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.

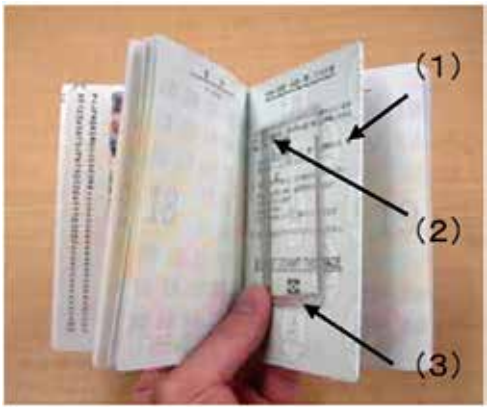
The coordinated terrorist attacks in the U.S. on September 11, 2001 led to an abrupt transformation of the structure promoting international biometric standards. Up until the attacks, ISO/IEC JTC 1 Subcommittee 17 (SC 17) with responsibility for identity card standards was just about to begin considering 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].

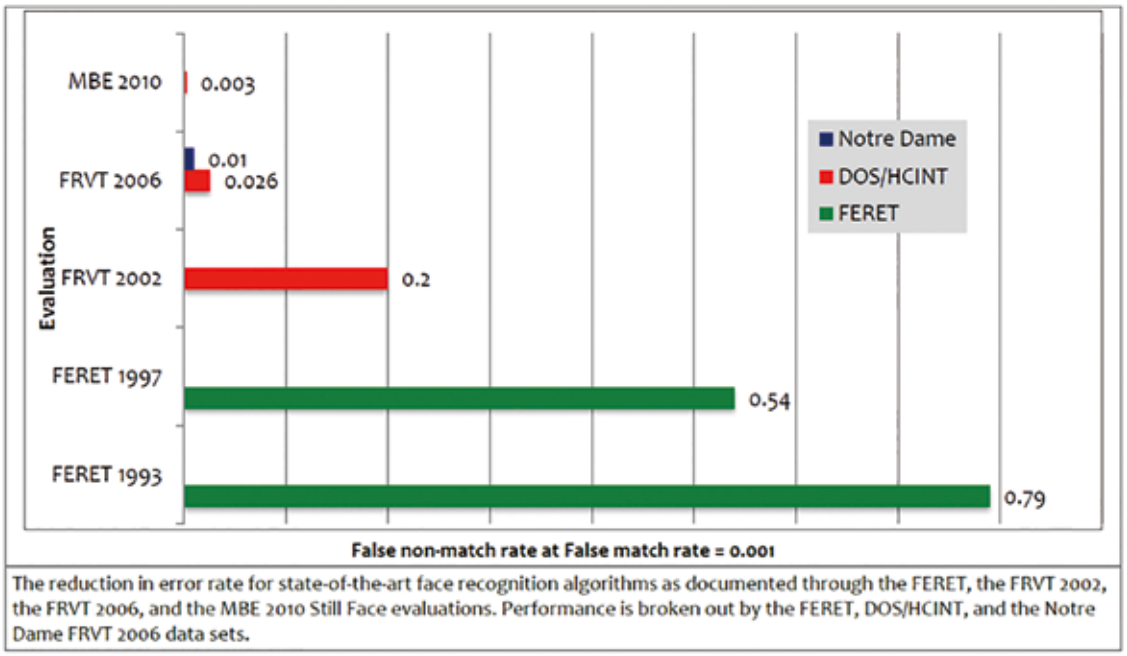
4. Progress in Face Recognition Accuracy

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

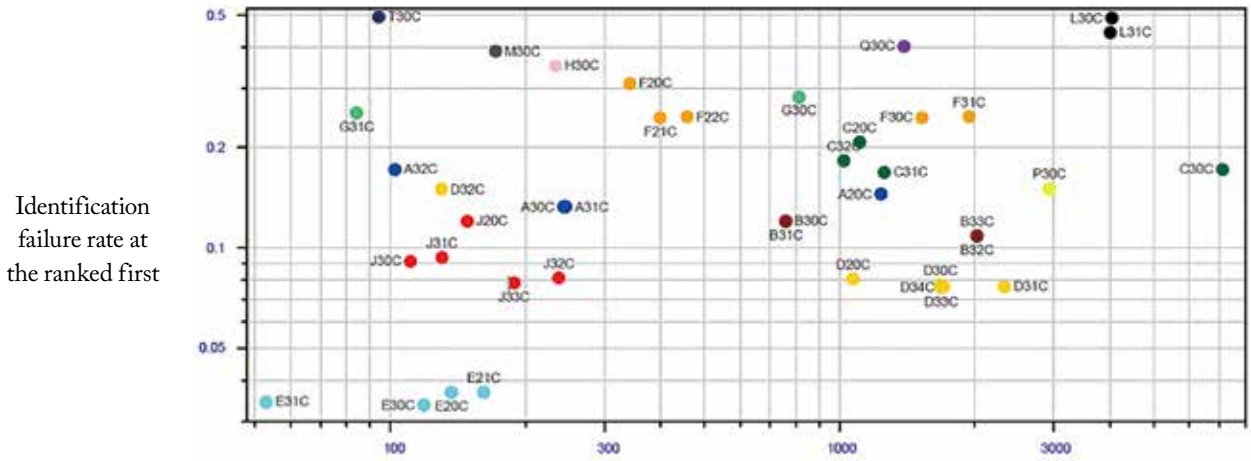
Figure 2: Progression of face recognition accuracy measurements (false non-match rate) from 1993 to 2010 (Reference[7], Figure 28)



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/