- **Features of usage**
  - Iris is visible from the outside and the image can be obtained without contact.

 26

Iris（3）

- **Latest trend**
  - The basic patent of iris authentication is expired.
    New iris authentication algorithms are being developed so that cheap and compact implementation is possible.
  - It is expected that not only applications such as conventional physical access security but also iris authentication will be utilized broadly from now on.

Application to owner verification for personal device

Smartphone

You can use it if the matching result between the scanned iris pattern and the owner's iris pattern registered in advance is good.

Application to authorization check when entering and leaving

Office

Mansion(Entrance)

You can enter in it if the matching result between the scanned iris pattern and one of the person's iris pattern registered in advance is good.

 29

Vein（1）

- **Mechanism of vein authentication**
  - An artery sends oxygenated hemoglobin into each bodily tissue, and supplies oxygen. A vein returns the reduced hemoglobin which lost oxygen to the heart. The patterns of the blood flow are different among individuals.
  - Reduced hemoglobin absorbs light with a wavelength of about 760 nm of a near-infrared light domain.
  - If near-infrared light is applied to a palm, only the vascular pattern of a vein will be reflected darkly.
  - The vascular pattern of a vein gives a dark reflection.

- **Accuracy**
  - High accuracy comparable with that of the fingerprint and the iris is expectable.
  - There is almost no aging influence.

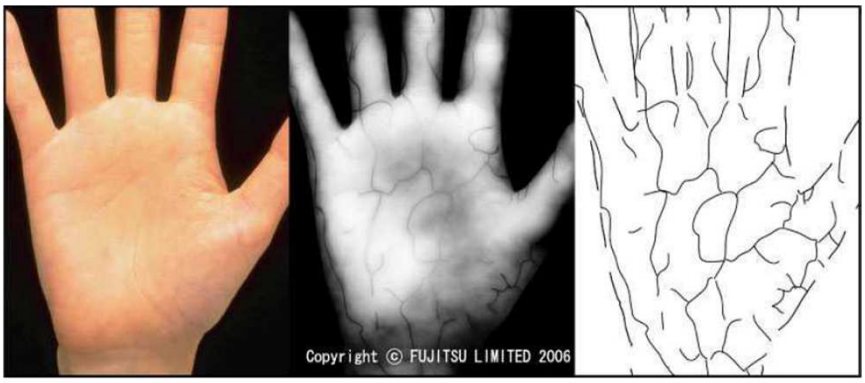
 30

Vein (2)

- **Features of usage**
  - There are few contact portions and there is almost no resistance of a user.
- **Places used**
  - ATMs with Palm vein authentication developed by Fujitsu are installed in many banks such as Mitsubishi UFJ, Hiroshima, etc.
  - ATMs with Finger vein authentication developed by Hitachi are installed in many banks such as Sumitomo Mitsui, Yucho, and Mizuho, etc.
- **Technical feature**
  - The adaptation rate is good. (There are few people that can not use the vein authentication.)
  - Compared with other biometrics, forgery is difficult.

 31

Palm vein pattern



(a) photograph of the palm by the ordinary camera

(b)photograph of the palm by the infrared camera

(c)outline and vein pattern of a palm

This vein pattern is different for each person.

 32

Application to authorization check when entering and leaving

Office
<Palm vein (F)>

出典：http://pr.fujitsu.com/jp/news/2005/08/18.html

Mansion(Entrance)
<Finger vein (H)>

出典：http://www.kaji-gl.com/security/index.html

You can enter in it if the matching result between the scanned palm/finger vein pattern and one of the person's palm/finger vein pattern registered in advance is good.

Application to account owner verification for ATM

Finger vein (H)

出典：http://www.itmedia.co.jp/mobile/articles/0410/01/news076.html

Palm vein (F)

出典：http://jbpress.ismedia.jp/articles/-/42629

You can operate the ATM if the matching result between the scanned palm/finger vein pattern and the owner's palm/finger vein pattern stored in cash card is good.

Comparison of Biometric Authentication methods

This is the example comparison table of biometric authentication.
Usually biometric authentication methods will be evaluated from various viewpoints such as accuracy, ease of use, size, cost, cleanliness, data leakage, environment, and aging.

	Fingerprint	Face image	Iris pattern	Vein pattern
Accuracy	◎	○	◎	○
Ease of use	◎	◎	○	◎
Size	◎	○	○	△
Cost	◎	○	○	△
Cleanliness	△	◎	◎	◎
Data Leakage	△	△	△	△
Forgery	○	○	◎	○
Environment	△	△	◎	◎
Aging	◎	○	◎	○

Comparative results differ according to the time of comparing the various biometric authentication products.

So, you should compare them again and you should select the most suitable biometric authentication method for your application.

 35

The summary of this part is …

- Explained 4 major Biometric Authentication methods.
- There is no method that is most suitable in all the applications.
- It is necessary to choose the optimal method in view of actual use environment, such as availability, convenience, cost / performance, and system requirements, etc.

(13:40)

 36

（4）

Fourth part of my lecture is

“Process of
Biometric Authentication”

 37

Procedure of Biometric Authentication

registration

Human body features extracted from people are registered with their names and personal information (template data)

feature extraction

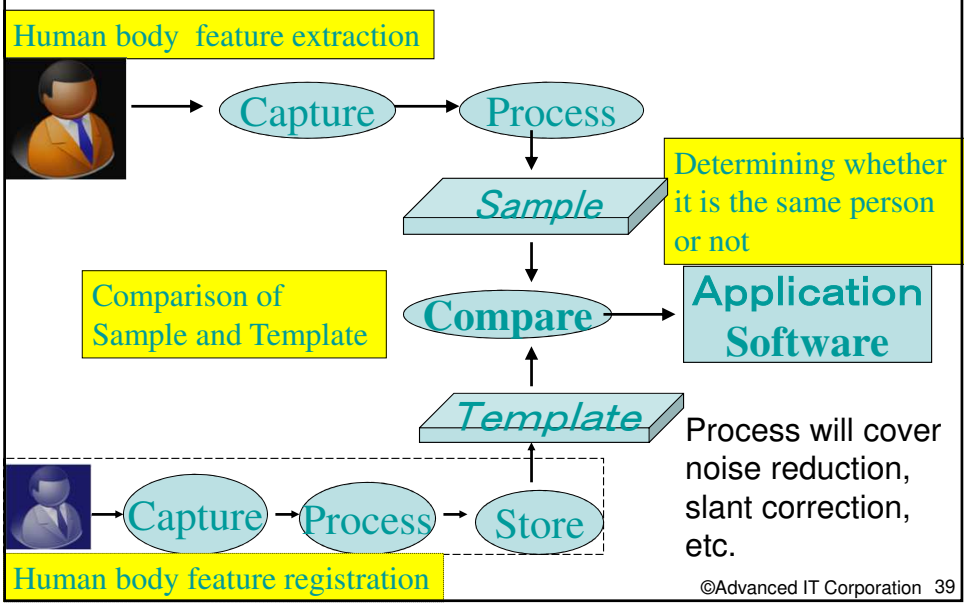
Human body features of a person who is going to be identified is extracted (sample data)

comparison and identification

By comparing the extracted feature from the person with the registered feature of all the candidate people, judge whether the person is identical with one of the people registered beforehand.

 38

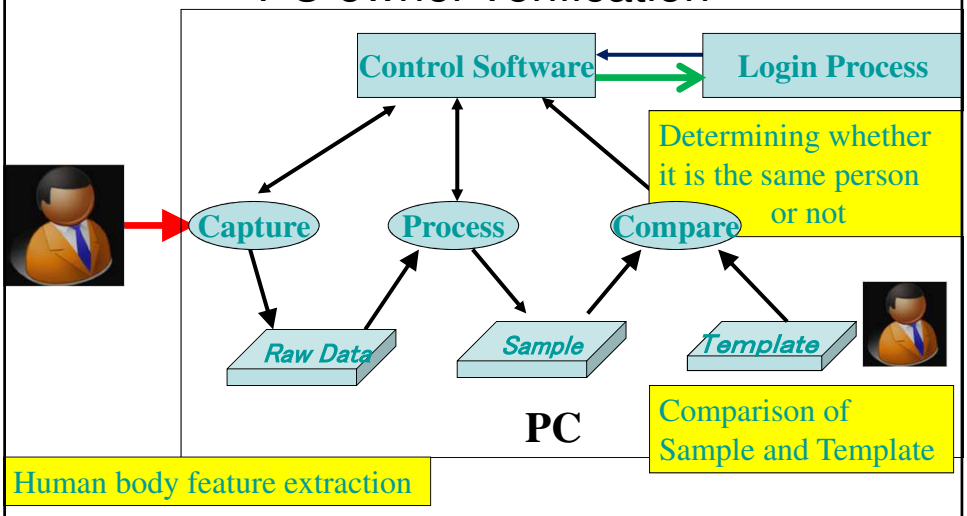
General Biometric Authentication Process



Process will cover noise reduction, slant correction, etc.

 39

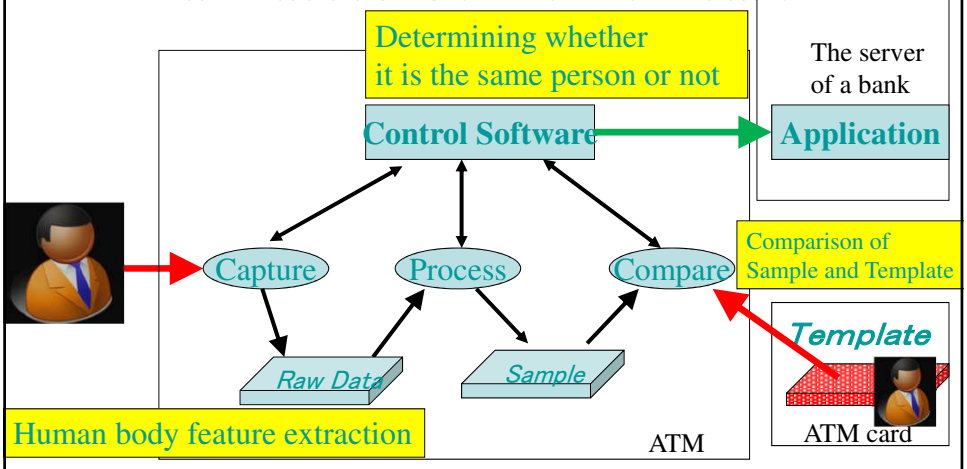
Example Biometric Authentication Process — PC owner verification —



Template of PC owner is usually stored on PC hard disc.
Only the PC owner can login this PC.

 40

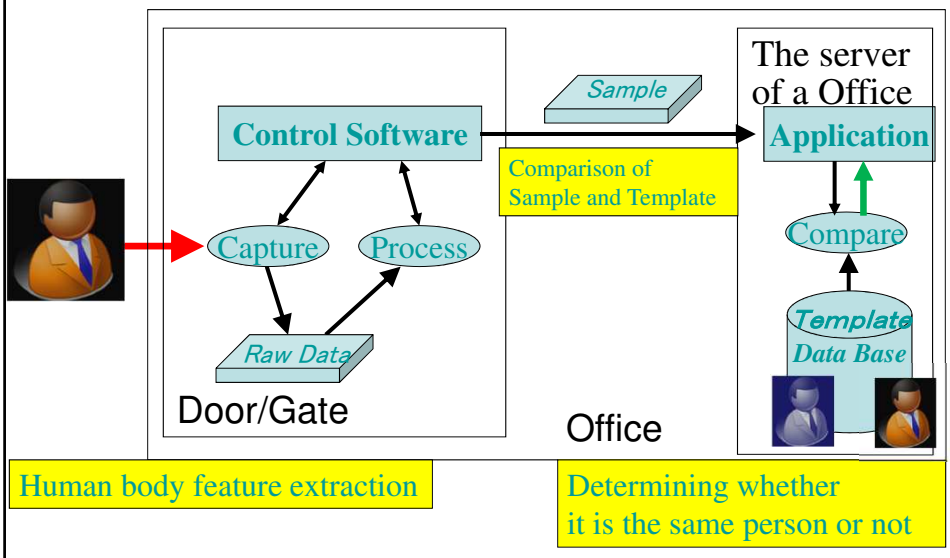
Example Biometric Authentication Process
— Bank account owner verification —



The important point of this system is that the user's template is being stored on the ATM card which the user itself is carrying. (Because template is the personal information which will pose a big problem if it leaks, the bank doesn't want to store user's template on their server.)
Only the account owner can access his own account at ATM.

 41

Example Biometric Authentication Process
— Entrance authorization verification —



Templates of registered people are usually stored on the server of office.
Only authorized person can pass the door/gate.

 42

Summary of this part is

- Although there are various biometric authentication methods, the processes are very similar. And Biometric Authentication process uses almost the same method as the one that people usually use.
- Sensor captures the human body features and processes it and stores it as the sample.
- And then, the sample will be compared with the template stored beforehand.
- And then, it judges that the person who has sample data is the same person whose human body features were extracted as the template.
- Biometric data such as template and sample should be managed carefully due to sensitive personal data. (13:50)

(5)

Fifth part of my lecture is

"Applications of Biometric Authentication"

(5-1)

Biometric Authentication applications in Immigration Control field

 45

2 major reasons(purposes) to use Biometric Authentication

（1）Enhancing Security

Prevent entry of criminals and terrorists

（2）Improving Convenience/Efficiency

Immigration procedures in a short time

➔ merit for user

Efficiency of immigration procedures

➔ merit for immigration office

Security

Biometrics in US-VISIT（USA）

US-VISIT is an immigration control system of USA.

The goals of US-VISIT are to:

Enhance the security of our citizens and visitors
Expedite legitimate travel and trade
Ensure the integrity of the immigration system
Safeguard the personal privacy of the visitors

History of biometrics in US-VISIT

Sep., 2004: (upon arrival) face image and fingerprints of both index finger

Nov., 2007: (upon arrival) face image and fingerprints of all fingers of both hand

DHS US-VISIT What to Expect When Visiting the United States(2:51)
（Automated Passport Kiosk（1:36)）

Mar., 2015: (upon departure) face image
<new biometric exit system for tracking visitors>
The purpose is tracking of Illegal stayers/terrorists and grasping the number of immigrants.

Biometrics in US-VISIT is being used to enhance security.

 47

Convenience/Efficiency

Biometrics in ePassports gate（UK）

ePassport gates are automated self-service barriers operated by the UK Border Force, offering an alternative to using desks staffed by immigration officers.

ePassport gates use facial authentication to verify the user's identity against the data stored in the chip in their biometric passport.

Citizens of the EU Member States and Iceland, Liechtenstein, Norway, Switzerland can use ePassport gates.

ePassport gates(2:00)

Biometrics in e-Passports gate is being used to improve convenience/efficiency.

 48

Security/convenience/efficiency

Biometorics in Smart Gates(UAE)

UAE(United Arab Emirates) applies iris recognition for foreigner's immigration examination from 2001 in all the 17 borders examination.

Conventional passport control procedure needs the time about 50 minutes at Dubai Airport.

New passport control service using Smart Gates needs only about 22 seconds at Dubai Airport. Only the UAE residents can use it.

SmartGate at Dubai Airport(4:44) comparing conventional system and smart gate system

Biometrics in UAE conventional immigration control is being used to enhance security.
Although biometrics in Smart Gates is being aiming at convenience/efficiency, it is as secure as conventional immigration control.

 49

Immigration control of Japan

- Since March 20, 2006, the Passport changed to a new one equipped with a microchip.
- Even if photograph of owner is replaced by other photograph, it is detected by comparing the facial image in microchip and the photograph of passport.
- But, biometric authentication is not used.

The main purpose of new passport is a measure to the forged passport with which a picture was replaced.

 50

Biometrics in automatic gate(Japan)

Two automatic gates utilizing biometrics exists in Japan.
One is fingerprint authentication gates for foreign nationals.
The other one is facial authentication gates for japanese citizens.

Security

Nov., 2009：Automatic Gate(Fingerprint)
Register forefingers of both hands in advance
Automated immigration by fingerprint verification

Automatic Gate by fingerprint is
being used to enhance security.

Convenience/Efficiency

Apr., 2018：Automatic Gate(Face image)
Automated immigration by face image verification for Japanese
(New system needs only about 10 seconds.)
Verifying by matching the face picture in the passport's IC chip
with the face image taken at the immigration screening place

Automatic Gate by face image is being expected
to improve convenience/efficiency.

 51

Summary of this part is

Biometrics authentication is being used for enhancing security and improving convenience/efficiency in immigration control.

Face image authentication, fingerprint authentication and iris pattern authentication are used in immigration control of many countries, because ICAO(International Civil Aviation Organization) selected face image(mandatory), fingerprint(optional) and iris pattern(optional) as biometric data for eMRTD(electronic machine readable travel document). (14:00)

 52

(5-2)

Biometric Authentication applications in Payment Service field

 53

Two types of Biometrics Use Case

Type A: Payment by card

which is associated with biometrics data

When biometrics authentication succeeds, payment can be made with the card associated with the registered biometrics data.

Type B: Payment by card

which is installed biometrics authentication

When biometrics authentication succeeds on the card, payment can be made by that card.

 54

Type A

Payment by fingerprint authentication

On February 9, 2015, Japanese company “Liquid” launched a fingerprint-certified credit card payment/deposit payment service "Liquid Pay”.

Registration procedure(credit card payment) :
Register fingerprint on store terminal dedicated to registration and register credit card information via application on smartphones

Payment procedure : Only fingerprint verification when purchasing items

Usecase : Payment service operated in Huis Ten Bosch from Oct 31, 2015.

In Huis Ten Bosch, "Tenbosu Currency" can be used for payment

By registering the fingerprint at the entrance and depositing the amount, payment is completed just by touching the finger at the terminal in the park.

Millions of people visit in Huis Ten Bosch, a large-scale example of unprecedented examples in the world.

 55

Type A

Omotenashi Platform Plan(Japan)

The Japanese government has been promoting the Omotenashi Platform Plan aiming the drastic increase in foreign tourists, from 25millions in 2016 to 40millions in 2020.

The government plans to achieve the target by realizing Japan where foreign tourists can enjoy sightseeing without having cash or credit card for convenience and crime prevention effect(until 2020 Olympic year).

Plan of Kanto region is to utilize fingerprint authentication.

(1)Foreign tourists register fingerprint, credit card information, and other personal information at airport.

(2)Foreign tourists can pay and tax exemption procedure only by fingerprint authentication of 2 fingers using the terminal placed in the store.

(3) Foreign tourists can substitute presentation of passport at hotel for fingerprint authentication.

Participants of this trial are about 300 souvenir shops, restaurants and hotels in Kamakura, Hakone, and Yugawara in Kanagawa prefecture, and also Atami in Shizuoka prefecture.

This is the short video about Demonstration experiment of Kanto region(3:37) 56

Type A

Payment by face authentication

On Sep. 2017, Ant Financial（Alibaba Group Company）announce
'SMILE TO PAY' FOR COMMERCIAL USE IN CHINA.
"Smile to Pay" is debuted at a KFC's new,
healthy-food concept restaurant（KPRO）in Hangzhou.
ALIPAY is a deposit type payment service.
Usually, ALIPAY uses QR code for user authentication.
"Smile to Pay" is a service that extends
the authentication of a user from QR code to face image.
Registration procedure : Register face image
on the payment service "ALIPAY".
Payment procedure : After you receive the authentication
by face authentication, then enter the mobile phone number.

This is the short video about "smile to pay" at KPRO.

In Jan. 2018, VISA announced an experimental demonstration of
payment service using face authentication at Tokyo from Feb. 2018.
NEC face authentication is used.

 57

Type A

Payment by vein authentication

On Sep. 2018, AEON Credit Service announces
experimental demonstration of the payment service
using vein authentication at convenience store "MINISTOP".
Fujitsu palm vein authentication is used.

Registration procedure : Register palm vein pattern
and bind it to AEON credit card information on Fujitsu server.
Payment procedure:
Palm vein pattern is captured at shop and transferred to Fujitsu server.
If palm vein authentication done on Fujitsu server is successful,
the credit card information is sent to AEON server
for checking whether the payment is acceptable or not.
If the payment using that credit card is acceptable,
the result is transferred to shop terminal via Fujitsu server.

 58

Type B

Fingerprint Sensor Incorporated Card

Mastercard is testing out new fingerprint sensor-enabled payment cards that, combined with the onboard chips, offer a new, convenient way to authorize your in-person transactions.

This is the introductory short video of biometric card of Mastercard.

MasterCard biometric card(1:52)

The new cards are currently being tested in South Africa, and Mastercard hopes to roll them out to the rest of the world by the end of 2017.

 59

Type B

Fingerprint Sensor Incorporated Card In Japan

On Jan. 2018, TOSHIBA annouced next generation IC card with fingerprint authentication sensor.
Major US credit cards etc. will be scheduled to adopt it in 2018.

On Apr. 2018, JCB starts experimental demonstration of payment service using non-contact IC card with fingerprint authentication（JCB Biometrics card）.
For demonstration experiments,
JCB Biometrics card is issued mainly to JCB employees from Apr. 2018.
JCB Biometrics card was developed by IDEMIA, France company.

 60

Summary of this part is

Utilization of Biometric Authentication is promoted aggressively in the world, also in Japan.

Biometric Authentication is used
for protecting service providers and
for improving safety / convenience / efficiency of service users.

(14:15)
 61

Closing Remarks

（1）Biometric Authentication is expected to become a secure and convenient authentication method.

（2）Application of Biometric Authentication is rapidly progressing in many fields.

（3）I would like everyone to continue interest in Biometric Authentication as researchers, developers, business people, or aggressive users, from now on.

 62

End

Report Theme（2019）

Following A, B and C are the explanation of three systems of the personal authentication.

There are three types of personal authentication method such as Personal authentication by memory, Personal authentication by the thing, Personal authentication by the human body feature(Biometric Authentication).

Answer the personal authentication type and the reason for each system.

A： Let the person speech the password, and then the character string extracted by speech recognition is checked against the registered password to judge whether the person in the place is the person himself or not.

B： Let the person present his IC card storing his fingerprint data, and then that fingerprint data is checked against the registered fingerprint data to judge whether the person in the place is the person himself or not.

C： Acquire iris data of the person, and then that iris data is checked against the registered iris data to judge whether the person in the place is the person himself or not.

