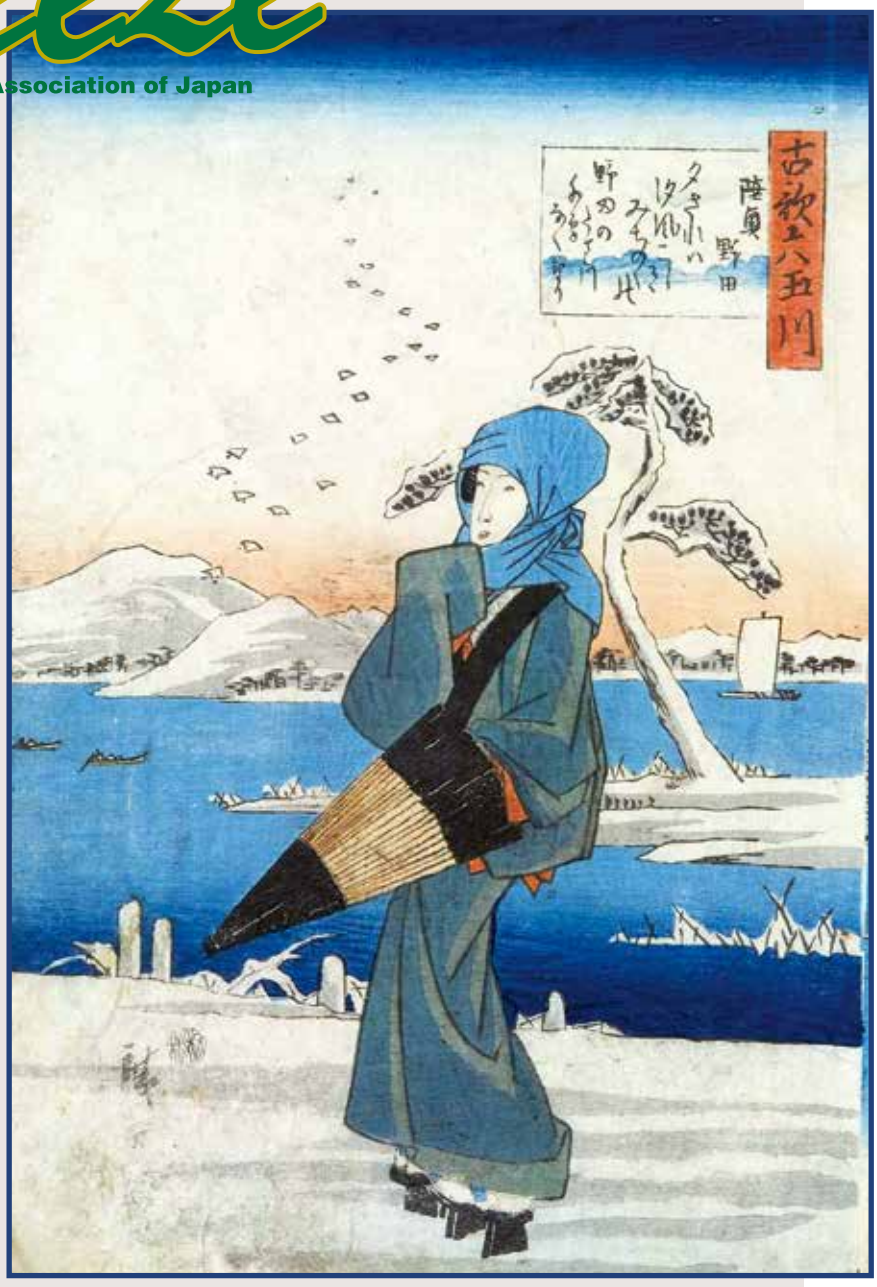
ISSN 0915-3160

平成二十九年一月十日発行（年四回一、四、七、十月の十日発行）通巻百十三号 New Breeze

New Breeze

Quarterly of the ITU Association of Japan

No. 1
Vol. 29 January 2017
Winter



New Year Messages

From the Minister for MIC, Secretary-General of ITU, President of ITU-AJ

Special Feature

Biometrics

International Standardization in JTC 1/ Palm Vein Authentication Technology/
Progress in Face Recognition Technology and International Standardization/
Utilization and Challenges of Biometrics in the Financial Sector

New Breeze ISSN 0915-3160
Quarterly of The ITU Association of Japan
BN Gyoen Bldg., 1-17-11 Shinjuku, Shinjuku-ku,
Tokyo 160-0022 Japan
Tel: +81-3-5357-7610 Fax: +81-3-3356-8170
https://www.ituaj.jp/?page_id=310

Publisher: Michiaki Ogasawara

Editors: Yuzo Mori
Kaori Ohno
Naoko Ishida

Letters to *New Breeze*

New Breeze welcomes readers' opinions. Please send comments with your name, address, and nationality by e-mail, fax, or post to the editor.

e-mail address: kikanshi@ituaj.jp

Subscription forms are available on the ITU-AJ website:
http://www.ituaj.jp/english/subscription_form.pdf

Subscription Fee:

Single issue:	¥1,500
Annual subscription (4 issues):	¥6,000

CONTENTS

About ITU-AJ

The ITU Association of Japan (ITU-AJ) was founded on September 1, 1971, to coordinate Japanese activities in the telecommunication and broadcasting sectors with international activities. Today, the principle activities of the ITU-AJ are to cooperate in various activities of international organizations such as the ITU and to disseminate information about them. The Association also aims to help developing countries by supporting technical assistance, as well as by taking part in general international cooperation, mainly through the Asia-Pacific Telecommunity (APT), so as to contribute to the advance of the telecommunications and broadcasting throughout the world.

2017 New Year Greeting from the Minister for Internal Affairs and Communications

Sanae Takaichi
Minister for Internal Affairs and Communications

Happy New Year!

In the two years and four months since I took office as the Minister for Internal Affairs and Communications, I have been working as hard as I can in various fields that are closely related to the everyday lives of Japanese people.

Thanks to the "Abenomics" policies promoted by the current government, an economic "virtuous circle" of expanding employment and increasing salaries has been set in motion. 2017 is going to be an important year with the acceleration of efforts to prepare Japan for the future by making this flow more secure.

There will be a general mobilization of the policy resources of the Ministry of Internal Affairs and Communications (MIC) so that Japanese people will really start to feel that their lives are becoming easier, and that their local communities are becoming more invigorated.

The new era of IoT, big data and AI

We are developing an integrated and comprehensive IoT promotion strategy for the forthcoming era of IoT, big data and artificial intelligence (AI), and we are taking steps to cultivate IoT skills in the workforce. We are also promoting social implementations and R&D of AI.

For social implementations, AI-related research results and data obtained by the National Institute of Information and Communications Technology (NICT) are being made available to other organizations, and we are introducing infrastructure technology to promote innovative new initiatives that make use of AI in a wide range of fields.

This research and development also incorporates the latest findings in brain science, and is accelerating the research and development of next-generation AI technology that is capable of learning at a level comparable to big data analysis, even from small amounts of data.

At G7 ICT Ministers' Meeting in Takamatsu, Kagawa last April, we proposed a set of principles for AI development that were accepted following international discussions among each of the participating countries. In March this year, we will hold an international symposium in Tokyo, at which we intend to discuss AI development guidelines embodying the content of our development principles. By working together with organizations such as G7 and OECD, we will play a central role in the embodiment and acceleration of international discussions.

We are also discussing measures to protect networks from new threats of the IoT era. To deal with the increasing damage caused by the complication and sophistication of cyber-attacks, we are making every effort to ensure that cyber security is maintained. At NICT, we have started to set up a National Cyber Training Center to provide more robust cyber-attack defense exercises and to train young security personnel.

Programming education

To cultivate logical thinking, problem-solving and creative skills that are needed in the IoT era, we are promoting model development and expansion of programming education targeted at younger age groups.

Since programming is due to become a compulsory subject in Japanese primary schools from 2020, it is essential that efforts are made to ensure the availability of sufficient teaching materials and trained instructors. At MIC, we have started hands-on training at 24 schools with the aim of building a practical model that taps into cloud-based teaching materials and local human resources.

This year, we will expand the education model across the whole of Japan, and we will develop a variety of models to cover different situations including the education needs of children with disabilities.

Toward the further spread of smartphones

Today, the smartphone is part of the everyday infrastructure of ordinary people, and reducing the communication charges incurred by smartphone users has become an important issue.

Based on previous efforts, the leading mobile phone operators have introduced new billing plans to suit light users, long-term users and heavy users.

Ministerial ordinance amendments are being made to introduce revised guidelines for shortening the SIM unlocking period and for giving assistance in purchasing terminals by early January, and for normalizing the mobile phone connection charges paid by mobile virtual network operators (MVNOs) to the major mobile phone operators by the spring of this year.

This will lead to greater competition, providing users with environments that support a greater choice of communication services and terminals, and will lead to the implementation of billing systems and services that are easier to understand and more reasonable.

I hope 2017 brings good health and happiness to all of you.

1st January, 2017

New Year Message from ITU

Houlin Zhao
Secretary-General
International Telecommunication Union

It is an honor for me to have this opportunity to greet ITU's Japanese community via the ITU Association of Japan's journal. The ITU Association of Japan (ITU-AJ) has been a key partner in enhancing and promoting ITU's work in technical standardization, radiocommunications management, and information and communication technology penetration in developing countries, helping connect the world and bringing the benefits of modern communication technologies to people everywhere.

Looking back at the events held in 2016, we find that ITU and the world took good steps towards a brighter future, but there's much more work to be done. As the United Nations specialized agency for Telecommunications and ICTs, we have been working towards ensuring that ITU's activities contribute most effectively to the achievement of the goals and objectives set by the 2030 Agenda for Sustainable Development and the UNGA Overall Review on the World Summit on the Information Society (WSIS).

In May, ITU and other UN agencies successfully organized the WSIS Forum in Geneva with a focus on the UN's 2030 Agenda for Sustainable Development. The work of WSIS in strengthening and aligning with the SDGs will be a continued focus in 2017.

I applaud the work done by the ITU-T Review Committee chaired by Mr. Maeda from Japan. The committee's work helped ITU membership call for ITU's standardization arm to expand its study of the wireline networking innovations required to achieve the ambitious performance targets of smart 5G system as an outcome of WTSA-16. ITU celebrated the 60th anniversary of CCITT/ITU-T during WTSA-2016.

The work of the ITU's Radiocommunication sector and the Radio Regulations ensure interference-free operation of radiocommunication systems and provide all countries with equitable access to the radio spectrum — a scarce natural resource that does not distinguish national borders and needs to be harmonized globally.

As we approach 2017 we also celebrate, on 12 December 2016, the 110th anniversary of the ITU Radio Regulations, the essential international treaty governing the use of the radio-frequency spectrum and satellite orbits for ubiquitous wireless communications.

The work of ITU's Telecommunication Development Sector continues to foster international cooperation in the delivery of technical assistance and in the creation, development and improvement of telecommunication and ICT networks and applications in developing markets. ITU-D successfully organized GSR-2016 and WTIS-2016. The ITU's work on the indicator index has received ever increasing recognition by the global business stakeholder.

As you are well aware, ITU Telecom World was held again in Bangkok last year. Since 2015, ITU Telecom World has taken the initiative to promote SMEs' access to the world ICT market through the event. To our great pleasure, many SMEs were actively utilizing these opportunities and bringing new waves of ideas to ITU, including a successful case of "Japan Battery Regeneration" from Japan.

In all these activities, ITU recognises the active participation of Japan, including its government, industry, academia and ITU-AJ.

In 2017, I hope ITU's members will embrace ITU's commitment to close the digital gender gap in ICT and work hard to help bring the billions of people still without access to ICTs online.

I am confident that Japan will continue to contribute actively to all of ITU's activities, and I would like to thank Japan for its continuous support of ITU ever since joining the Union in 1879.

Lastly, I take this opportunity to wish all of Japanese friends and partners, as well as your families, a peaceful and prosperous 2017.

New Year Greeting

Michiaki Ogasawara
President of The ITU Association of Japan

As one year draws to a close and a new one begins, I am reminded of the excitement that we stirred up at last year's Rio Olympics. In just three more years, it will be Tokyo's turn to host the games. The fact that it is now possible for people all over the world to watch live video of the Olympic and Paralympic games and share it in high quality is partly due to the previous standardization efforts centered around the ITU (International Telecommunication Union). Today, the ITU is also involved in discussions relating to diverse fields such as 5G and IoT that are expected to bring about significant social innovations.

In July last year, the Asia-Pacific Telecommunity (APT) held its 16th APT Policy and Regulatory Forum (PRF-16) in Tokyo. This event was attended by many high-level delegates from the Asia-Pacific region, and made a large contribution towards the sharing and resolution of telecommunication issues in this region. ITU-AJ was given the honor of taking part in the running of this event.

This year, ITU-AJ will continue looking out for important trends in the ITU and APT, and disseminating these trends to everyone through workshops, technical journals, and other such means.

Last year, WTSA-16 (World Telecommunication Standardization Assembly) was held by the ITU-T (Standardization) Sector, while in October this year WTDC-17 (World Telecommunication Development Conference) will be held in Buenos Aires (Argentina) by the ITU-D (Development) Sector. These events are important meetings leading up to next year's ITU PP-18 (Plenipotentiary Conference). This year, ITU-AJ will therefore be turning its attention to the development of information in preparation for WTDC-17 and PP-18.

Fostering skilled personnel who can play an active role in standardization and other efforts in the international arena is a major challenge for Japan. Two years ago, we commenced a "Performative Seminar", where we employed foreign actors to recreate the proceedings of international conferences in role-play exercises aimed at improving the negotiating skills of our international staff. The event was a popular hit among all the participants from our member companies. This year, we hope to come up with training scenarios that are even more useful.

Through activities such as these, ITU-AJ is helping to raise Japan's international profile while carrying out our public duties including the commendation of distinguished achievements. I hope you will be able to continue giving us your support during 2017, and that this new year brings success and happiness to each and every one of you.

Performative Seminar
13 July 2016

International Standardization in JTC 1

Asahiko Yamada
Invited Senior Researcher
Information Technology Research Institute
National Institute of Advanced Industrial Science and Technology (AIST)

1. Introduction

This paper presents an overview of international standardization activities relating to biometrics technology at ISO/IEC JTC 1 — Joint Technical Committee 1 of the ISO (International Organization for Standardization) and the International Electrotechnical Commission (IEC).

JTC 1 creates international standards relating to information technology, and currently consists of subcommittees (SCs) in 20 different fields. JTC 1 includes three SCs that work with technology related to biometrics: SC 37 (Biometrics), SC 27 (IT Security techniques), and SC 17 (Cards and personal identification). This paper introduces the organizational structure and activities of SC 37, which is concerned with biometrics itself, and also introduces the work related to biometrics technology that is being carried out by SC 17 and SC 27.

But first, here is an overview of the international standard development process in JTC 1. The development of an international standard starts with a New Work Item Proposal (NWIP). NWIPs are made by SCs or by the National Bodies (NBs) that participate in SCs. The NBs participating in JTC 1 then vote to decide whether or not to turn the NWIP into a project. When a project is established, an editor is appointed and a series of draft documents are produced: WD (Working Draft), CD (Committee Draft), DIS (Draft International Standard), and FDIS (Final Draft International Standard). At the WD stage, comments on the WD are collected from the experts participating in the WG (Working Group) subordinate to the SC, and these comments are compiled by the editor and examined at an international conference. No voting takes place at the WD stage. From the CD stage onwards, the actual deliberations are carried out by the WG, but votes are cast at the SC level in the CD stage, and at the JTC 1 level in the DIS and FDIS stages.

The Japanese organization participating in JTC 1 is the Japanese Industrial Standards Committee, which delegates its technical deliberations to the technical committee of the IPSJ/ITSCJ (Information Processing Society of Japan/Information Technology Standards Commission of Japan). Participation in each SC is the responsibility of the expert committee in ITSCJ corresponding to each SC. However, for SC 17, the expert committee is set in the Japan Business Machine and Information System Industries Association.

2. SC 37

2.1 Overview

As described below, SC 37 consists of 6 working groups WG 1 through WG 6. The host country is the United States, and the American National Standards Institute (ANSI) is appointed as the secretariat. Since the establishment of SC 37 in 2002, this subcommittee has been chaired by Fernando Podio (US) who will remain in office until 2017. In order from WG 1, the WG conveners are appointed from Australia, South Korea, Germany, the US, the UK and Italy.

There are countries represented at SC 37, comprising 28 P members (actively participants) and 13 O members (observers). Of the P members, the main participating countries in the WG (normally held in January and July) and Plenary Meeting (held in January) over the last few years have been Australia, Canada, France, Germany, Italy, Japan, South Korea, Malaysia, New Zealand, South Africa, Spain, the UK, and the US. The countries that have been actively contributing are France, Germany, Japan, the UK and the US. Contributions have also been made by Australia, Canada, South Korea and Spain.

As of October 2016, SC 37 has created and published 122 International Standards (IS), 15 Technical Reports (TR), 23 Amendments (Amd), and 20 Corrigenda. There were eleven standard publications in 2015, with two Japanese editors in two projects and four Japanese co-editors in four projects. There are 25 projects currently under development, of which one has a Japanese editor and three have four Japanese co-editors.

The national expert committee comprises a chairperson (Asahiko Yamada (National Institute of Advanced Industrial Science and Technology)), secretaries (Soichi Hama (Fujitsu Laboratories) and Mitsutoshi Himaga (Hitachi)), WG convenors of Japanese NB, and liaison representatives (with SC 17, SC 31, ISO/TC 68 and ITU-T/SG 17), and meets roughly once per month. Each WG subcommittee also meets about once per month, but as a rule, WG 4 and WG 6 hold joint meetings, while WG 1 holds its discussions by email and does not hold meetings.

In the following, the prefix ISO/IEC is omitted from the representations of standards, and only the numbers are shown.

2.2 WG 1: Harmonized Biometric Vocabulary

WG 1 (WG convenor of Japanese NB: Masanori Mizoguchi (NEC)) is standardizing biometric technical terms with the aim of harmonizing the diverse concepts used in SC 37. Their activities are centered around the creation of SD (Standing Document) 2 Harmonized Biometric Vocabulary.

Terms for which stable definitions had been obtained from SD 2 were published in 2382-37 Biometric Vocabulary in 2012. An early revised version is currently in production.

They are also making revisions to TR 24741 Biometric tutorial, which provides an overview of biometric technology.

2.3 WG 2: Biometric Technical Interfaces

WG 2 (WG convenor of Japanese NB: Takeshi Kikuchi (Hitachi Solutions)) is a group that is drawing up specifications for interfaces that share biometric information. Their activities are centered around the development of two series of common interface specifications: one is 19784 BioAPI (Biometric API) which specifies a standard application programming interface (API) for biometrics, and the other is 19785 CBEFF (Common Biometric Exchange Formats Framework) which specifies metadata formats for biometrics.

a) 19784 BioAPI series and related projects

The BioAPI series includes specifications on a hierarchical software structure comprising the following three layers:

BioAPI framework
BSP (Biometric Service Provider)
BFP (Biometric Function Provider)

The BioAPI framework is called from the application, BSP is called from the BioAPI framework, and BFP is called from BSP.

19784-1 defines the BioAPI API (the programming interface to the BioAPI framework) and the BioAPI SPI (the service provider interface to BSP). 19784-2 and subsequent standards define interfaces for BFPs such as sensors. Biometric data received by the API and SPI conform to the CBEFF data structure specified by 19785.

After the publication of 19784-1 in 2006, three amendments were published relating to GUIs and security. Japanese experts worked as editors for two of these amendments. 19784-1 and its amendments are referred to as BioAPI version 2, and the ANSI specifications upon which 19784-1 is based are referred to as BioAPI version 1. In 2010, it was agreed that the consolidation of version 2 and version 3 would be developed. Version 3 was proposed by Germany and reached the CD stage in 2015, but the editor resigned and development was put on hold. Although the consolidation of version 2 was halted, it was resumed in 2016. The development of version 3 may be resumed when the consolidation of version 2 has been completed.

The 19784 series provide specifications in the C language, but after it was argued that the specifications also need to be in object-oriented languages, progress was made in developing the 30106 series that standardize object-oriented BioAPI specifications. Part 1: Architecture, Part 2: Java implementations and Part 3: C# implementations were entered and published in 2016. A C++ version has been proposed as a NWIP for Part 4.

Standards for testing conformance to the specifications of 19784-1 have been developed in the 24709 series. Part 1 specifies test methods and test scenario description methods for BioAPI products, Part 2 specifies conformance test specifications for SPIs for BSPs, and Part 3 specifies conformance test specifications for APIs in BioAPI frameworks. Part 3 came out later than Parts 1 and 2. It was worked on by a Japanese editor, and became an international standard in 2011. Part 3 introduced an efficient new description format to the test specification of 24709. As a result, a revision was made to reflect the new description format in Part 1.

b) 19785 CBEFF series

Part 1: Data Element Specifications defines abstract data elements, and for each field of use, Part 3: Patron Format Specifications defines concrete data structures (binary format and XML format). The CBEFF data structure consists of three blocks.

SBH (Standard Biometric Header): Consists of attribute information such as data formats of biometric data put into a BDB (described below).
BDB (Biometric Data Block): The main body of the biometric data. Uses the data format of 19794, described below.
SB (Security Block): includes information for the integrity and confidentiality of SBH and BDB.

Part 1 became an international standard in 2006, followed by the other parts which are now also international standards. A Japanese editor was appointed for the SB specifications, which became an international standard as Part 4 in 2010. The ISO secretariat pointed out that the content of Part 2 — which specifies patron format registration procedures — departs from the ISO's legal policy, and for this reason Part 2 was abandoned.

2.4 WG 3: Biometric Data Interchange Formats

WG 3 (WG convenor of Japanese NB: Takashi Shinzaki (Fujitsu Laboratories)) is a group that is drawing up formats for the exchange of biometric data in order to facilitate interoperability between biometric systems. Specifically, it is involved in deliberations of the multipart 19794 (Biometric Data Interchange Formats) series of standards for each modality (i.e., biometric characteristic: fingerprint, vein, etc.), the 29794 series of related standards on biometric sample quality, and the 30107 standard on presentation attack detection (PAD).

a) Data exchange formats and related projects

1) 19794 series

The 19794 series is a multipart standard consisting of

Part 1 (which specifies a framework common to all modalities) and separate parts for each of the 13 modalities listed below:

Part 1: Framework
Part 2: Finger minutiae data
Part 3: Finger pattern spectral data
Part 4: Finger image data
Part 5: Face image data
Part 6: Iris image data
Part 7: Signature time series data
Part 8: Finger pattern skeletal data
Part 9: Vascular image data
Part 10: Hand geometry silhouette data
Part 11: Signature feature data
Part 12: (missing number)
Part 13: Voice data
Part 14: NDA data
Part 15: Palm crease image data

The first generation of formats became international standards between 2005 and 2007, and the standardization of the second generation is currently under way. Japanese experts were appointed as the editor for Part 8 and as the editor and co-editor for Part 9.

The first-generation face image format standard ISO/IEC 19794-5:2005 was adopted in ICAO e-passports, which are used by 108 countries. However, following the issue of two amendments and four corrigenda, it has continued to be difficult to refer to this standard. To improve this situation, since the plenary meeting of 2014, SC 37 has continually asserted the importance of a consolidated publication to JTC 1, and having gained the consent of SC 17/WG 3 and the ICAO relating to this standard, the decision to publish a consolidated standard was made by the ISO Technical Management Board in February 2016.

Third generation development was also started, and the specifications are being studied based on the precondition of maintaining backward compatibility with the first generation used in e-passports.

2) XML format

The conversion of each part of 19794 to XML format was developed as Amendment 2. Amendments for Part 1: Framework, Part 5: Face image data and Part 9: Vascular image data have already been published. Progress is also being made with Part 2: Finger minutiae data, Part 4: Finger image data, Part 6: Iris image data and Part 7: Signature time series data. Japanese experts have been appointed as the editor and co-editor of Part 9.

3) Conformance test methods

The conformance test standards for each part of 19794 are standardized in the 29109 series for the first generation of 19794, and in Amendment 1 of each part of 19794 for the second generation. In each case, Japanese experts have been appointed as the editor of Part 8 and as the editor and co-editor of Part 9.

b) Projects related to the quality of biometric samples

The standards in the 29794 series deal with the quality of biometric samples corresponding to each part of 19794. Four parts have been published — Part 1: Framework, Part 4: Finger image data, Part 5: Face image data and Part 6: Iris image data.

c) Presentation attack detection (PAD) project

30107 is a project for PAD technology that includes the detection of fake biometric sources. SC 37 started this project from a recognition of the need for international standards relating to PAD so that biometrics can be more widely accepted. This standard consists of three parts: Part 1 covers detection models and the classification of presentation attacks, Part 2 covers data structures for the transmission of detection results, and Part 3 covers the testing and reporting of PAD technology. Part 3 is being developed in collaboration with WG 5. Part 1 was published in January 2016, and as of October 2016, Parts 2 and 3 are at the DIS stage. Japanese experts have been appointed as the co-editor for each of these parts.

2.5 WG 4: Technical Implementation of Biometric Systems

WG 4 (WG convenor of Japanese NB: Asahiko Yamada (National Institute of Advanced Industrial Science and Technology)) is drawing up standards relating to biometric application systems.

The central standard is Part 1: Overview of 24713 series for biometric system profiles. This is applied to physical access control for employees at airports in Part 2, and to biometrics-based verification and identification of seafarers in Part 3. SC 37 has also published TR29195: Traveller processes for biometric recognition in automated border control systems, TR29196: Guidance for biometric enrolment, and TR30125: Biometrics used with mobile devices.

Projects that are currently under development include 30124 (Code of practice for the implementation of a biometric system) and 30137 (Use of biometrics in video surveillance systems) Part 1: Design and specification. Note that Part 2: Performance testing and reporting is being discussed by WG 5. Since the deliberations of this project require expertise in surveillance cameras, it is being carried out with the cooperation of an expert committee on video surveillance systems at Japan Electronics and Information Technology Industries Association (JEITA).

2.6 WG 5: Biometric Testing and Reporting

WG 5 (WG convenor of Japanese NB: Masanori Mizoguchi (NEC)) is working to standardize the testing of biometric systems

and components. Centered on the 19795 series of standards, this WG is developing standard test procedures for various types of tests at each level from technology evaluation, scenario evaluation and operational evaluation, and for each modality such as fingerprints, for certain applications such as access control applications. A Japanese expert has been appointed as the editor of TR 19795-3, which relates to testing specialized for each modality. Also, the electronics format of test reports is covered by 29120-1, for which a Japanese expert was appointed as the editor.

Japan has also been appointed as the co-editor of project 30136, which relates to performance testing of template protection schemes.

For document 30137-2 discussed in section 2.5, as in Part 1, discussions in Japanese NB are being performed with the cooperation of the JEITA expert committee.

2.7 WG 6: Cross-Jurisdictional and Societal Aspects of Biometrics

WG 6 (WG convenor of Japanese NB: Asahiko Yamada (National Institute of Advanced Industrial Science and Technology)) is performing standardization in the area of social aspects of the application of biometric technology. To improve the usability of biometrics, the 24779 series that standardizes pictograms, icons and symbols is being developed as a multi-part standard.

a) 24779 series

Part 1 sets forth policies common to all modalities, and each modality is allocated a number corresponding to the part number of 19794. Ahead of the other parts, with a Japanese editor, Part 9: Vascular applications became an international standard in 2015. Part 1: General principles, Part 4: Fingerprints and Part 5: Face images are under development.

The symbols used in each SC have to be standardized by ISO/TC 145 or IEC/TC 3, but SC 37 had not taken this action. Liaison relationship in Japan having extended the international liaison relationship with IEC/TC 3/SC 3C, the development of the 24779 series improved very much.

b) Others

TR 30110 summarizes the considerations affecting the use of biometrics by children, and was published in 2015. Following on from this, considerations affecting the use of biometrics by the elderly are currently being developed as TR20322.

3. SC 27

In SC 27, international standardization relating to biometrics technology is being performed by WG 3 (security evaluation criteria) and WG 5 (identity management and privacy technologies).

In WG 3, biometrics security evaluation became an international standard as 19792 in 2009, with a Japanese expert working as co-editor. 19792 summarizes the considerations regarding the application of security evaluation according to ISO/IEC 15408 to biometrics, and the need for more detailed security evaluations relating to false acceptance/rejection rate, vulnerability assessment and privacy issues. 19989, which is currently under development, is advancing the progress of 19792 and of the creation of an evaluation methodology to facilitate security evaluations of biometrics products based on ISO/IEC 15408. The project was established in 2014, starting with the security evaluation of PAD, but at the meeting in April 2016, the scope was extended to include performance evaluation and the project name was changed to "Criteria and methodology for security evaluation of biometric systems". Furthermore, at the meeting in October, it was split into Part 1: Framework, Part 2: Biometric recognition performance, and Part 3: PAD. A Japanese expert was appointed as the editor of Parts 1 and 3, and as the co-editor of Part 2.

In WG 5, with a Japan expert appointed as editor, 24761 (Authentication context for biometrics) became an international standard in 2009. This standard defines data structures that make it possible to judge the reliability of biometric authentication results in remote environments. At present, revisions are being made to simplify the data structures to facilitate the data validation. 24745 (Biometric information protection), which was published in 2011, summarizes the management measures and techniques for the protection of biometric information. The summarized techniques include not only encryption but also cancellable biometrics models. A project that is currently under development jointly with ITU-T is X.1085 | 17922 (Telebiometric authentication framework using BHSM (biometric hardware security module)). This defines user registration and authentication mechanisms for PKI (public key infrastructure) authentication in which the signing key is activated by biometric authentication, and is at the FDIS stage as of October 2016.

4. SC 17

7816-11 defines a PBO (Perform Biometric Operation) command for biometric processing on IC cards. A Japanese expert has been appointed as editor, and is also working to apply 24761 specified in SC 27 to PBO commands. 7816-11 is at the DIS stage as of October 2016.

Palm Vein Authentication Technology

Soichi Hama
Senior Researcher
Authentication & IoT Security Project
FUJITSU LABORATORIES LTD.

1. Introduction

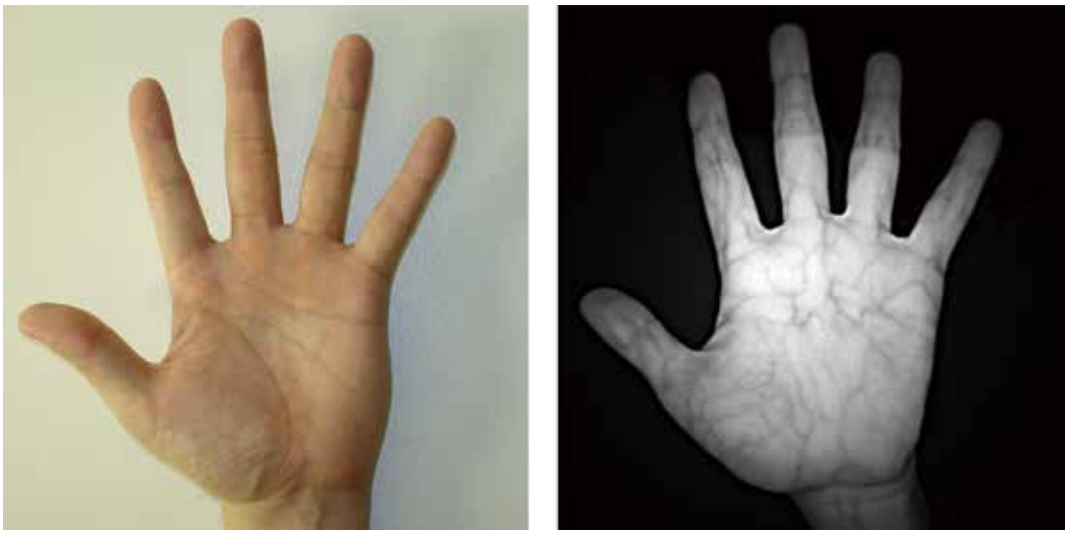
Biometrics encompasses a range of personal authentication technologies based on physical characteristics such as facial features, fingerprint, and iris; and behavioral characteristics such as voice and signature. While passwords and ID cards are a security liability if they are lost or stolen or lent to a buddy, biometric authentication is resistant to misappropriation and impersonation or spoofing. Biometric technologies are being incorporated in ever more areas as people become increasingly aware of security issues, and we anticipate a greater range of applications in the years ahead. This paper will provide a broad overview of palm vein authentication, a biometric technology whose time has come and is being more widely adopted every year.

2. Vein Authentication Technology

Vein authentication works by comparing the vascular pattern under the skin, which are unique to each individual. Since vascular patterns exist inside the body, vein authentication has a number of advantages over other biometric techniques. First, vein patterns are unaffected by environmental changes or by grime or dirt on the users' hand, and thus is perfectly stable and reliable under these conditions. Second, vascular patterns—the authentication feature—are invisible under normal visible light conditions, which makes it virtually impossible for a would-be identity thief to steal someone's authentication data without that person being aware. This second advantage is particularly important in areas requiring a high degree of authentication security. Third, vein authentication is completely contactless, which means that users are identified without actually touching the authentication device. This contactless design minimizes hygiene concerns and psychological resistance when the authentication device is used in public places by an unspecified large number of users.

Let us next consider the near-infrared technology for photographing vascular patterns. Visible light is largely absorbed by the body, so very little light penetrates beneath the skin. Mid-infrared and longer wavelength light is absorbed by H2O, and therefore it too does not penetrate the body. Intermediate between these two light sources is the near-infrared band ranging from 650 to 1000 nanometers, the so-called "biological optical window", that penetrates the body to a significant depth, and is used to photograph the vascular pattern. When the near-infrared is used to irradiate and photograph the body, light is scattered by body tissue but some of the light makes its way back to the surface and clearly reflects the tissue that it passed through. Deoxidized hemoglobin absorbs near-infrared light, which reduces the reflection rate and causes the veins to appear as a black pattern in contrast to the surrounding area. Photo 1 shows an example of a hand photographed with visible light on the left and the

Photo 1: Palm vein images (L: visible light, R: near-infrared light)



same hand photographed with a near-infrared light experimental system on the right. One can see that the vascular pattern is practically invisible under visible light, but clearly revealed under near-infrared light.

There are two types of sensors used to photograph veins, the reflection type and the transmission type. With the transmission type, the palm is positioned between the camera and the light source, and the camera captures light passing through the hand. In the reflection type, the camera and light source are in approximately the same location, and the camera captures light that is reflected off the hand. The palm vein authentication technology employs a reflection type sensor.

Essentially, vein authentication works as follows. First an image of the hand is captured using near-infrared light as described above, then the vascular pattern in the image is extracted using image processing technology, and stored as an encrypted biometric template. An individual's identity is established by photographing and extracting the user's vascular pattern as described above, then matching the pattern against the biometric template that was previously stored.

3. Vein Authentication Technology: Application Examples

We shall now briefly describe some application examples of palm vein authentication. Using palm veins has a number of advantages over other parts of the body. The palm covers a broader area than a finger, for example, so the pattern of blood vessels running through the palm is much more random. The palm is also less affected by cold weather than the fingers, which permits accurate authentication results that are largely impervious to environmental conditions. Compared to the back of the hand, it is more natural to present the palm for authentication purposes. Also, some people have hair growing on the back of their hands which blocks light and interferers with authentication. Of course, we don't have this problem with the palm so it works well for everyone.

Fujitsu began researching palm vein authentication in 2000, and launched the world's first commercial application of the technology for bank ATMs in 2004 (Photo 2). This financial solution uses palm vein authentication to identify bank customers when they withdraw money from the bank, and capitalizes on the accuracy and contactless features mentioned earlier. The product delivers exceptional accuracy with a false acceptance rate of less than 0.0008% and a false rejection rate of 0.01%.

Following the roll out of palm vein authentication bank ATMs, this form of biometric authentication has been extended to physical access control systems (Photo 3), computer login control (Photo 4), and other applications. Starting with banks, palm vein authentication is also being widely adopted in overseas markets. Particularly in developing countries where a secure infrastructure for identifying people is not yet available, there are high expectations for palm vein authentication with the various advantages described. So far more than seventy million people have had an opportunity to use palm vein authentication, and we anticipate that this number will only continue to grow in the years ahead.

Photo 3: Access control panel featuring palm vein authentication

Photo 2: ATM featuring palm vein authentication

Photo 4: Mouse with build-in palm vein authentication sensor

4. Miniaturization of Palm Vein Sensors

Since the first palm vein authentication systems were put into service, palm vein sensors have steadily shrunk to accommodate a growing number of mobile applications. Referring to Photo 5, the large unit on the right is the sensor developed for the initial bank ATM back in 2004, the square unit in the middle is the current mainline sensor, and the two smaller sensors on the right have been scaled down for mobile applications.

Let us take a closer look at some of the mobile applications that will likely adopt biometric authentication in the near future. Notebook PCs, tablet computers, and other mobile devices are now available that are as powerful both in terms of processing power and functionality as the desktop computers of just a few years ago. Laptop computers and other mobile devices have quickly emerged as a primary tool of business, so it is only natural that people are becoming increasingly concerned about the security of their mobile devices.

Mobile devices are generally carried around and used in different locations, and this makes them susceptible to loss or theft. The security of mobile devices is especially important when they are used to store personal and/or confidential information.

We observed earlier that palm vein authentication uses reflection photography. The obvious advantage of this approach over transmission photography is that the camera and the light source can be integrated, which means that the sensor can be downscaled and made much thinner. In order to implement a compact/thin palm vein sensor that can provide accurate authentication, design of the optical system is critically important. For this, Fujitsu used computer simulations to develop a specialized low-distortion wide-angle lens that provides the same angle of view as a conventional lens and a lighting component for compact/thin sensor packages. The lighting component was designed to provide a wide radiation range and very bright luminosity despite its compact implementation by carefully positioning the LED and optimizing the shape of the waveguide. The authentication algorithm was also upgraded to better match the properties of images captured by the miniature sensor.

Through these initiatives, Fujitsu developed a practical palm vein authentication sensor that is appreciably thinner and more compact than other sensors (Photo 6), and Fujitsu is now bringing

Photo 5: Miniaturization of palm vein sensor

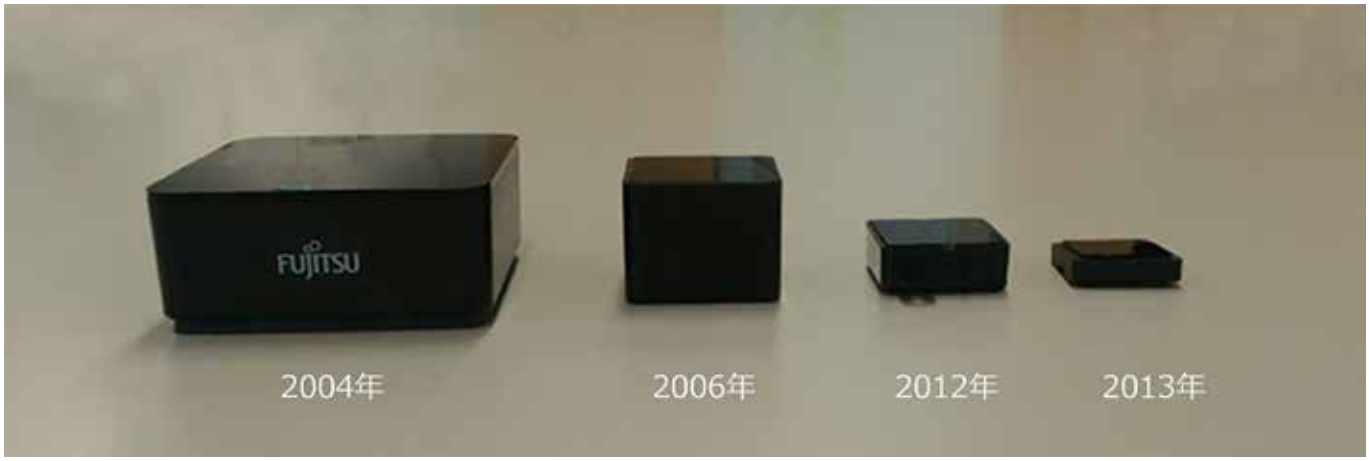


Photo 6: New compact sensors

Photo 7: Tablet computer with built-in palm vein sensor

Photo 8: Thin notebook PC with built-in palm vein sensor

mobile products to market that incorporate this sensor including a tablet computer and a slim-profile notebook PC (Photos 7 and 8). It is apparent even now that mobile devices will become increasingly important for on-site business purposes in the coming years, and the palm vein authentication technology will play a significant role in this development by safeguarding confidential and personal data through robust security. Applications using biometric authentication to identify individuals are also expected to surge when using online services for online shopping, to settle online transactions, and so on, and in this online cyber world too we can expect palm vein authentication to be widely adopted.

5. International Standardization Initiatives

International standards covering vein authentication are making headway even as research and development on this biometric technology is in progress. ISO/IEC JTC 1/SC37, which we will refer to here as Subcommittee 37 or SC37, is in charge of international standards for general biometrics. SC37 is organized into six working groups dealing with "Harmonized biometric vocabulary" (WG01), "Biometric technical interfaces" (WG02), "Biometric data interchange formats" (WG03), "Technical Implementation of Biometric Systems"(WG04), "Biometric testing and reporting" (WG05), and "Cross-Jurisdictional and Societal Aspects of Biometrics" (WG06). Focusing on applications for communications, SC37 entered into a liaison relationship with ITU-T SG17 Telebiometrics, and collaborated in drafting Recommendation / International Standard ITU-T X.1083 / ISO/IEC 24708 (Biometrics—BioAPI interworking protocol) published in 2008 that deals with interchange of biometric authentication data.

Vein authentication is a relatively new technology compared to older biometric technologies—facial recognition, fingerprints, and so on—so there wasn't much awareness of the vein authentication technology when SC37 launched. Consequently, Japanese companies took the initiative in developing vein authentication and in pushing development of international standards relating to vein authentication. For example, content pertaining to vein authentication in the 19784 Series (ISO/IEC 19784 Information technology—biometric application programming interface: BioAPI) defining standard APIs for biometric authentication applications and in 19785 Series (Information technology—Common biometric exchanges formats framework: CBEFF) defining a framework for storing biometric data clearly reflects international standards that have already been published. Moreover, standardization of data interchange formats for system interoperability includes considerable standards development work done by the author in his capacity as editor of the Vein Image Data Format Project, and was published in 2011 as International Standard, ISO/IEC 19794-9 (2011 Information technology—Biometric data interchange formats—Part 9: Vascular image data). Note that this standard is the revised second generation version of a first generation draft that was published in 2007. The second generation version adopts common headers that were harmonized to other 19794 parts which define finger, face, iris, and other modalities, and is much easier to use.

6. Future Developments

This paper presented a broad overview of palm vein authentication technology, and covered the most recent development trends and standardization activity relating to palm vein authentication. Palm vein authentication is a relatively recent biometric technology compared with fingerprint-based authentication, so there is still plenty of room for further technological progress. Fujitsu will continue to pursue multiple objectives in conducting work in this area: we will collaborate in building a large-scale social infrastructure system by continuing to improve the accuracy of sensors and systems, while at the same time continuing to reduce the size and cost of sensors. These measures will pave the way for a wider range of applications that use palm vein authentication, not just in Japan but around the globe. To take full advantage of palm vein authentication technology throughout international society, it is essential that we pay close attention to new and ongoing updating of international standards.

Progress in Face Recognition Technology and International Standardization

Shizuo Sakamoto
Technology General Manager
Second Government and Public Solution Division
NEC Corporation

1. Abstract

In the course of our everyday lives we recognize people we encounter, and respond appropriately as we go about living our lives. In recognizing people, we exploit biometrics in a direct way by observing the physical and behavioral characteristics that make us unique. Particularly in the aftermath of the coordinated terrorist attacks that occurred in the U.S. on September 11, 2001—the so-called 9/11 attacks—biometrics has taken on much greater importance in society and is rapidly being applied to passports and immigration control.

NEC has rolled out a diverse range of solutions since the company began researching and developing face recognition technology in 1989. Not only has the company continued to improve the overall face recognition accuracy of its products, NEC took the top accuracy scores in U.S. National Institute of Standards and Technology (NIST) face recognition benchmark tests in 2009, 2010, and 2013.

This paper will address international standardization of face recognition particularly as it relates to passports, provide an overview of NEC's face recognition technology, review the performance assessment results of NEC's face recognition engine by the NIST, and briefly describe an incident where the technology served to apprehend a robbery suspect.

2. Introduction

In the course of our everyday lives we recognize people we encounter, and respond appropriately as we go about living our lives. Similarly, personal authentication is exceedingly important as the entry point to various man-machine interfaces. Besides the usual standby authentication techniques of carrying an identity card or memorizing a password, biometric methods that use physical or behavioral attributes to authenticate the individual have become available, and are now becoming well established.

The coordinated terrorist attacks of September 11, 2001 on the U.S. had enormous impact on American society and on other countries around the world. Remarkably, it was found that the nineteen hijackers who perpetrated the 9/11 attacks had acquired 62 legitimate drivers licenses from state licensing authorities in the U.S., and the sudden awareness that possession of these official documents could not be relied upon to prove someone's identity immediately made biometrics much more important. The U.S., Japan, and other countries very quickly stepped up efforts to adopt biometrics to passports and immigration control. These initiatives have recently been further bolstered by a string of terrorist tragedies in Europe, long thought to be relatively safe region of the world: first the coordinated terrorist attacks in Paris on November 13, 2015 followed less than six months later by three coordinated suicide bombings in Belgium on March 22, 2016.

Biometrics is based on various physical attributes—fingerprints, iris, veins, face, etc.—or behavioral characteristics such as gait (manner of walking). Of these various methods, reliance on the face most closely approximates the way people usually recognize one another, and face recognition technology can be readily applied to all sorts of other applications besides security. Moreover, face recognition can be implemented using mug shot images taken with an ordinary camera. This sets it apart from other biometric methods that generally require a special dedicated sensor. Another advantage of face recognition is that the user is not forced to undergo any special procedure to obtain the recognition samples.

After the first ten years since beginning R&D on face recognition in 1989 until the first systems were delivered in 1999, NEC has deployed quite a wide range of solutions. Since then, we have continued to improve the matching accuracy of the recognition technology, and NEC has achieved top accuracy scores and best-in-class performance in the U.S. National Institute of Standards and Technology (NIST) benchmark tests among leading recognition vendors in 2009, 2010, and 2013.

3. International Standardization of Biometrics: Passports

Let us look back to the closing days of World War II.

The war years saw dramatic improvements in aircraft technology, and it was common knowledge that civil aviation sector would flourish in the post war era. As the wound down, the Allies gathered in Chicago in 1944 and drafted the Convention on International Civil Aviation, also known as the Chicago Convention. After the war in 1947, the International Civil Aviation Organization (ICAO) was established as a specialized agency of the UN charged with coordinating and regulating international air travel based on the Chicago Convention. The purposes of the ICAO was to foster planning and development of international air transport to ensure safe and orderly growth, to ensure international cooperation among countries to ensure international air transport services are operated in a sound and economically viable way, and today, as of March 2016, 191 nations are the members of the ICAO[1]. The ICAO has drafted many international standards and recommendations, including Document 9303 which contains ICAO specifications for machine-readable passports, visas and identity cards used

in crossing borders. The Traveller Identification Programme in the Travel Advisory Group (ICAO TAG / TRIP) is in charge of maintaining and developing Document 9303, but this group entered into a liaison relationship with *ISO/IEC JTC 1/SC17/WG3* (Subcommittee 17, Working Group 3) to undertake the technical expertise and cooperation needed to maintain and further develop the standard.

Even as detecting and preventing counterfeit passports have been largely successful, fraudulent use of genuine passports in the wrong hands to get across borders has been increasingly seen. The ICAO convened meetings to discuss this issue around the year 2000, and broad consensus was reached that biometrics-based authentication technology offered the best solution. Consensus was hastened when the 9/11 attacks occurred while these meetings were in progress, and during the Berlin meeting in June 2002 and the New Orleans meeting in March 2003, it was decided to incorporate IC chips with a contactless interface in passports, and that standardized interoperable face images shall be stored on the chips as primary biometric data. It was also decided that internationally standardized interoperable fingerprint images and iris scan images can be optionally stored on the chips as secondary biometric data.

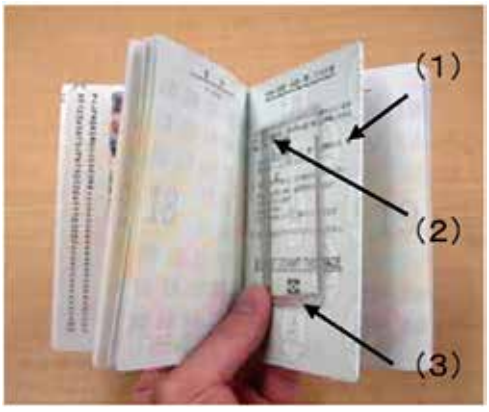
The coordinated terrorist attacks in the U.S. on September 11, 2001 led to an abrupt transformation of the structure promoting international biometric standards. Up until the attacks, ISO/IEC JTC 1 Subcommittee 17 (SC 17) with responsibility for identity card standards was just about to begin considering biometric applications for identity cards. But then the 9/11 attacks occurred, and these plans changed. The U.S. strongly urged that a new subcommittee to facilitate standards in the field of biometrics be established, and ISO/IEC JTC 1 Subcommittee 37 was inaugurated in August 2002 to take on this responsibility. Consequently, Document 9303 that provides international specifications for IC passports references specifications for biometrics developed by SC37 through the international standard ISO/IEC 7816-11 developed by SC17 in charge of IC cards and biometrics. Currently, the author is Editor of ISO/IEC 7816-11, and he has revised it to incorporate the new functions. Just recently in October 2016, the Draft International Standard ballot was taken and it was approved.

The person's face image data, biometric information recorded on the passport, is stored in the chip, as specified in Standard ISO/IEC 19794-5 developed by SC37. The face image data is stored in a container type data format called the Common Biometric Exchange Format Framework Tag-Length-Value (CBEFF TLV) patron format, as specified in ISO/IEC 19785-3, also developed by SC37.

The photo studio conditions under which face images are taken are strictly prescribed in ISO/IEC 19794-5 including the lighting, color balance, the expression and orientation of the face, size of the photo, background, and so on. These conditions not only satisfy visual confirmation needs as in the past, but also facilitate face recognition by machine. In Japan, since the face image to be recorded in the IC passport is a frontal mug shot photo supplied by the applicant, the Ministry of Foreign Affairs provides passport applicants with guidelines and easy-to-understand sample photos[2] [3].

In the case of passports issued in Japan, the face photo is printed on the first page of the passport, the IC chip is embedded in a somewhat thicker plastic-like page in the middle of the passport booklet, and the format of the mug shot image stored on the passport is compliant with the international standards as described above (see Figure 1). Before performing face recognition to match the image with the passport holder, the face image is read from the IC chip for authentication processing.

Figure 1: IC chip embedded in an IC passport
(explanatory photo of the Ministry of Foreign Affairs, http://www.mofa.go.jp/mofaj/gaiko/bluebook/2006/pdf/pdfs/4_2.pdf)



(1) Plastic card
* (2) IC chip
* (3) Communication antenna (coil)

*IC chip is invisible since it is embedded in the plastic card.

Since the Ministry of Foreign Affairs began issuing IC passports in March 2006, the passport holder can be verified by using the face image stored on the IC passport alone, and the fact that no additional procedures like other biometrics are required represents a major advantage. Since the date of expiration on passports is ten years, the change over to IC passports with recorded face images is now as of 2016 complete, enabling citizens to enjoy safe, secure, and fair public services.

Meanwhile, Australia has now adopted automated border control gate services based on face authentication not only for its own citizens but for New Zealand, U.K., U.S., and Singapore passport holders as well[4]. And the U.K. soon followed suit with a similar service for passport holders of the EU countries in the European Economic Zone, Norway, Iceland, Liechtenstein, and Switzerland[5].

Japan has also been conducting face recognition demonstration trials on its citizens at Haneda and Narita airports since the summer of 2014, so we can anticipate new user-friendly services will soon become available that also ensure greater safety and security[6].

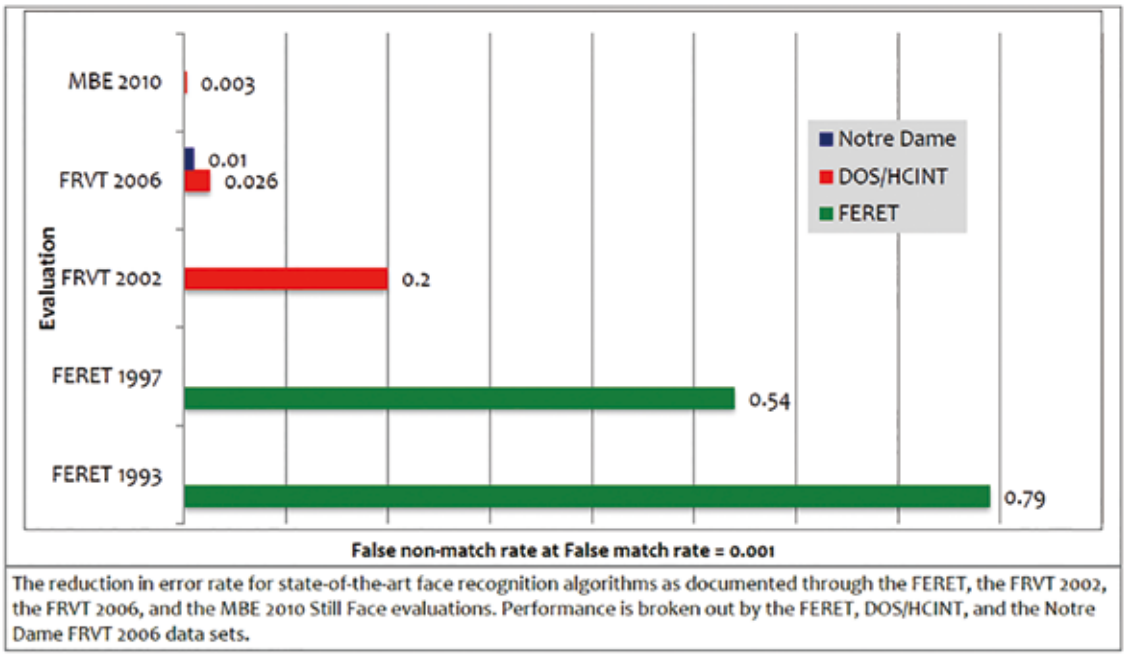
4. Progress in Face Recognition Accuracy

The coordinated September 11 terrorist attacks in the U.S. greatly spurred innovation of face recognition technology.

U.S. Congress mandated that the National Institute of Standardization and Technologies (NIST) evaluate biometrics technologies and develop standards needed to procure such technologies with the aim of securing the country against would-be terrorists. The NIST has thus taken on the role of conducting regular third-party benchmark tests to assess the accuracy of biometric fingerprint, iris, and face recognition systems. The latest recognition accuracy results regarding 1:1 matching for IC passport holder verification were released in August 2011[7], and it was reported the errors have been dramatically reduced with false acceptance rates and false rejection rates falling by two orders of magnitude from 2002 to 2010 (see Figure 2). This same report reveals that NEC's engine achieved the highest accuracy score in the 2010 benchmark tests.*

The most recent recognition accuracy results for face discrimination using a very large database were published in

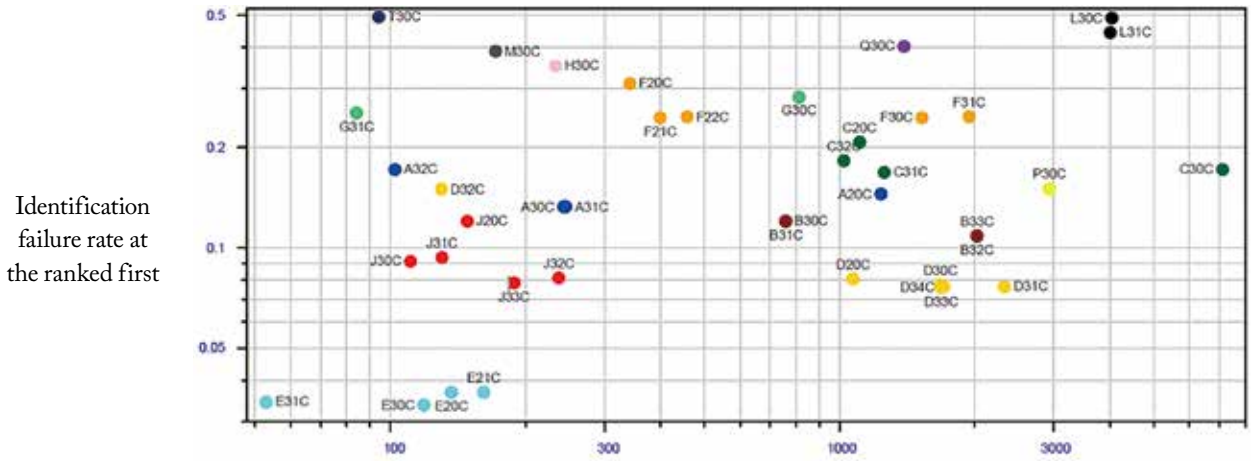
Figure 2: Progression of face recognition accuracy measurements (false non-match rate) from 1993 to 2010 (Reference[7], Figure 28)



The reduction in error rate for state-of-the-art face recognition algorithms as documented through the FERET, the FRVT 2002, the FRVT 2006, and the MBE 2010 Still Face evaluations. Performance is broken out by the FERET, DOS/HCINT, and the Notre Dame FRVT 2006 data sets.

* Results shown from NIST benchmark tests do not constitute endorsement of any particular product by the U.S. Government.

Figure 3: Face identification evaluation test results from 160,000 people (Reference [8])



May 2014 [8]. Using a database of 160,000 people, NEC's engine achieved the fastest results and the fewest errors. Match processing was completed in about 52 milliseconds with an error rate of 3.4% due to lookalike faces (see Figure 3). In other words, when 100-times searches are performed using a database of 160,000 people to select the most similar mates, 96 to 97 times out of 100 NEC's engine will succeed in selecting the right person.

Real-world performance of face recognition technology was recently demonstrated in the U.S. through the identification, arrest, and conviction of a robbery suspect [9].

The incident took place in a train on the outskirts of Chicago; a passenger was held up at gunpoint, her iPhone was stolen, and the perpetrator got away. Chicago police searched a suspect database of 4.5 million using images captured by the train's suveillance camera, and NEC's engine quickly identified a suspect that looked very similar to the perpetrator. A backup investigation revealed they had the right man, and he was arrested and convicted. The incident was reported in the U.S. as the first instance of a criminal arrest based on face recognition technology.

5. Conclusions

Although we have emphasized face recognition applications for criminal investigation and to thwart would-be terrorists in this paper, we should note that face recognition technology has an unlimited range of potential applications. For example, after the Great East Japan Earthquake in 2011, NEC's system was used for returning a photo album that was carried off in the tsunami to its rightful owner by applying face recognition to a portrait found in the album. Or consider a system that was set up at Tachibanadai Hospital for patients returning to the hospital for follow-up treatment. The system based on NEC's engine allows elderly patients to securely and easily check in at the hospital and see their doctor without the hassle and confusion of locating their patient ID cards. Face recognition clearly has enormous potential—for monitoring admission to theme parks and concerts, and countless other situations and settings—and we remain committed to further research and develop face recognition as a contribution to a safer and more secure society.

References

[1] Ministry of Foreign Affairs: International Civil Aviation Organization: http://www.mofa.go.jp/mofaj/gaiko/icao/

[2] Ministry of Foreign Affairs: Regarding photography standards for passports: http://www.mofa.go.jp/mofaj/toko/passport/ic_photo.html

[3] Ministry of Foreign Affairs: Advisory regarding photographs submitted for passports: http://www.mofa.go.jp/mofaj/files/000149961.pdf

[4] Australian Customs: SmartGatehttps://www.gov.uk/uk-border-control/at-bordercontrol

[5] U.K. Customs: Entering the UK: https://www.gov.uk/ukborder-control/at-border-control

[6] S. Sakamoto, "Face Recognition Automated Gate Trial at Haneda and Narita Airports," Information Processing Society of Japan/Information Technology Standards Commission of Japan, IPSJ/ITSCJ Newsletter, No. 104, pp. 5-8 (2014). https://www.itscj.ipsj.or.jp/hasshin_joho/hj_newsletter/NL104-w.pdf

[7] P. Grother, G. Quinn, and J. Philips, "Report on the Evaluation of 2D Still-Image Face Recognition Algorithms," NIST Interagency Report 7709 (2011). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968

[8] P. Grother and M. Ngan, "Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms," NIST Interagency Report 8009, (2014). http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf

[9] C. Farivar, "First Robber Caught via Facial Recognition," Wired online edition, June 11, 2014. Wiredhttp://wired.jp/2014/06/11/first-robber-caught-viafacial-recognition/

Utilization and Challenges of Biometrics in the Financial Sector[1]

Masashi Une
Director
Center for Information Technology Studies,
Institute for Monetary and Economic Studies
Bank of Japan

1. Recent Trend of Biometrics in the Financial Sector

Biometrics is used as a way to authenticate customers at automated teller machines (ATMs) and other services in the financial sector. A survey of financial institutions in Japan in 2015[2][3] conducted by the Center for Financial Industry Information Systems (FISC) revealed that banks and other institutions are starting to introduce biometric methods to authenticate customers at ATMs, branch counter terminals, and safe deposit boxes. In addition to finger vein pattern, palm vein pattern, and facial recognition techniques that have already been deployed, financial institutions are now considering iris scanning as a way to authenticate customers.

A growing number of Japanese financial institutions are shifting to IC cash cards at their ATMs as a way to thwart use of counterfeit magnetic stripe cash cards and prevent fraudulent withdrawals. According to a survey by the Financial Services Agency, by the end of March 2015, 16.4% of all cards issued were IC cash cards with biometric features, and 51.8% of installed ATMs are capable of using those features[4]. Most ATMs employ a finger or palm vein pattern to authenticate customers, but now a few banks are conducting trials of ATM transaction services that rely on fingerprint authentication alone and do not require a card or a Personal Identification Number[5].

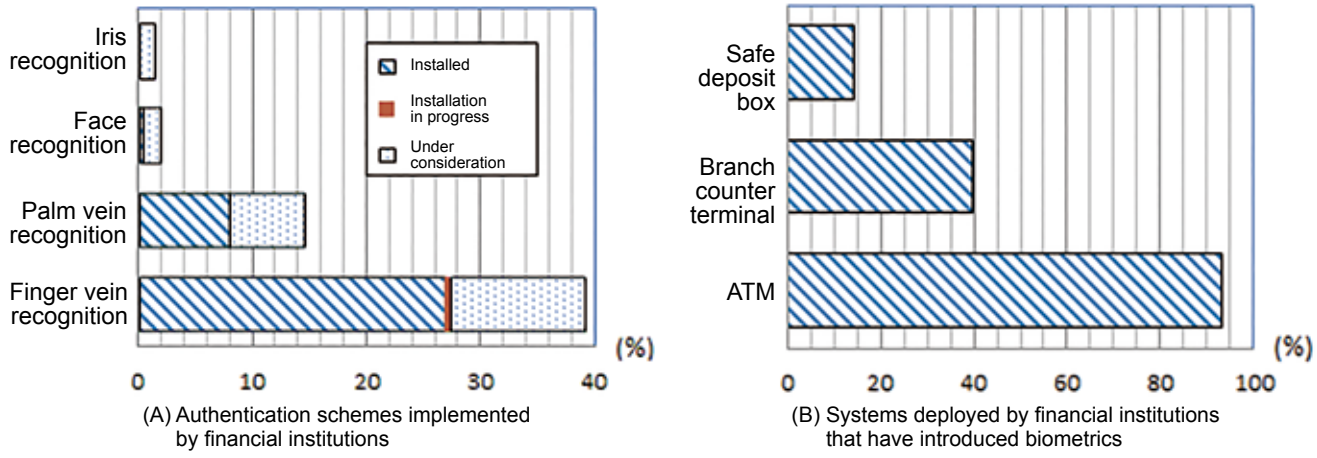
Several foreign financial institutions have adopted biometric authentication for Internet banking. For example, Bank of America introduced fingerprint authentication that enables customers to access services using a fingerprint sensor built into their smartphones in September 2015, and KEB Hana Bank followed with a similar service in February 2016. Both of these services adopted FIDO (Fast IDentity Online), which is a technical specification for implementing biometric authentication over the network[6]. In addition to smartphones, FIDO has also been incorporated in Microsoft Windows 10, and it should see widespread adoption in the future. As the result, biometric authentication may become more prevalent.

From the viewpoint of implementing biometric authentication using smartphones, a palm vein pattern captured with a smartphone's built-in camera has also been proposed for user authentication, and some financial institutions are studying the feasibility of this approach[7].

2. Necessity for Security Evaluation and the Current Situation

The primary purpose of biometric authentication is to detect and defeat malicious recognition attempts by third parties impersonating or spoofing legitimate users. When implementing a system that uses a biometric method to authenticate users (*biometric authentication system*), we have to assume that the system will be subject to a deliberate attack through impersonation or

Figure: Status of biometric deployment in Japanese financial institutions



(Figures based on Center for Japanese Financial Industry Information Systems "2015 Financial Institution Questionnaire Results")

spoofing, so it's critically important that we assess and verify in advance the probability that such an attack will succeed (*i.e., attack success probability*). If verification proves inadequate, this raises concern that the system will not be able to detect and defeat the attacks at the expected level.

In the most naïve deliberate attack, the attacker merely presents his own biometric information to impersonate a legitimate user. For this type of attack, assessment indices and methods of measuring the false accept rate (FAR) defining the attack success probability have already been standardized, so systems can be evaluated using these methods.

On the other hand, we must consider the possibility of a more sophisticated attack in which the attacker presents an artifact to the sensor that closely replicates the user's biometric information. Since the year 2000, many academic studies have shown there is a significant probability of artifacts being falsely accepted by several commercial biometric authentication systems[8]. Currently, no standardized security evaluation methods have been established for dealing with artifact attacks, so vendors of biometric authentication systems have been left to come up with their own evaluation procedures, making it virtually impossible to compare evaluation results across different systems.

3. Security Evaluation Research Trends

Recently we have seen a surge of research interest in evaluation of system security in the face of artifact attacks. In May 2015 an academic competition was held to evaluate and compare several finger vein pattern authentication schemes at the International Conference on Biometrics 2015 in Phuket, Thailand. At this competition, a forged artifact—a finger vein pattern printed on paper—was presented to vein pattern sensors; the rate of detecting the fake pattern was then calculated and compared across different schemes.

The Swiss Idiap Research Institute has been developing a finger vein pattern (image data) database. Several studies reported findings based on an artifact created from this database and used to assess some existing finger vein pattern authentication schemes.

Meanwhile, Japan has been pursuing a private-public partnership project[9] to establish a robust security evaluation method for biometric authentication systems. Launched in 2014, the three-year project is being carried out by the Japan Automatic Identification Systems Association, National Institute of Advanced Industrial Science and Technology, and OKI Software Co., Ltd. Goals of the project are to establish security evaluation methods for dealing with deliberate attacks specific to biometrics—including artifact attacks—and to promote international standards supporting third-party evaluation and certification based on standardized evaluation methods. Building on results achieved so far, the project team plans to conduct security evaluation trials using vein patterns on existing authentication systems in fiscal year 2016.

4. International Standardization Trends Relating to Security Evaluation

These recent research findings have led to activities now reflected in international standards. Case in point is the international standard ISO/IEC 30107 series addressing security evaluation methods for dealing with a presentation attack that is now being deliberated in ISO/IEC JTC1/SC37 (Biometrics). The presentation attack involves presentation of some malicious instrument or information with the goal of interfering with the operation of the biometric authentication system to be attacked, and includes artifact attacks.

Security requirements for thwarting presentation attacks are currently under deliberation in ISO/IEC JTC1/SC27 (Security) charged with drafting international standard ISO/IEC 19989. ISO/IEC19989 will be used to evaluate and certify biometric authentication systems in accordance with the Common Criteria (ISO/IEC 15408)[10]. The Common Criteria provides for *testing laboratories* with highly skilled personnel and capabilities that evaluate the security of systems and products, and for *certification bodies* that certify the appropriateness of the evaluation process. Finalization of the ISO/IEC 19989 standard is expected to further bolster evaluation and certification of biometric authentication systems by accredited third parties.

5. Advantages of Use of Standardized Security Evaluation Methods

The establishment of standardized security evaluation methods and use of evaluation and certification results by independent testing and certification bodies will have two major advantages for banks and other financial institutions:

The first advantage is improved security governance. Although the financial sector has been using biometric authentication systems for some time, the security of these systems has not been subject to evaluation by standardized methods. If such methods were available, they could be applied by financial institutions with the cooperation of their vendors to existing systems to determine (a) if countermeasures against presentation attacks are commensurate with the cost and (b) if the countermeasures actually keep security risks below an acceptable level. We would also expect that certification of the adequacy of evaluation by a certification body would appeal to customers and give them a greater confidence in security.

Another advantage of using standardized security evaluation is that this makes it possible to compare the security provided by different biometric authentication systems. Suppose a financial institution wishes to adopt biometric authentication across the board to personal computers, tablets, smartphones, and other devices. When faced with the task of choosing a new biometric authentication system from a host of contenders, naturally one wants to select the system that best satisfies specific security requirements. As it stands now, all we have to go on is the vendor's own assessment of his system's security functionalities, which does not really help in comparing evaluation results among different systems. The ability to refer to evaluation results derived by a standardized procedure not only enables financial institutions to compare the security of different systems, it also permits them to narrow down their search and to quickly identify systems that best meet their particular security requirements.

6. Future Challenges

If financial institutions are to exploit these advantages, it is important for them to consider how they might support research

into security evaluation methods and international standardization activities, and how they might utilize evaluation results based on the standardized methods.

In terms of utilizing evaluation results, consider a financial institution faced with the task of choosing a biometric authentication system that will provide a certain level of security against artifact attacks. The process of selection might involve the following steps.

(1) Gather information about all the candidate biometric authentication systems (*e.g.*, systems that have been evaluated and certified by testing laboratories and certification bodies). Be sure to verify from the vendors of the various candidate systems that they are compatible with financial application systems: ATMs, smartphones, tablets, etc.

(2) Obtain documentation used when evaluating and certifying the systems from the vendors such as the Security Target and the evidence of developer testing.

(3) Refer to the documentation obtained in the abovementioned steps, verify that each system fully satisfies the security requirements set by the financial institution: assumed threats (attackers), security policies and functionalities, security evaluation results, and so on. Systems that pass this screening are shortlisted as "candidates providing adequate security against artifact attacks." If more than one system meets this criterion, narrow the list by considering other requirements: processing performance, cost, and so on.

Practices following this protocol will highlight a number of items that should be carefully considered: (1) need to reassess operational procedures when deploying the system, (2) need to set security requirements corresponding to the standardized evaluation method, (3) need to specify information obtained from vendors, (4) need to track requests to furnish information to vendors, and so on. Sorting through these issues and figuring out how best to respond will be fundamental challenges for financial institutions as they incorporate biometric authentication systems.

Notes

[1] The views expressed in this paper are those of the author, and do not necessarily reflect the official views of the Bank of Japan. Analysis and discussion in this paper is based on the following literature: Masashi Une, "Efforts to establish security evaluation methods enabling biometric authentication systems to detect artifact attacks," *Kinyu-Kenkyu*, 35 (4), Institute for Monetary and Economic Studies, Bank of Japan, pp.55-90, 2016 (in Japanese).

[2] Center for Financial Industry Information Systems (FISC), "2015 Financial Institution Questionnaire Results," *Financial Information Systems*, No. 338, FISC, pp.1-289, Oct. 2015 (in Japanese).

[3] The questionnaire was distributed to 873 institutions including city banks, trust banks, regional banks, regional banks II, and other banks licensed under the Banking Act, Shoko Chukin Bank, Norinchukin Bank, Shinkin Banks, Shinkin Central Bank, credit unions, Shinkumi Federation Bank, Labour Banks, Credit Federations of Agricultural Cooperatives, life insurance companies, non-life insurance companies, securities companies, and credit card companies (709 institutions responded).

[4] Financial Services Agency, "Status of countermeasures dealing with counterfeit cash cards (as of the end of March 2015)," 2015 (in Japanese).

[5] In March 2016, Aeon Bank announced a trial service relying solely on a fingerprint to authenticate customers at ATMs (Aeon Bank, "Trial demonstration launch of fingerprint authentication system," March 29, 2016 (in Japanese)).

[6] Security related aspects of FIDO for Internet banking are covered in the following literature: Hidemitsu Izawa, and Hidehito Gomi, "What financial institutions should consider when deploying next-generation authentication technologies: focusing on FIDO," *Kinyu-Kenkyu*, 35 (4), Institute for Monetary and Economic Studies, Bank of Japan, pp.21-54, 2016 (in Japanese).

[7] Takashi Hara, "Vein authentication just using a smartphone camera," *Nikkei FinTech*, Nikkei Business Publications, Inc., May 25, 2016 (in Japanese).

[8] For examples of this work, refer to the following literature: Masashi Une, and Tsutomu Matsumoto, "Vulnerability of biometric authentication systems: focusing on forgery of human physical characteristics," *Kinyu-Kenkyu*, 24 (2), Institute for Monetary and Economic Studies, Bank of Japan, pp.35-83, 2005 (in Japanese).

[9] The project is referred to as: "Project to accelerate strategic international standardization: construction of an infrastructure that promotes international standardization needed to develop a biometric authentication security evaluation infrastructure contributing to cloud security."

[10] Regarding the security evaluation and certification framework in keeping with the Common Criteria standard, refer to the following paper: Yuko Tamura, and Masashi Une, "Third party evaluation and certification schemes for information security products and systems in the financial sector," *Kinyu-Kenkyu*, 27 (1), Institute for Monetary and Economic Studies, Bank of Japan, pp.79-114, 2008 (in Japanese).

Cover Art

Koka Mutamagawa Mutsu Noda
(A woman standing by a river in Tohoku region, one of six popular rivers for composing tanka poems.)

Utagawa Hiroshige (1797-1858)

Collection of the Art Research Center (ARC), Ritsumeikan University
Object number: Ebi0107

Vehicle antennas are evolving

Yoshio Aoki
Principal Research Fellow
Management Planning H.Q., Research & Development Div.
Yokowo Co., Ltd.

I belong to a company called Yokowo Co., Ltd., which recently joined the ITU Association of Japan as a supporting member. Let me take this opportunity to tell you about what we do.

Yokowo is an OEM manufacturer of electrical and electronic components. Over many years, we have built up a range of core technologies that we have used to develop products such as antennas, microwave equipment and micro-precision processing equipment. Our main strengths lie in products such as vehicle antennas, semiconductor testing connectors and probes, spring connectors for electronic equipment, and medical catheter units. Regarding vehicle antennas, we are working on antennas that cover a broad spectrum of frequencies including digital TV, GPS, satellite radio broadcasting and ETC/DSRC. In particular, we produce roof-mounted shark fin antennas (Photo 1) and micro antennas (Photo 2).

Photo1: Shark fin antenna

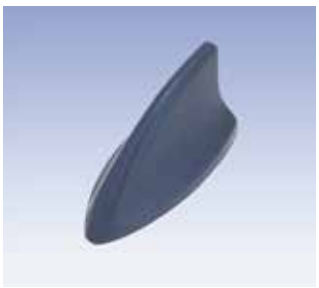
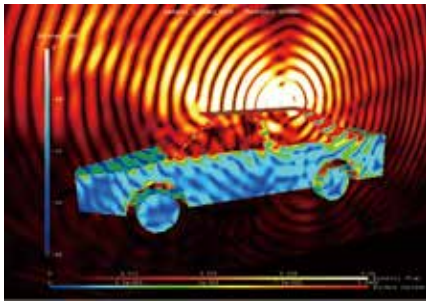


Photo2: Micro antenna

Our company was founded in 1921 by Chutaro Yokoo, who laid the foundations for worldwide growth by inventing a "spring bar" (Photo 3) using skills he had acquired in the field of precision engineering, especially the stretching and cutting of metal tubes. The structure of this spring bar has been passed down to modern-day spring connectors and semiconductor testing contact probes. Our interest in vehicle antennas dates back to 1957, when we started making car radio antennas using the same metal tube processing techniques that we had been using in rod antennas for audio and visual appliances. In 1996, we developed a micro antenna (pole type) that incorporates electronic circuitry to achieve a much shorter length than an ordinary antenna, and we transitioned from vehicle antennas based on mechanical components to antennas based on electrical components. Since then, by designing antennas based on techniques such as electromagnetic field simulations (Photo 4) and establishing mechanisms for avoiding interference between radio wave media, we developed and entered into the market for multi-frequency integrated antennas and shark fin antennas, which we are still involved with to this day.

Photo3: Spring bar

Photo4: Designing antennas based on electromagnetic field simulation



Today, vehicle antennas are about to change dramatically in order to keep up with new trends such as driverless cars, IoT, and connected cars. Cars will soon be able to drive while gathering traffic information from their surroundings by sensing, and using communication to exchange information by themselves. Vehicle antennas are no longer just passive receiving devices, but are evolving at an accelerating rate into adaptive active components while harmonizing with developments in radio communication, such as performing control adapted to the surrounding electromagnetic environment by working in conjunction with radio sensors, radars and communication equipment.

Practical applications of new media such as V2X*1 and 4G/5G*2 are also starting to find their way into automobiles. Yokowo is more involved than ever with these media standards and specifications, and is developing and providing antennas that meet all the required specifications by cooperating with car manufacturers, electronic equipment manufacturers and communication equipment manufacturers while creating optimal designs that take account of trends in the mounting positions and performance of communication equipment, and communication standards.

We recently joined the ITU Association of Japan, and, through exchanging information with other members, we will contribute to the standardization and spread of radio usage and communication standards from the viewpoint of an antenna manufacturer. I look forward to working with you in the future.

*1 V2X: Vehicle to X (X=vehicle, infrastructure, pedestrian, etc.)
*2 4G/5G: 4th/5th-generation communication systems

= A Serial Introduction Part 2= Winners of ITU-AJ Encouragement Awards 2016

In May every year, The ITU Association of Japan (ITU-AJ) proudly presents ITU-AJ Encouragement Awards to people who have made outstanding contributions in the field of international standardization and have helped in the ongoing development of ICT.
These Awards are also an embodiment of our sincere desire to encourage further contributions from these individuals in the future.
If you happen to run into these winners at another meeting in the future, please say hello to them.
But first, as part of the introductory series of Award Winners, allow us to introduce some of those remarkable winners.

Kei Kawamura
KDDI Corporation
ki-kawamura@kddi.com http://www.kddi.com/english/
Fields of activity: ITU-T Q6/SG16 (Video Coding Expert Group

Development and standardization of video coding technology

It is a great honor for me to receive the ITU-AJ Encouragement Award (ICT Field), and I would express my appreciation not only to the Selection Committee but to all who helped me along the way.

The video coding field has a particularly well known international standard called MPEG-2 that was jointly developed by ITU and ISO/IEC JTC1. More recently, a state-of-the-art standard called High Efficiency Video Coding (HEVC) was developed by the Joint Collaborative Team on Video Coding (JCT-VC), a collaboration between ITU-T Q6/SG16 (VCEG) and ISO/IEC JTC 1/SC29/WG11 (MPEG). The first edition of HEVC was published in 2013, and subsequent editions have followed up to the present.

I began to participate in JCT-VC meetings in March 2011, and have made regular technical contributions. Taking over the job of ad-hoc group co-chair and editor, I led discussions leading to and standardization of scalability extensions and multiview extensions of HEVC. Parts of these extensions must be backward compatible and interoperable with codec products already on the market. Indeed, interoperability is essential not only for standardization but also for video coding technology. Video encoding is realized by proprietary technology of each company, while the decoding process is specified in the standard since this is lossy coding technology.

The HEVC series is almost completed, and discussion has now turned to future video coding (FVC). The objective of FVC is to achieve further bandwidth reduction without sacrificing visual quality. Until HEVC standardization, double performance (50% bandwidth reduction) was regarded as a mandatory requirement. Recently, over-the-top (OTT) video services have become very popular. OTT providers bypass traditional distribution and deliver content directly via the Internet. With a 1.5 times performance gain (a 33% bandwidth reduction), this development will be welcomed by the market. Virtual reality (VR) video is another attractive use-case. VR content requires ultra-high 4K or 8K resolution (4000 pixels by 2000 pixels or 8,000 pixels by 4,000 pixels). Such high resolution video has considerable room for bandwidth reduction and is a very challenging research target.

In the development of FVC, I have been designated the co-chair of the requirements ad-hoc group in VCEG. In this capacity, I will lead discussions of future video communication services for the 5G era. Development of the new FVC standard is scheduled for completion by the end of 2020. As an expert in the field, I am committed to the development of new recommendations and standards supporting attractive new services for the general public.

Tetsuya Kawanishi
National Institute of Information and Communications Technology (NICT)
kawanishi@nict.go.jp
http://www.nict.go.jp/en/
Fields of activity:
International standardization of radio-over-fiber technologies

Toshiaki Kuri
National Institute of Information and Communications Technology (NICT)
kuri@nict.go.jp
http://www.nict.go.jp/en/
Fields of activity:
International standardization of radio-over-fiber technologies

Toward integration of wired and wireless communication technologies

We have been working at the NICT on international standardization of radio-over-fiber (RoF) technologies for more than 10 years. Our initial goal was standardization of measurement technologies necessary needed to evaluate key devices used in RoF systems in the IEC. We have made significant contributions to IEC standards for evaluating the characteristics of optical modulators and photo-detectors photodetectors for converting electrical signals into optical signals and vice versa. We also began work on system architecture standards and have helped draft technical documents supporting system integration of wired and wireless technologies in the ASTAP and the AWG. More recently in February 2013, we became involved with the ITU-T. At that time, it was thought that RoF technology could be applied to access networks, so RoF was taken up by a group charged with handling optical systems for fiber access networks (Q2/15). In February 2013, we proposed our first contribution relating to RoF technologies, potentially including analog technologies. However, most discussion of optical access networks assumes digital transmission technology, so RoF was little understood and agreement on our proposal could not be achieved. There was clearly a lack of basic understanding about RoF technology, so we proposed that we prepare some basic technical documents explaining the technology at the Q2/15 interim meeting in May 2013. This proposal was agreed upon and officially accepted as a new work item at the ITU-T SG15 plenary meeting in July 2013. The proposal and agreement went smoothly thereafter, and two years later ITU-T G-Series Recommendations Supplement 55 (G Suppl. 55) entitled "Radio-over-fibre (RoF) technologies and their applications" was formally accepted at the ITU-T SG15 plenary meeting in July, 2015. At this same meeting, it was agreed that work would commence on new standards for RoF systems, and discussion of these RoF standards now continues. Activities within ITU are clearly divided between the ITU-T handling wired communication and the ITU-R handling wireless communication. Thanks to our proposal, the ITU-T began delving into standardization of wireless communication, thus signifying a new direction unifying the fields of wired and wireless communication in the physical layer.

Confident that radio-over-fiber (RoF) technology will become increasingly important for international 5th-generation (5G) and beyond, as well as for other future radio communication systems, we will continue to contribute to standardization in this valuable field.

Ashiq Khan

NTT DOCOMO, INC.
khan@nttdocomo.com
https://www.nttdocomo.co.jp/english/corporate/technology/rd/rdcenter/
Fields of activity: Network Functions Virtualisation (NFV)

Standardization of NFV-based Telecom Networks

It is a great honor for me to receive the ITU-AJ Encouragement Award (ICT Field), and I would like to express my appreciation not only to the Selection Committee but to all who have helped me along the way.

As a network virtualization specialist, my participation in the standardization of telecom network virtualization in the ETSI Industry Specification Group Network Functions Virtualisation (ETSI ISG NFV, ETSI NFV below) began in 2013. ETSI NFV was established in November 2012 to develop a specification for virtualized telecom networks and their operation.

Within the first year, ETSI NFV evolved into a community of over 300 participants. During the first two years, we focused on defining use cases, deriving requirements, and determining the NFV architecture. Since then, we have focused on the specification of Management and Orchestration (MANO) functions, which control the operation of virtualized telecom networks. Over the next two years, implementation details and protocol-level standards will be specified. So far, ETSI NFV has delivered more than 20 Group Specifications (GSs), and more than 400 of my own contributions have been accepted.

Compared to conventional voice and data communications, services offered over telecom networks have greatly diversified, including high-definition video, Machine-to-Machine (M2M) communications, among other services. Accommodating such versatile services requires flexibility in the network. Flexibility is also required to ensure service availability during large-scale natural disasters. NFV, based on network virtualization, provides this much-desired network flexibility to network operators. Virtual Machines (VMs) can be instantiated and migrated on demand. By using Software-Defined Networking (SDN), network paths can be dynamically established and re-established to ensure that the connectivity to the VMs is maintained. Operating such a flexible network is a challenging task. ETSI NFV's role is to provide global standards for the flexible operation of a virtualized telecom network.

Another unique initiative in which I am involved is an open source community called Open Platform for NFV (OPNFV). OPNFV is responsible for developing an NFV reference platform by using only open source software. So far, we have delivered three OPNFV releases. The OPNFV Doctor project, initiated by me, has already completed its feature development in OpenStack.

As ETSI NFV will now focus on determining implementation details, using OPNFV as a reference platform for further developments will make good sense. Being committed to both of these communities, one of my future tasks will be to bring these two communities even closer together.

Shoichiro Oda

Fujitsu Limited
oda.shoichiro@jp.fujitsu.com http://www.fujitsu.com/
Fields of activity: ITU-T SG15 WP2 Q6 100G-class optical interface

Contribution to 100G-class optical interface standardization activity in ITU-T

Since November 2011, I have been involved with Question 6 (Q6) in ITU-T SG15 WP2 (Study Group 15, Working Party 2), the WP in charge of drafting an optical interface (I/F) for terrestrial optical transmission systems, and in 2012 I became the editor of Supplement 39 (G-Sup39) describing design and engineering considerations for optical transmission systems including digital coherent technology that has now been adopted as the basis for high-capacity, long-distance optical transport networks.

The most important work in addressing Question 6 involves drafting a recommendation for 100G-class optical interfaces. Ongoing deliberations began four years ago in 2012 about the time I got involved in ITU-T standardization activities, and work has continued on this recommendation up to the present. 100G optical transmission systems have adopted new and very different technologies from the current standard 10G optical systems (e.g., digital coherent technology), and this has required considerable time to verify the measured data attached to the proposed contribution. Utilizing knowledge gained while researching and developing digital coherent optical transmission systems, I am in a perfect position to facilitate smooth deliberations by pointing out defects and proposing improvements to the evaluation measurement system, and taking actions that raise questions in assessing the measurement results.

The demand for terrestrial optical transmission systems that serve as the backbone for ICT infrastructure will only continue to grow in the years ahead. The work I do in developing international recommendations and standards for high-capacity terrestrial optical interfaces is also becoming more important, and this has strengthened my commitment to continue representing Japan's perspective in developing and deploying global optical transmission infrastructure.

Satoshi Oode

NHK (Japan Broadcasting Corporation)
oode.s-hy@nhk.or.jp http://www.nhk.or.jp/strl/index-e.html
Fields of activity: ITU-R WP6B, WP6C (Audio)

Standardization of Advanced Sound Systems for Next-Generation Broadcasting Services

It is a great honor to receive the ITU Association of Japan Encouragement Award, and I would like to express my appreciation for the award and to all the people who have supported me.

Since 2014, I have taken part in meetings of ITU-R SG6 (WP6B and WP6C), and have been in charge of the standardizations for advanced sound systems including the audio-related metadata, audio file format and subjective evaluation method.

"Advanced sound systems" is a general term for next-generation audio systems beyond the 5.1-multichannel sound system. These systems include both channel-based sound systems such as the 22.2-multichannel sound system used in 8K Super Hi-Vision broadcasting and the latest object-based sound systems used in the cinema industry. Recommendation ITU-R BS.2051, which specifies loudspeaker layouts for advanced sound systems, was published in 2014, but the specifications for the renderer, an essential device to reproduce object-based sound signals, are currently under consideration. I was involved in revision of the Recommendations for advanced sound systems with priority on channel-based sound systems in time to start 4K/8K test broadcasting. The most important and highest priority issue was to revise Recommendation ITU-R BS.1770, which specifies the measurement algorithm for objective multichannel loudness.

Currently, the loudness measurement algorithm for up to 5.1-multichannel sound is widely used in the digital broadcasting services worldwide to ensure that the sound volume does not suddenly change when the broadcasting program changes. I developed an expanded algorithm with position-dependent channel weighting coefficients that remains compatible with the existing algorithm, which can calculate the loudness of any channel-based sound system. However, when Japan proposed the revision of Recommendation ITU-R BS.1770 to calculate the loudness of 22.2-multichannel sound, some countries not planning to adopt advanced sound systems were concerned that it might have an adverse effect on domestic standards while other countries promoting object-based sound systems expressed reservations about developing a new algorithm including object-based sound.

Eventually, Recommendation ITU-R BS.1770 was revised on the basis of the Japanese contributions. This was because the Recommendation provided significant technical advances and can also be attributed to savvy negotiations. It is important to form strong relationships with fellow overseas associates with whom one can negotiate favorable conditions in international standards. In my capacity as Chairman of the Drafting Group and Rapporteur Group, I gained the trust of many close associates who supported the revision in negotiations. I remain committed to standardization work, and will continue to make contributions supporting implementation of advanced sound systems for next-generation broadcasting services.

New Breeze
平成二十九年一月十日発行（年四回一、四、七、十月の十日発行）第二十九巻第一号（通巻百十三号）

The ITU Association of Japan

定価　一冊　一、六二〇円（本体価格　一、五〇〇円、消費税　一二〇円）　年間購読料　六、四八〇円（本体価格　六、〇〇〇円、消費税　四八〇円）