Paper on Consumer Systems

Identity Verification of Ticket Holders at Large-scale Events Using Face Recognition

Akitoshi Okumura[1,a)] Takamichi Hoshino[1] Susumu Handa[1] Yugo Nishiyama[1]
Masahiro Tabuchi[1]

Received: September 30, 2016, Accepted: February 27, 2017

Abstract: This paper proposes a system of verifying the identity of ticket holders at large-scale events using face recognition, which is called Ticket ID System. Such a system has been required to prevent illegal resale such as ticket scalping. Since illegal resale is a critical problem for popular events in Japan, strict steps are followed for verifying individuals holding tickets at event venues by human visual inspection with ID cards. This task is time consuming for venue attendants. It is also stressful because ticket holders feel uncomfortable when being kept waiting. The problem in verifying ticket holders is how to simultaneously verify identities efficiently and prevent individuals from impersonating others at a large-scale event in which tens of thousands of people participate. Ticket ID system makes it possible to secure the identity of the purchaser and holder of a ticket by using a face-recognition system developed for tablet terminals. Ticket ID System was proven effective for preventing illegal resale by verifying 50,324 attendees at a large concert of a popular music group. The average accuracy of face recognition was 90%. The average time for identity verification was 7 seconds per person including guidance to ticket holders, which decreased identity-verification time by 30% compared to using only human visual inspection as well as reducing the psychological workload of venue attendants. Survey results obtained from the attendees showed that 94.6% felt it provided more equity in ticket purchasing than methods used before, 83% felt it provided added convenience in verification, and 93.8% felt it would effectively prevent illegal resale.

Keywords: face recognition, biometrics, identity verification, illegal ticket resale prevention

1. Introduction

In today's modern society, where individuals are free to change residences and communicate with others, the communities and organizations to which individuals belong are becoming increasingly complex and diverse. This is happening concurrently with the development of transportation facilities and the spread of the Internet. In a so-called "Gemeinschaft" community, where territories and kinships were linked through friendships, it was not uncommon for all community members to know each other. However, in many modern communities and organizations, members are not necessarily acquainted with each other. When individuals exercise the rights they are given or carry out the obligations imposed on them, it is assumed that the actions are performed by the individuals themselves. In many cases, this is verified through the use of such means as ID cards. Legally verifying a person's identity requires verifying two points: "the person actually exists (reality)" and "the person is who he/she claims to be (identity)" [1]. The foundation of reality is the family register. There are limited situations in which "reality" needs to be strictly confirmed, but there are many situations in which "identity" needs to be verified. In modern society, many people have their identity verified many times in various ways, such as having their employee ID cards checked when they enter the workplace, using IT devices in the workplace, and using personal IT devices while taking advantage of the various IT services associated with them. This personal-authentication confirmation is called "identity" and is often used in the same sense as verification.

Identity verification is required in more situations than before. Let us take an example of a case in which many people are admitted to participate in an event. It used to be that in such cases, having a document, such as a ticket or an attendance certificate, checked was enough to gain entry; the need for personal authentication was not seriously considered due to the limited amount of time for admitting all the participants. Many events with high ticket prices had designated seating so it was not necessary to assume that some tickets may have been counterfeit. However, the advent of net auctions in recent years has made it easier to buy and sell tickets at the individual level. This has resulted in an increase in illegal ticket scalping, i.e., tickets being purchased for resale purposes [2], [3]. Consequently, event organizers have had to deal with complaints about the risk of malicious acts by undesignated individuals who take advantage of fans by buying and selling tickets on the Internet. In many cases, therefore, any ticket buying and selling outside the normal sales channels is prohibited. Ticket sales terms now often stipulate that tickets are invalid when people apply for them using a pseudonym or false name and/or false address, or when they have been resold on an Internet auction or through a scalper. Illegally resold tickets have in fact been invalidated at amusement parks [4] and concert halls [5]. Verification has therefore become a more important social issue than ever before. Equity in ticket purchasing is required not only

[1] NEC Informatec Systems, Ltd., Kawasaki, Kanagawa 213–8511, Japan
[a)] a-okumura@bx.jp.nec.com

by ticket purchasers but also by event organizers and performers [6].

Thorough verification for preventing individuals from impersonating others is in a trade-off relationship with efficient verification. Conventionally, venue attendants verify ticket holders by way of possession certification, i.e., possessions such as an ID card or driver's license. However, such verification is not effective in preventing individuals from impersonating others because these possessions are easy to transfer by lending or reselling. There are resellers who will offer ticket-and-resident-card sets or rent out ID cards at high prices. There are also ticket buying and selling sites on the Internet that make offers like "Ticket and photo-less ID card sets available for women in their 20s or 30s. Cards must be returned after the event." Furthermore, a photo ID may not necessarily genuine since photos can easily be color copied and superimposed. In fact, there are a number of sites on the Internet where one can have an ID card created.

At events attended by many people, it is not uncommon for people to stand in line to have their identities verified. Taking thorough measures to prevent individuals from impersonating others inevitably takes time. Some people stow their identity cards in a shoulder bag, purse, etc... and are unable to show them immediately. There are also people who will bring in a non-photo ID and insist that they are the person in question regardless of obvious differences in age and appearance. In such cases, the attendant will need to spend considerable time in verifying the person's identity. When the waiting time becomes long, some people might start feeling physically unwell or become frustrated at having to wait for so long and will start verbally abusing the attendant. This increases the verification time and the mental and physical burden on the attendant. It may also make quickly finishing the verification procedure more important than accurately ascertaining identity. Therefore, it is vital to make the verification procedure more efficient. Also, the procedure should not impair attendees' convenience.

The problem in verifying ticket holders is how to simultaneously verify identities efficiently and prevent individuals from impersonating others at a large-scale event in which tens of thousands of people participate. The solution should be based on non-transferable information to prevent impersonation. It should be also suitable within practical operation costs for various sized events held in various environments including open air. To solve this problem, we propose a system of verifying the identity of ticket holders at large-scale events using face recognition. The system matches a photo of the ticket-purchaser's face with the face of the person being admitted to the event to verify that the individuals are the same.

The remainder of the paper is as follows. In Section 2, we survey related work on electric ticket systems and personal authentication. In Section 3, we describe problems with a conventional method of verifying ticket holders and present our system of verifying the identity of ticket holders at large-scale events using face recognition in Section 4. In Section 5, we report the results suggesting our system's suitability for large-scale events and in verifying individuals attending the events as well as survey results obtained from 241 attendees who had seen the system in use when entering the events. In Section 6, we discuss our system from the view-points of efficiently verifying identities and preventing individuals from impersonating others, as well as considering the outlook for future issues involved in verifying ticket purchasers. We conclude the paper in Section 7.

2. Related Work

2.1 Electric Ticket Systems

Electric ticket systems have made it unnecessary to issue physical admission tickets and the admission procedure more efficient at large-scale events. These systems provide an electric ticket, which is a barcode or QR code displayed on a smart phone or tablet terminal instead of a paper ticket. One such system offers an electric tearing ticket that is invalidated when it is used for admission in the same way as a normal paper ticket is invalidated when it is physically torn [7]. However, an ordinary electric ticket is not effective in preventing impersonation because it is transferable. Therefore, an electric system has been investigated that electrically verifies identities of attendees to control admission. A transfer prohibited electronic ticket system with anonymity makes it possible to prohibit ticket-transfer with an interactive signature and undeniable signature [8]. Although this system presented promising experimental results, it has not been put into practical use because of the following reasons:

1) This system uses an IC card securing a secret key about a ticket purchaser on the presupposition that the IC card is never transferred to people other than the purchaser. The system cannot practically prevent impersonation because the presupposition cannot be always arranged.
2) This system verifies the identity between a ticket purchaser and ticket holder at an event venue by communicating with a remote server machine managed by the ticket issuer. The system requires high-speed and stable telecommunication environments at the event venue for real-time transaction. Therefore, the system tends to incur high costs regarding the environmental arrangement such as mobile telecommunication station vehicles, because a large-scale event in which tens of thousands of people participate is held at various types of venues, including open air, without adequately resourced communication facilities.

2.2 Personal Authentication

The following episodes denote personal authentication using a countersign, pillbox and tattoo during the Edo period (between 1603 and 1868) in Japanese history, The Akou Roushi (The Forty-seven Ronin) gave the countersign *yama* (mountain) and k*awa* (river) when they fought in the darkness to avenge their master's honor [9]. Those who were not ready with these countersigns were to be treated as enemies. A retired lord of the domain of Mito, Mitsukuni Tokunaga fought wrongdoing while masquerading as a commoner. He revealed his identity to the evildoer by having one of his two servants show them a small pillbox bearing the symbol of the Tokugawa clan [10]. A magistrate, Kinshiro Tohyama fought to catch wrongdoers while masquerading as an ordinary citizen and baring a distinctive cherry blossom tattoo without identifying himself. He bared his tattoos again at his

court to convince the wrongdoers that the magistrate himself was a witness to their crimes [11].

In today's modern society, personal authentication can be divided into three methods: (1) knowledge certification using information only the person in question knows, such as a password or personal identification number, (2) possession certification, i.e., possessions such as an ID card or driver's license, and (3) biometric authentication by confirming a person's fingerprints face, etc... Although knowledge and possession certification are already widely used, such as at bank terminals and in e-commerce, both methods can be transferable if the individuals purchasing tickets and those entering the event match. Therefore, neither can be effective means to prevent individuals from impersonating others.

Many anticipate that biometric authentication can be a means of solving these problems [12], [13]. One advantage of biometric authentication is that there is no risk of biological information being lost or forgotten. Also, biometric authentication can be considered a means to prevent individuals from impersonating others because it uses person-specific biological information. Biometric authentication verifies identity by matching pre-registered biometric information and collation information obtained through a sensor. For example, both the vein authentication procedure used in financial institutions [14] and fingerprint authentication procedure used in national and local governments [15] require dedicated biometric information sensors. Biometric authentication, which requires dedicated biometric information sensors, is not acceptable for verifying the identity of the purchaser and holder of a ticket because it is not practical for ordinary people to have their biological information registered in advance at home and checked at event sites on the day of the event with such sensors.

On the other hand, a sensor for face recognition is a normal camera that ordinary people can easy handle. Face recognition has been put into limited practical use for verifying identity such as entrance and exit control for rooms, immigration control, and reception control [16], [17], [18]. They are aimed at enhancing security, that is to say, preventing individuals from impersonating others. Their purpose is not improving efficiency of identity verification, which is required for checking a large number of people. There has been no reports on a system that is successful in increasing the throughput of identity verification, that is to say, the number of people who can be verified per unit time, by using face recognition.

No conventional identity verification system using electric tickets and personal authentication can verify identities efficiently as well as prevent individuals from impersonating others at a large-scale of event in which many people participate.

3. Problems with Conventional Method of Verifying Ticket Holders

3.1 Conventional Procedure

The conventional procedure for verifying individuals holding tickets for popular events is shown in **Fig. 1**.

Step 1: Tickets to popular events are often sold on a lottery basis at fan clubs or other organizations where membership is registered. Individuals apply for tickets by using their registered member information. Applicants are advised that if they are selected they will, as a measure to prevent illegal resale, be asked to show identification upon entering the event venue to confirm that they actually purchased the ticket.

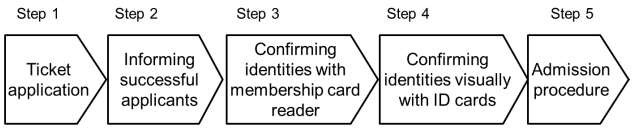

Fig. 1 Conventional ticket verification procedure.

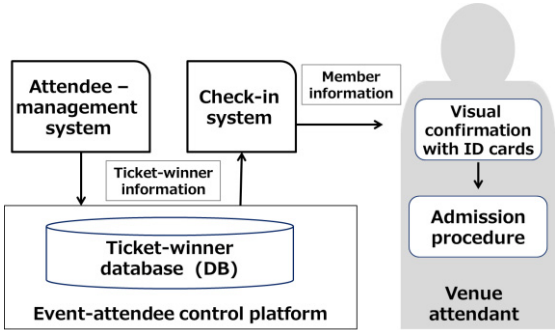

Fig. 2 Event-attendee control platform.

Step 2: Event organizers notify ticket winners, i.e., successful applicants that have been selected. Since the resale risk is high, applicants may only be notified of their selection and not sent the tickets in advance.

Step 3: On the day of the event, venue attendants use a membership card reader or other means to verify that individuals entering the venue are successful applicants.

Step 4: Venue attendants ask to see ID cards to visually ensure that the person's face matches that on the card. This is to guard against illegal resale and cards being lent or borrowed. Acceptable verification generally includes a driver's license, passport, student ID card, or basic resident register card. For minors or others who do not have photo identification, a resident card, insurance card, family register transcript, family register copy, or sealed registration certificate can be used instead.

Step 5: Venue attendants admit entry after verifying identities.

3.2 Configuration of Conventional System

Figure 2 shows an event-attendee control platform used to carry out the above-mentioned conventional procedure. The platform organizes both an attendee-management system for constructing a database of ticket winners who have to be verified as successful applicants entering the event venue before the event day and a check-in system for carrying out the admission procedure on the event day. The attendee-management system consists of a membership-registration module for the membership database and a ticket-winner-selection module, as shown in **Fig. 3**. The membership-registration module stores applicants' personal information, such as their membership numbers and names, in the membership database. When the number of applicants is more than the limited number of an event, the ticket-winner-selection module selects the successful applicants and sends their information to the ticket-winner database. The ticket-winner information is transferred to the check-in system,

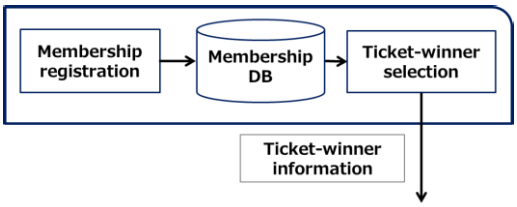

Fig. 3 Attendee-management system.

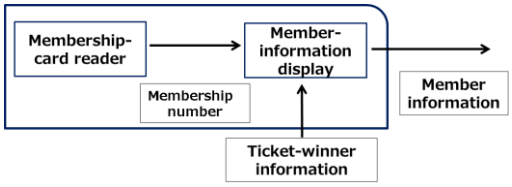

Fig. 4 Check-in system.

which is used on the event day. The check-in system consists of a membership-card reader and membership-information display that help venue attendants verify that individuals entering the venue are successful applicants, as shown in **Fig. 4**. At an event venue, the system shows the attendants the member information of the attendees, which is retrieved from the ticket-winner database with search keys of membership numbers obtained through the membership-card reader. The attendants admit the attendee to the event venue after they ensure the member information on the display is the same as that of their ID cards, as well as verifying their identities visually from their ID cards.

3.3 Problems with Conventional Method

The fundamental problem with the conventional method is that it cannot prevent individuals from impersonating others because it depends on possession authentication, i.e., verifying identities with a membership card and an ID card that contain transferable information. The solution to this problem should be a non-transferable method. The practical problem with the conventional method is that it is inefficient and time-consuming. Visual verification increases to 10 seconds per person on average except for problems such as failing to find the necessary cards or forgetting to bring them to the event venue. These problems are likely to add several minutes to verify identities. One way to solve the problem is to increase the number of experienced attendants, but cost and space problems make this a somewhat unrealistic approach. The solution should be to improve the throughput of identity verification, i.e., to increase the number of people who can be verified per unit time according to the number of attendees for a large-scale event. Also, it should be superior in portability for various types of venues including open air. In other words, the solution should combine non-transferability, efficiency, scalability, and portability for a large-scale event.

4. System of Verifying Identity of Ticket Holders at Large-scale Events Using Face Recognition

4.1 Identity Verification Using Face Recognition

As mentioned in Section 2.2, face recognition makes use of non-transferable facial image information and a normal camera as the sensor. Since a camera is a non-contact sensor different from that of fingerprinting, face recognition can provide hands-free authentication, which makes it possible for attendees to be verified when both of their hands are busy. What is better, face recognition is highly consistent when used with the conventional procedure for verifying identities because recognition results can be visually confirmed through the facial images by attendants.

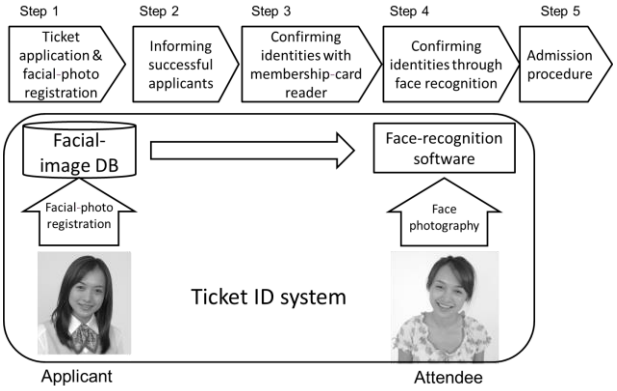

Fig. 5 Ticket-verification procedure with Ticket ID System.

For efficient identity verification to prevent individuals from impersonating others, we developed a system of verifying the identity of ticket holders that involves face recognition, which is called Ticket ID System. This system makes it possible to secure the identity of the purchaser and holder of a ticket through face recognition. Ticket ID System assists ticket applicants in registering their facial photos on their tickets then helps venue attendants verify the identities of ticket holders on the event day. The tablet-based face-recognition system is implemented within a single tablet terminal, which makes identity verification possible without requiring communication with remote server machines. It can be carried to any event venue, and the necessary number of systems can be easily set up at check-in places of event venues. This portability and scalability make the system practical for various types of venues and event sizes. Since the system executes face recognition using a camera mounted on a single tablet terminal, it can accommodate up to 100,000 people at large scale events by providing as many terminals as needed.

Figure 5 shows the ticket verification procedure from the first step of ticket application to the last step of admission supported by Ticket ID System. The procedure is different from the conventional procedure in the following steps. At Step 1, ticket application, facial photo registration is added. At Step 4, face recognition replaces visual verification by adding face photography to the procedure. Ticket ID System involves the following steps to verify ticket applicants and ticket holders.

Step 1: Individuals applying for tickets register their membership information as well as their facial photos. At that time they are advised of the privacy policy in effect regarding the handling of the photo and other personal information and the verification of their identity on the day of the event. In the same way as for an ordinary ID photo, the registered facial photo is a clearly visible frontal image taken against a plain background. The face must not be obstructed by a hat, sunglasses, mask, muffler, etc. . . , or by excessively long hair or a flashed peace sign.

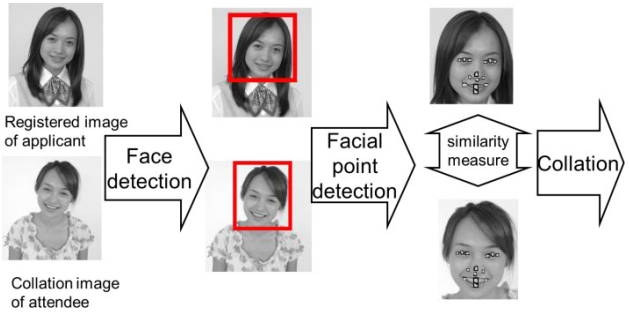

Fig. 6 Outline of face recognition process.

Fig. 7 External view of AGT10 commercial tablet terminal.

Step 2: Successful applicants are notified in the usual manner.
Step 3: Successful applicant identities are verified using a membership-card reader in the usual manner.
Step 4: At the event, the attendant uses face-recognition software to confirm that the photo taken at the time of application and the registered photo show the same person.
Step 5: The admission procedure is carried out in accordance with the face-authentication results.

4.2 Tablet-based Face-recognition System

The face-recognition software that Ticket ID System uses is the high-speed and high-precision commercial product NeoFace. NeoFace exhibited the highest performance evaluation in the Face Recognition Vendor Test 2014 conducted by the U.S. National Institute of Standards and Technology (NIST) [19], [20], [21]. The results were released in NIST's Interagency Report - NISTIR 8009 - Performance of Face Recognition Algorithms [22]. The NIST report is widely viewed as the benchmark of determining which face recognition software solution is the most accurate under a variety of situations. The face-recognition process is outlined in **Fig. 6**. In the process, registration images are compared with collation images to determine whether they show the same person [19], [20]. Ticket ID System compares registered images of applicants with collation images of individuals entering the event site. First, face detection is executed by detecting and processing the facial areas for each image. Next the facial-feature points of the detected areas — the eyes, nose, mouth edges, and so forth — are processed to carry out facial-point detection. Finally, the obtained facial-point positions are used to normalize the size and positions of the facial areas and measure their similarity, and the collation process is carried out for the registered and collation images.

The tablet-based face-recognition system was implemented in a commercially available AGT10 tablet terminal, as shown in **Fig. 7**. The terminal is equipped with a built-in rear view camera (15 Megapixels) with an autofocus function. Its basic specifications are CPU: ARM Cortex™ -A9, RAM: 1 GB (DDR2), and FLASH ROM: 8 GB (eMMC). The operating system is Android™ 4.1 [23].

Fig. 8 Display screen of face recognition software.

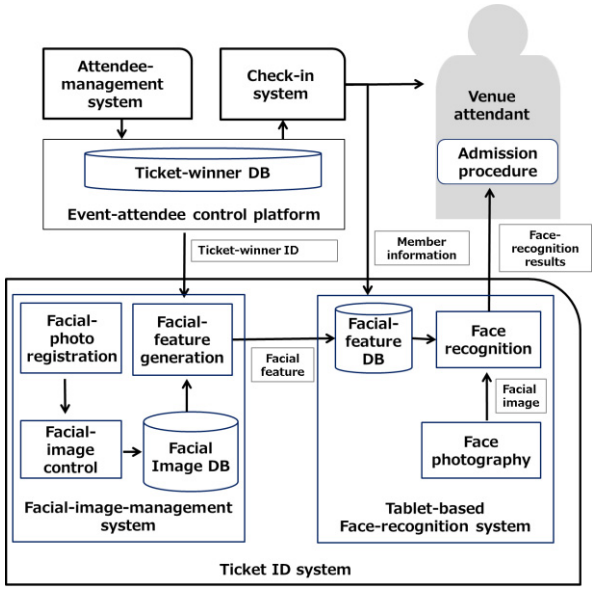

Fig. 9 Event-attendee control platform and Ticket ID System.

An applicant's facial feature information is encoded and copied to the tablet-based face-recognition system in advance, and the tablet executes the face-recognition process. The rear view camera in the terminal takes a photo of the ticket holder. When the face-recognition process starts, a message to that effect is displayed along with the detected facial area in a square frame (**Fig. 8** left). Within about 0.5 seconds, the recognition result is displayed with regard to facial image information of 100,000 people. If recognition is successful, a "Recognition confirmed" message appears (Fig. 8 middle). If recognition is not successful, a "Recognition not confirmed" message appears (Fig. 8 right).

4.3 Configuration of Ticket ID System

Figure 9 shows the configuration including the event-attendee control platform and tablet-based face-recognition system.

Ticket ID System consists of the facial-image-management system and tablet-based face-recognition system. The facial-image-management system constructs the facial image database by means of facial-photo registration and facial-image control. In the facial-image-management system, the facial-photo registration module involves uploading applicants' facial images on their tickets, and facial-image control module involves storing their images to the facial-image database after making sure that

the facial areas for the images are detectable. Facial-image control module also involves requesting the applicants to register different facial photos again when their facial areas are not detected due to obstructions, as mentioned in Step 1 of Section 4.1. The facial-image-management system generates facial features of ticket winners after obtaining their image data from the facial-image database with search keys of ticket-winner IDs, which are stored in the ticket-winner database controlled by the event-attendee control platform. The generated facial features of ticket winners are transferred in advance to the facial-feature database in the tablet-based face-recognition system.

When attendees check-in on the event day, the check-in system transmits their member information to the tablet-based face-recognition system. The system searches their facial-feature information through the facial-feature database then executes face recognition for the checking-in attendees by comparing their face photos taken at the event venue to show the attendants the face-recognition results. The attendants carry out the admission procedure in accordance with the results. Since they can visually see the registered photos and member information of attendees, which are transmitted by the check-in system, the attendants can verify them in case recognition is not confirmed.

4.4 Parameters and Threshold for Ticket ID System

Ticket ID System is controlled using intrinsic, extrinsic and operational parameters. The intrinsic parameters are due purely to the physical nature of the face, and are independent of the observer. They include age, expression and facial paraphernalia such as facial hair, glasses, and cosmetics. Extrinsic parameters are related to the appearance of the face. They include lighting, pose, background and imaging such as resolution and focus. Operational parameters are related to the interaction between attendants and attendees. They include how many times the face recognition process should be repeated per attendee until his/her identity is verified, whether an attendee should stop for the face recognition process, and whether an attendee should face the camera.

The intrinsic and extrinsic parameters were set up in accordance with the standards of NIST personal identity searches for passport/visa photo images [24]. The standards are preferable for Ticket ID System, and acceptable for individuals applying for tickets to register. Several specific standards on images are as follows:

1) Photos taken within 3 months
2) Face centered and no hair covering front of face
3) Eyes open on the same horizontal line
4) Single color background
5) No shadows on background and no shadows on face
6) No sunglasses and no glare on glasses
7) Remove hats and caps
8) No other face, partial face, toys nor other objects in image
9) No camera capture artifacts and no stretched images

These standards are illustrated on websites for individuals applying for tickets [25]. The operational parameters allowed the face recognition process to be executed within twice per attendee until his/her identity is verified. They made an attendee stop for face recognition and face the camera. As mentioned in Section 4.2, the similarity between a registered image and collation image is measured at the collation process. The measurement is carried out on the assumption that the images are taken in accordance with the parameters. When the similarity measure exceeds a certain threshold, the face recognition is regarded as successful. The initial threshold was set up in accordance with that of NIST personal identity searches which achieved the lowest false reject rate (FRR) 0.3% in processing the passport/visa photo image database at a false accept rate (FAR) of 0.1% [19].

5. Demonstration of Ticket ID System

5.1 Verification at Concert Venue

One hundred twenty sets of the check-in and tablet-based face-recognition systems were used for a pop concert on July 26, 2014 at Nissan Stadium (Yokohama, Kanagawa Prefecture), as shown in **Fig. 10**. They were installed just behind the baggage inspection site at the stadium's East, West, and North gates. Temporary tents were set up, as shown in **Fig. 11**. Venue attendants carried out Steps 3, 4, and 5, as mentioned in Section 4.1.

Step 3: Attendees' membership cards are placed on the card reader and the monitor screen confirms that the attendees are suc-

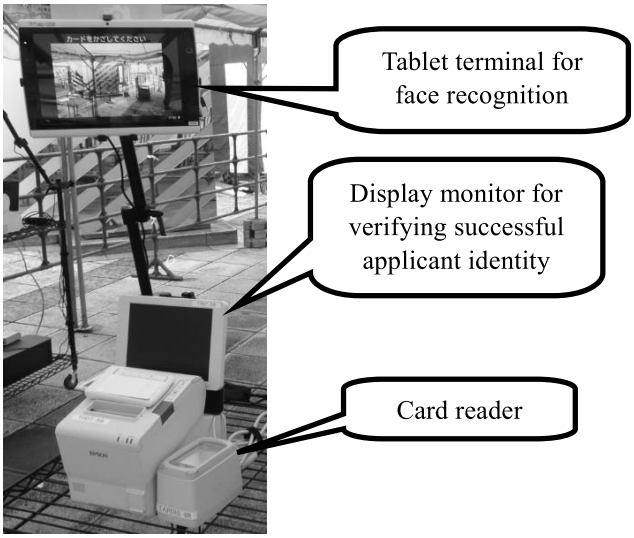

Fig. 10 Check-in and tablet-based face-recognition systems.

Fig. 11 Attendees being verified through face recognition.

Fig. 12 Recognition system admitting attendee.

Fig. 13 Examples of recognition failure.

cessful applicants. The screen displays the face images that were registered at the time of application.

Step 4: The attendant explains the verification through face recognition to the attendees and instructs them where to stand in front of the terminal. Then, they execute the face-recognition process using the terminal to confirm the attendees are those who applied for the tickets.

Step 5: If identity is verified, the attendee is admitted entry. If identity is not verified, the face-recognition process is repeated or identity is verified by direct visual inspection.

5.2 Results

Face recognition was carried out for 50,324 attendees over two days, as shown in **Fig. 12**. The weather was mostly sunny, but the area darkened temporarily due to a thunderstorm. Face recognition was carried out only for ticket applicants and not for individuals accompanying them; the event organizer allowed entry of one additional person or family accompanying each ticket-winner at the concert without face recognition. The recognition rate was 90%. Examples in which recognition was not successful are shown in **Fig. 13**. The recognition failed because the individuals had their eyes closed (Fig. 13 left), were not looking directly forward (Fig. 13 middle), or had hair covering their face (Fig. 13 right). There were also cases in which the darkness due to the thunderstorm was a factor.

The verification process took 6 seconds on average and 7 seconds in cases in which recognition was not successful. Where visual verification was required, this rose to 10 seconds. This was 30% more efficient than visually verifying identities by comparing conventional ID cards. No cases of individuals impersonating others were reported for this event.

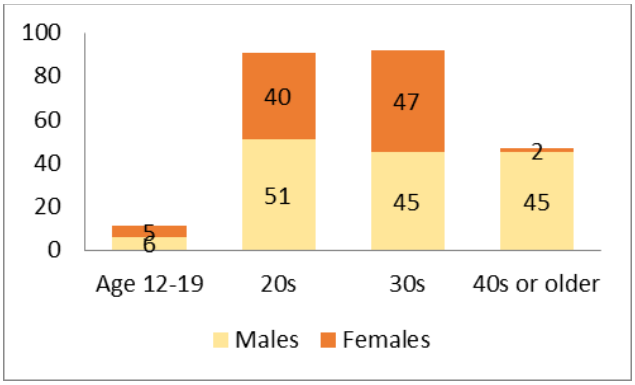

Fig. 14 Survey respondents by age and gender.

Table 1 Should there be more equity in ticket purchasing?

Responses	%
Definitely yes	66.4
Yes, I think so	25.3
No, I don't think so	6.2
Definitely no	2.1

Table 2 Does the system provide more equity in ticket purchasing than methods used before?

Responses	%
Yes, much more	36.5
Yes, somewhat more	39.4
It may; I'm not sure	18.7
No	5.4

Table 3 Why does the system provide more equity in ticket purchasing than methods used before?

Responses	%
It makes illegal resale harder	85.4
It makes it easier to get tickets	59.6
It cuts down on scalping	47.4
It reduces problems for ticket holders	13.2

Table 4 Does the system effectively prevent illegal resale?

Responses	%
Definitely yes	55.2
Yes, I think so	38.6
No, I don't think so	4.1
Definitely no	2.1

5.3 Concert Attendee Survey

Ticket ID System should be evaluated from the view-points of equity in ticket purchasing and convenience in verification to show how practical the system is. Therefore, surveys were conducted for attendees who were admitted after undergoing face recognition, as shown in Fig. 11. They were asked to respond to four questions about the system's equity in ticket purchasing and three questions about its convenience in verification. The 241 survey respondents are broken down by age and gender in **Fig. 14**. The survey results are shown as percentages in **Tables 1**–**7**.

(1) Equity in ticket purchasing

Regarding the question, "Should there be more equity in ticket

Table 5 Is the system more convenient than having the attendant verify ID cards and the like visually?

Responses	%
Definitely yes	36.9
Yes, I think so	46.1
No, I don't think so	11.6
Definitely no	5.4

Table 6 Why do you think the system is more convenient?

Responses	%
It streamlines the admission procedure	63.0
It makes showing an ID card unnecessary	42.0
It shortens the waiting time	38.0
It makes showing the attendant personal data unnecessary	24.5

Table 7 Why do you think the system is not more convenient?

Responses	%
It makes the admission procedure longer	73.2
The attendant is not used to using it	31.7
I'm concerned it might not recognize me correctly	31.7
I'm concerned about how it will handle my personal data	26.8

purchasing?" (Table 1), 91.7% of the respondents said either "Definitely yes" or "Yes, I think so."

Regarding the question, "Does the system provide more equity in ticket purchasing than methods used before?" (Table 2), 94.6% of the respondents said either "Yes, much more", "Yes, somewhat more", or "It may; I'm not sure."

Regarding the question, "Why does the system provide more equity in ticket purchasing than methods used before?" (Table 3), the offered responses were, "It makes illegal resale harder", "It makes it easier to get tickets", "It cuts down on scalping", and "It reduces problems for ticket holders."

Regarding the question, "Does the system effectively prevent illegal resale?" (Table 4), 93.8% of the respondents said either "Definitely yes" or "Yes, I think so."

(2) Convenience in verification

Regarding the question, "Is the system more convenient than having the attendant verify ID cards and the like visually?" (Table 5), 83% of the respondents said either "Definitely yes" or "Yes, I think so."

Regarding the question, "Why do you think the system is more convenient?" (Table 6), the offered responses included, "It streamlines the admission procedure", "It makes showing an ID card unnecessary", and "It shortens the waiting time."

Regarding the question, "Why do you think the system is not more convenient?" (Table 7), the offered responses included, "It makes the admission procedure longer", "The attendant is not used to using it", "I'm concerned it might not recognize me correctly", and "I'm concerned about how it will handle my personal data."

6. Discussion

6.1 Preventing Individuals from Impersonating Others

The recognition rate of 90% means the FRR was 10%. There were no reports of people attempting to impersonate others at the event, i.e., there was no false acceptance. Though they mean the system achieved an FRR of 10% and FAR of 0%, the FAR should be more carefully examined from the view-point of the system's robustness. Individuals purchasing tickets from websites were well aware that the registered face images of ticket applicants would be matched with the facial images of individuals attending the event when they entered the venue. Since few people will dare to impersonate others under these conditions, it is necessary to evaluate the robustness with a kind of pseudo attack tests.

Survey results obtained from 241 individuals who had seen the system in use when entering the event showed that 94.6% of them felt the system provided more equity in ticket purchasing than methods used before. Various reasons were given for this, among them "I think it will help prevent illegal resale (female, 30s)", "I think it will actually make me feel more at ease about the competition involved in purchasing tickets (male, 40s)", and "It's disadvantageous because it will prevent me from giving tickets to acquaintances, but it's a good system because it will help to control the illegal resale and scalping of tickets (male, 30s)." Survey results showed that 93.8% of the respondents felt it would effectively prevent illegal resale.

The system's performance has been widely reported in the mass media [2], [26]. The system is highly regarded by the Japanese Society of Artificial Intelligence (JSAI) [27] and a special interest group of the Information Processing Society of Japan (IPSJ), Consumer Devices & Systems (CDS) [28]. In addition to the pop concert reported above, it has been used to carry out face recognition for 26,859 people at Saitama Super Arena on December 24-25, 2014, for 33,434 people at Fukuoka Yahoo! Auctions Dome on April 4-5, 2015, and for 38,563 people at Shizuoka Stadium ECOPA on July 31-August 1, 2015. In fact, since the above-mentioned pop concert, it has been used more than 20 times for large-scale events [29]. No cases of individuals attempting to impersonate others were reported for any of these events. This is indicative of the system's effectiveness in improving equity in ticket purchasing and deterring or preventing illegal resale.

6.2 Making Verification More Efficient

With the face-recognition process, identity-verification time took 7 seconds on average. This was 30% more efficient than the time required to visually verify identities by comparing conventional ID cards. It also reduced the psychological workload for the event attendants. Most of the attendants were part-time workers and had to visually verify 500 to 1,000 individuals per day. Verbal exchanges with attendees and other factors put a high psychological workload on the attendants, and many said they likely would not do such work at future events without the face-recognition system in use. According to the event organizers, verification with the face-recognition system makes it easier for them to find part-time attendants who will continue to do such

work at future events.

Survey results obtained from the same 241 individuals showed that 83% felt the system provided added convenience in verification. Various reasons were given for this, among them "It eliminates problems and makes the admission procedure smoother (male, 40s)" and "It frees me from having to show my ID card (male, 40s)." The opinion that "I hope it will be used for future concerts (male, 20s)" was also expressed. This indicates the system is also able to reduce the psychological burden on event attendees. On the other hand, there were attendees who did not feel the system provided added convenience. Reasons given for this included "It makes the admission time longer (male, 30s)", "People wearing hats, makeup and the like might not be recognized and be denied entry (male, 40s)," and "Having my photo taken embarrasses me (female, teenaged)." The opinion that "Increasing the number of lanes or hiring more experienced attendants might help to shorten the lines (male, teenaged)" was also expressed. Even though the system's identity-verification time is 30% shorter than that for the conventional method using human visual inspection, it is essential to shorten it even more. It will be necessary to further streamline the system to meet the expectations of a greater number of individuals.

6.3 Future Issues

To evaluate Ticket ID System's robustness, pseudo attack tests should be designed. The tests should include a disguise test and lookalike test. A disguise test makes people's facial appearances as similar as possible to those of different people by using facial paraphernalia such as facial hair, glasses and cosmetics. A lookalike test is conducted for those with a similar physical nature regarding facial appearances such as twins, brothers and sisters. The disguise test will reveal tricks and help in creating operational manuals for venue attendants. A lookalike test will disclose the technical limitation of current face recognition techniques and help in establishing next-generation technology.

To make the system's identity-verification process more efficient, we should consider ways to improve its operating environment and face-recognition method. Its operating environment can be improved by installing lighting to compensate for insufficient lighting at the site. We could also make the system more efficient by finding ways that would improve the understanding and cooperation of users. There have been cases at event sites in which attendees' photos were taken but their identity could not be verified because they had their eyes closed, they were not directly facing the camera, or their hair was obstructing their face. The problem was often compounded because the attendant was unable to give the attendees a good explanation as to why their identity could not be verified. Providing prior information relevant to face recognition at the ticket application time or other times would enable facial photos to be taken appropriately. It can be expected that attendee understanding will increase as the face-recognition process and systems, such as in ours, become more widespread. However, event attendants will need to more effectively explain to attendees how their photos taken on the day of the event will be handled to alleviate their concerns. We plan to study the possibilities of introducing a "walk-through" system to improve face recognition. This would be a system with which people are photographed as they approach the system equipment head on and be admitted entry if face recognition succeeds [18]. Having individuals photographed as they approach would save them from having to stop to have their photos taken; thus, reducing waiting time [30]. We will attempt to develop a practical method in which this can be done.

7. Conclusion

We developed a system of verifying the identity of ticket holders using face recognition and used it at large-scale events to verify its effectiveness in suppressing illegal ticket reselling and preventing individuals from gaining entry by impersonating others. Its face-recognition process for ticket applicants and event attendees enables it to decrease identity-verification time by 30% compared to using only human visual inspection and reduce the psychological burden on event attendants. Survey results obtained from 241 individuals who had seen the system in use when entering an event showed that 94.6% of them felt it provided more equity in ticket purchasing than methods used before, 83% felt it provided added convenience in verification, and 93.8% felt it would effectively prevent illegal resale. However, opinions were expressed that it could be made more efficient to reduce admission time. To further streamline the verification procedure, we plan to improve its performance by introducing ways to more clearly explain the procedure to users and introducing a "walk-through" system.

Acknowledgments Ticket ID System has been used at concerts organized by TAIPIRS Inc. The 2nd Government and Public Solutions Division and Central Research Laboratories in NEC Corporation helped us use their face recognition software. Thanks are expressed to the personnel related to NEC Informatec Systems, Ltd., especially to Mr. Takeshi Takagi and Mr. Kiyohito Kubota for their efforts in planning and developing the system, and Mr. Jun Tsukumo for his valuable comments on this paper. Our deepest gratitude is expressed to Mr. Hiroshi Sakuma, President of NEC Informatec Systems, Ltd. for his constant encouragement and support.

References

[1] Japan Information Economic and Social Promotion Association: 2012 Information Security Promotion Business survey report, *Survey Research on Social Infrastructure Construction Using Attribute Information for Identification*, p.16 (2013). (in Japanese)

[2] Nihon Keizai Shimbun Electronic Version: NEC's face recognition prevents illegal reselling of Momoiro Clover-Z tickets (Dec. 10, 2014), available from ⟨http://www.nikkei.com/article/DGXMZO80664930Y4A201C1H56A00/⟩. (in Japanese)

[3] The National Consumer Affairs Center of Japan: Internet auction, available from ⟨http://www.kokusen.go.jp/soudan_topics/data/internet3.html⟩. (in Japanese)

[4] The Japan Times: Universal Studios Japan cracking down on ticket scalping (Oct. 19, 2015), available from ⟨http://www.japantimes.co.jp/news/2015/10/19/national/crime-legal/universal-studios-japan-cracking-down-on-ticket-scalping/#.VtgxsZ5f3Sd⟩.

[5] JE fandom: Johnny's Tracks Illegally Sold Tickets for Arashi's Japonism Tour (Oct. 25, 2015), available from ⟨https://jnewseng.wordpress.com/2015/10/25/johnnys-tracks-illegally-sold-tickets-for-arashis-japonism-tour/⟩.

[6] The Asahi Shimbun, The Yomiuri Shimbun: No illegal ticket resale, full-page advertisements (Aug. 23, 2016), available from ⟨http://www.tenbai-no.jp/⟩. (in Japanese)

[7] fringe watch: "tixee" ticketless management system realized "Denshi Mogiri" service for smart phones without barcode or QR code, available from ⟨http://watch.fringe.jp/2013/0613200357.html⟩. (in Japanese)
[8] Kaine, I., Sasaki, R. and Saito, T.: The Proposal and Evaluation of a Transfer Prohibited Electronic Ticket System with Anonymity, *Information Processing*, Vol.47, No.7, pp.2267–2278 (2006). (in Japanese)
[9] Schilling, M.: Mito Komon, *The Encyclopedia of Japanese Pop Culture*, pp.135–138, New York: Weatherhill (1997).
[10] Takeda, I., Miyoshi, S. and Keene, D.: *Chushingura: The Treasury of Loyal Retainers*, p.170 (1971).
[11] Wikipedia, the free encyclopedia, Tōyama Kagemoto, available from ⟨https://en.wikipedia.org/wiki/T%C5%8Dyama_Kagemoto⟩.
[12] Imaoka, H., Mizoguchi, M. and Hara, M.: Biometrics technology to preserve safety and security, *Information Processing*, Vol.51, No.12, pp.1547–1554 (2010). (in Japanese)
[13] Seto, Y.: Trends and prospects in biometric security authentication technology, *Information Processing*, Vol.47, No.6, pp.571–576 (2006). (in Japanese)
[14] Soto, M.: Using biometric authentication technology in Japanese financial institutions, *Information Processing*, Vol.47, No.6, pp.577–582 (2006). (in Japanese)
[15] Sakamoto, S.: Present Status and Prospects of Biometric Products and Solutions, NEC Technical Report, Vol.5, No.3 (2010), available from ⟨http://www.nec.com/en/global/techrep/journal/g10/n03/pdf/100303.pdf⟩.
[16] Zhao, W., Chellappa, R., Rosenfeld, A. and Phillips, P.J.: Face Recognition: A Literature Survey, *ACM Computing Surveys*, pp.399–458 (2003).
[17] Jafri, R. and Arabnia, H.R.: A Survey of Face Recognition Techniques, *Journal of Information Processing Systems*, Vol.5, No.2, pp.41–67 (2009).
[18] Face Recognition Technology Evaluation Committee for Immigration: Demonstration experiment results on face recognition technology for Japanese going and returning from abroad (2014), available from ⟨http://www.moj.go.jp/content/001128805.pdf⟩. (in Japanese)
[19] Imaoka, H.: NEC's Face Recognition Technology and Applications, IPSG SIG Technical Report, Vol.2013-CVIM-187, No.38, pp.1–4 (2013). (in Japanese)
[20] Sato, A., Imaoka, H., Suzuki, T. and Hosoi, T.: Advances in Face Detection and Recognition Technologies," *NEC Journal of Technology*, Vol.2, No.1 (2005), available from ⟨http://www.nec.com/en/global/techrep/journal/g05/n01/pdf/a028.pdf⟩.
[21] NEC: NEC's Face Recognition Technology Ranks First in NIST Testing for Third Consecutive Time (2014), available from ⟨http://www.nec.com/en/press/201407/global_20140716_01.html⟩.
[22] NIST: Face Recognition Vendor Test (FRVT) (2014), available from ⟨http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf⟩.
[23] NEC Information Square: Changing field work by tablet terminals (2014), available from ⟨http://jpn.nec.com/info-square/solution-report/ws/04.html⟩. (in Japanese)
[24] International Civil Aviation Organization: Machine Readable Travel Documents, pp.25–28 (2007).
[25] Every Entertainment Inc.: Momokuro Tickets: The Face Image Format Standards, available from ⟨https://momoclo-ticket.jp/mp/ps⟩. (in Japanese)
[26] PollstarPro: More Face Recognition (2014), available from ⟨http://www.pollstarpro.com/NewsContent.aspx?cat=0&com=1&ArticleID=815399⟩.
[27] JSAI: The 2015 Gold Award for Field Innovation from the Japanese Society for Artificial Intelligence (2016), available from ⟨https://www.ai-gakkai.or.jp/about/award/#INNOVATION⟩. (in Japanese)
[28] IPSJ SIG CDS: The 2016 Best Presentation Award, CDS16, Identity Confirmation to Issue Tickets using Face Recognition (2016), available from ⟨http://www.sig-cds.net/doku.php?id=presentation_award⟩. (in Japanese)
[29] Tapirs Inc.: Evolution of ticketing systems, available from ⟨https://www.tapirs.co.jp/live-event2015.html⟩. (in Japanese)
[30] NEC: NEC Walk-through face recognition system is introduced to the JAPAN HOUSE of 2016 Summer Olympics (2016), available from ⟨http://jpn.nec.com/press/201607/20160720_01.html⟩. (in Japanese)

Akitoshi Okumura received his B.E. and M.E. degrees in precision engineering from Kyoto University, Kyoto, Japan in 1984 and 1986. He joined NEC Corp. in 1986 and was engaged in researching natural language processing, speech translation and AI robot at NEC Central Research Laboratories. He joined DARPA machine translation project as a visiting scientist at the Information Science Institute of the University of Southern California, Los Angeles, USA in 1993. He received his Ph.D. in computer science from Tokyo Institute of Technology, Tokyo, Japan in 1999. He has been an associate vice president of NEC Informatec Systems, Ltd. since 2011. He is the recipient of the 2005 FUNAI Achievement Award from FIT, the 2005 Nagao Award from AAMT, the 2007 METI Minister Award from Fuji Sankei Business i, the 2008 Kiyasu Special Industrial Achievement Award from IPSJ, and the 2010 and 2015 Gold Awards for Field Innovation from JSAI. He is a member of IPSJ, JSAI and the Association for Natural Language Processing.

Takamichi Hoshino received his B.E. degree from Tokai University, Kanagawa, Japan in 1983. In 1983, He joined NEC Informatec Systems, Ltd. His current interests include the business promotion and development of physical security systems related to advanced technologies. He is the recipient of the 2015 Gold Award for Field Innovation from JSAI.

Susumu Handa received his B.S. degree in physics from Chuo University, Tokyo, Japan in 1984 and his Ph.D. in computer science from Kyushu Institute of Technology, Fukuoka, Japan in 2001. He is currently a manager in the Advanced Technology Solutions Division at NEC Informatec Systems, Ltd. His current interests include the business promotion and development of computer systems related to advanced technologies, especially face recognition and visualization in a high performance computing area. He is the recipient of the 2015 Gold Award for Field Innovation from JSAI.

Yugo Nishiyama received his B.E. and M.E. degrees from Kyushu Institute of Technology, Fukuoka, Japan in 2001 and 2003. He has been engaged in developing software systems at NEC Informatec Systems, Ltd. since 2003. His current interests include developing software for face recognition. He is the recipient of the 2015 Gold Award for Field Innovation from JSAI.

Masahiro Tabuchi received his B.E., M.E., and Ph.D. degrees in computer science from Waseda University, Japan in 1987, 1989, and 1993. He joined NEC Corporation in 1993 as a Researcher at NEC C&C Research Labs. and is now a senior expert of business development in the Advanced Technology Solutions Division at NEC Informatec Systems, Ltd. He is interested in human augmentation by using cognitive science and artificial intelligence. He is the recipient of Best Paper Award for Young Researcher of IPSJ National Convention in 1987 and recipient of the IPSJ Yamashita SIG Research Award in 1994. He is a member of IPSJ and the Institute of Electronics, Information and Communication Engineers.