Biometric Authentication

Topics related to personal identification and verification
using the feature of human body such as fingerprint and facial image

2018-01-12

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

1

Personal Profile

- **Mar. 1970 Graduated from the Department of Engineering, University of Tokyo**
- **Apr. 1970～Dec. 1994 Got a job 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 softwares
- **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 company)
* Lecturer on Information Security (Hosei University)
* Special Researcher of Japan Association
for Public Human Resources Development
* 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

4

（1）

First part of my lecture is

“What is Biometric Authentication”

5

“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 image, voice feature, 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

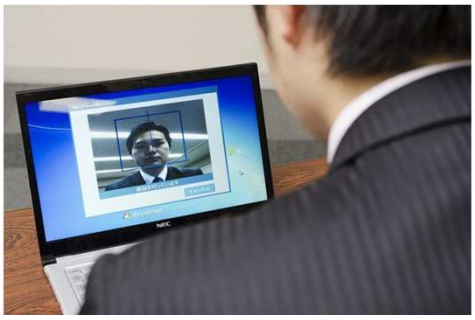
(2)the human body features of people who are going to be identified/verified are extracted

(3)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

6

Verification of PC Owner by Facial Authentication



Facial Authentication

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

(1)PC stores owner's facial feature in advance.
(2)PC gets facial feature of the person
sitting down in front of PC.
(3)Comparing 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!

7

Summary of this part is …

Biometric Authentication is
a method using
human body features.

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

（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 feature which only that person has

➔**Personal authentication by the human body feature**
（**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 check point 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
- Also you are 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 feature （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 in combination with the memory or the thing.)
* 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 feature 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.

(20m)

（3）

Third part of my lecture is

“Introduction of Major Biometric Authentication systems”

15

4 major 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**

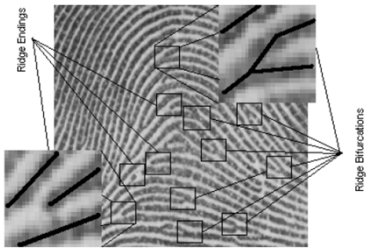
  Use the fact that the iris pattern of the eyes is different for each individual

* **Vein Authentication**

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

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.

(The reason is that 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 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.

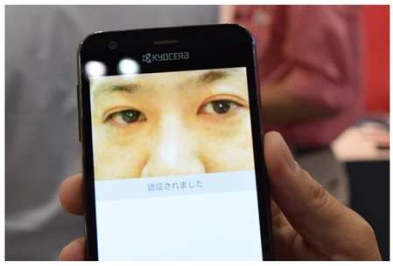
21

Face(2)

- **Features of usage**
  - Usually a face is always exposed, so face image can be obtained and can be compared even if the person does not notice it.
- **Places used for authentication**
  - Used at the 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.

22

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

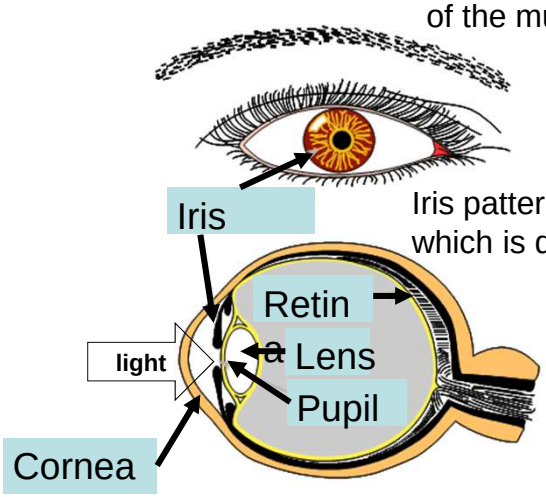
Building

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.

24

Iris（1）

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



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

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

25

Iris（2）

- **Comparison method**
  - Comparing the iris pattern on the surface of the muscles surrounding a pupil
- **Accuracy**
  - Accuracy of iris authentication is high in general.
  - Iris pattern doesn't change through 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 expired.
    New iris authentication algorithms are being developed so that cheap and compact implementation is possible.
  - It is expected that not only application with the conventional physical access security but also iris authentication will be utilized broadly from now on.

27

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.

28

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.

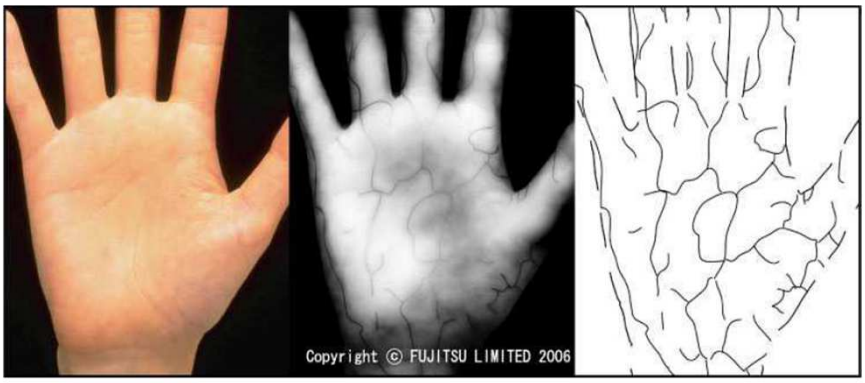
30

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>

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

Mansion(Entrance)
<Finger vein>

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.

33

Application to account owner verification for ATM

Finger vein

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

Palm vein

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.

34

Comparison of Biometric Authentication

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 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 which is most suitable in all the applications.
- It is necessary to choose the optimal system in view of actual use environment, such as availability, convenience, cost / performance, and system requirements, etc.

(50m)

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)

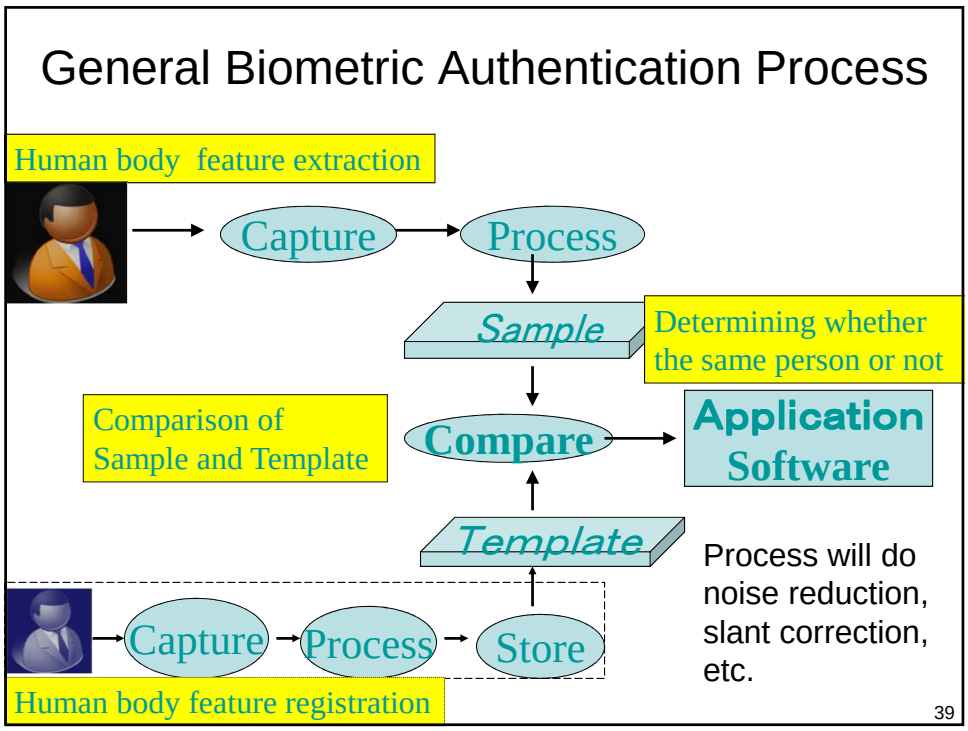
feature extraction

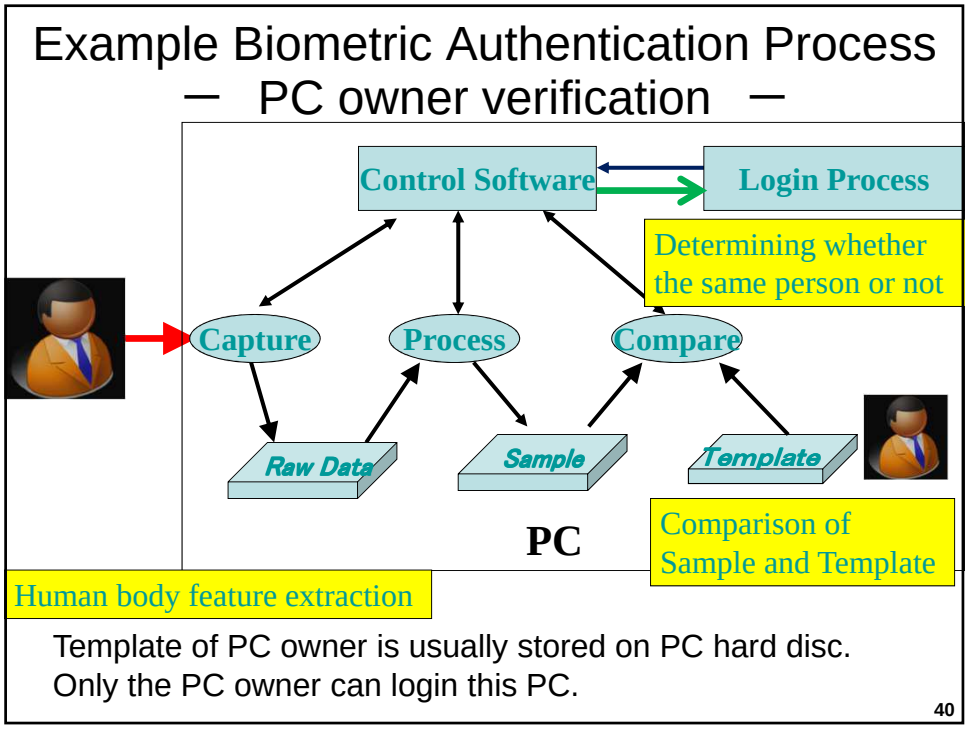
Human body features of a person who is going to be identified is extracted (sample data)

comparison and identification

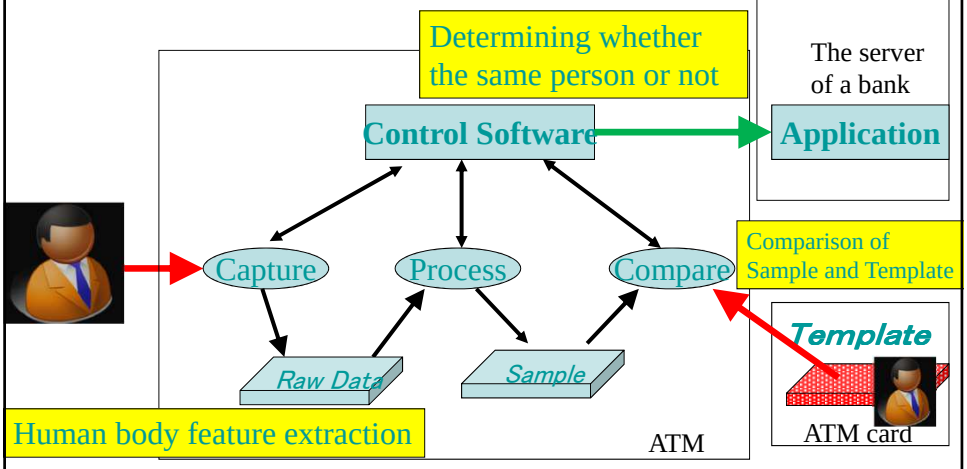
By comparing the extracted feature from the person with the registered feature of all the candidate people, judge whether the person is identical with one of the people registered beforehand.

38


General Biometric Authentication Process
Human body feature extraction
Capture
Process
Sample
Determining whether the same person or not
Comparison of Sample and Template
Compare
Application Software
Template
Process will do noise reduction, slant correction, etc.
Capture
Process
Store
Human body feature registration
39


Example Biometric Authentication Process
– PC owner verification –
Control Software
Login Process
Determining whether the same person or not
Capture
Process
Compare
Raw Data
Sample
Template
PC
Comparison of Sample and Template
Human body feature extraction
Template of PC owner is usually stored on PC hard disc.
Only the PC owner can login this PC.
40

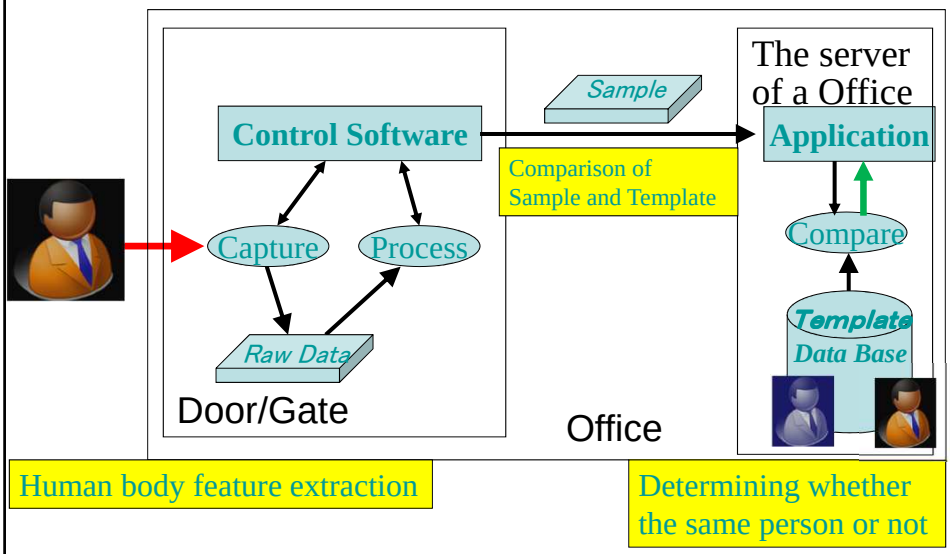
Example Biometric Authentication Process
– Bank account owner verification –



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 process is almost the same. And Biometric Authentication process uses almost the same method as the one that people usually use.
- Sensor captures the human body feature 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 feature was extracted as the template.
- Biometric data such as template and sample should be managed carefully due to sensitive personal data. (60m) 43

（5）

Fifth part of my lecture is

“Applications of Biometric Authentication”

44

(5-1)

Immigration Control

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

46

Security

Biometrics in US-VISIT（USA）

US-VISIT is an immigration control system of USA.

The goals of US-VISIT are

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 to a foreigner's immigration examination from 2001 in all the 17 border 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)

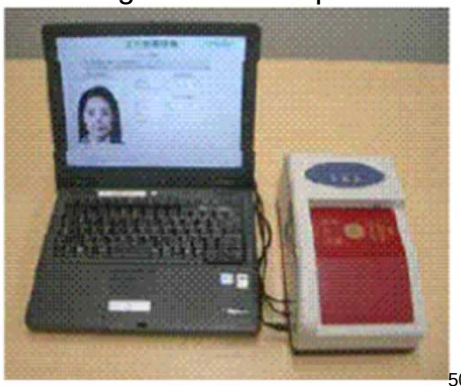
Biometrics in UAE conventional immigration control is being used to enhance security.
Although biometrics in Smart Gates is being aiming at convenience/efficiency, it is as secure as conventional immigration control.

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 already operational(fingerprint authentication).
The other one(facial authentication) will be planned to be operational next year.

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) planned
Automated immigration by face image verification for Japanese
(New system needs only about 15 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).

52

(5-2)

Payment Service

53

Payment by fingerprint authentication introduced by Liquid

On February 9, 2015, 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 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.

54

Payment by facial authentication introduced by NEC

Hiroshima Bank:

Feb.2016~Apr.2016: Demonstration experiment

Registration procedure : Register face image on company server

Payment procedure : Only face image verification when purchasing items

Hiroshima Bank intends to provide a more convenient payment environment such as introduction to regional electronic money

Sumitomo Mitsui Financial Group:

Dec.2016~Jan.2017 Demonstration experiment

Registration procedure : Register face image on company server

Payment procedure : Only face image verification when purchasing items

Sumitomo Mitsui Financial Group intends to promote use at actual stores

55

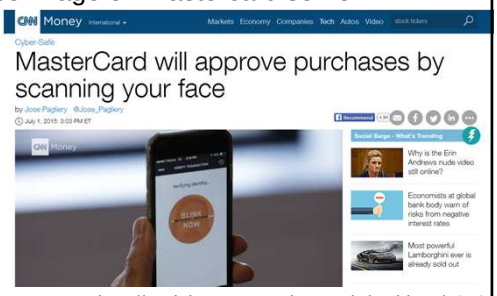
Payment by face image or fingerprint introduced by Mastercard

Jul.2015:Demonstration experiment at UK

Registration procedure : Register face image on Mastercard server

Payment procedure :

Face image captured by phone will be transferred to Mastercard who will allow card payments or money transfers.



http://ecclab.empowershop.co.jp/archives/5242

Oct.2016:Announce ‘selfie’ payment technology that uses biometrics like fingerprints or facial authentication to verify cardholder’s identity

56

Payment by Vein pattern introduced by Fujitsu/JCB

Jul.2015: Experimental demonstration

Fujitsu and Fujitsu Frontech incorporated Fujitsu's palm vein authentication technology into JCB's global payment network and built a cardless payment system.

Registration procedure : Register palm vein pattern and credit card information on Fujitsu server

Payment procedure: Palm vein pattern is captured and transferred to Fujitsu server.

And then, credit card information is selected by palm vein pattern.

Paid by that credit card which is transferred from Fujitsu server.

57

Mastercard adds fingerprint sensors to payment cards

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.

58

Omotenashi Platform Plan(Japan)

Japan government promote Omotenashi Platform Plan aiming the drastic increase of foreign tourists, from 25millions in 2016 to 40millions in 2020.

Japan government plan 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)

Japan government is promoting many projects for Omotenashi Platform Plan throughout the country.

59

Summary of this part is

Utilization of Biometric Authentication is also promoted aggressively in payment service.

Biometric Authentication is used for protecting service providers and for improving safty/cnvenience/efficiency of service users.

60

Closing Remarks

（1）Biometric Authentication is expected as 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.

61

End

62