Connected AR for Combating COVID-19

Tatsuya Amano, Hirozumi Yamaguchi, and Teruo Higashino

Abstract

Combating COVID-19 requires everyone to be aware of her surroundings, which may lead to the risk of infection, such as the density of persons nearby, fever status, and cleanliness of objects like doorknobs. Nevertheless, most of these situations are invisible to humans and are not recognized by them. This motivates us to leverage start-of-the-art wearable AR/MR devices such as Microsoft Hololens with high-capability sensing technologies to understand our activity space. This article addresses our challenges to recognize such situations by wearable AR/MR devices. Furthermore, we design a secure platform named Secure Connected AR Platform (SCARP) to share the detected information among those people who reside in the spatial space, in a privacy-aware fashion if the data is privacy-sensitive (e.g., body temperature). The significant feature of SCARP is that it does not require those people to register their personally identifiable digital IDs (e.g., email addresses) to access the platform and obtain the secured information. We hope this concept helps to reduce the risk of COVID-19 infection in places such as restaurants, airports, stations, and shopping malls, and bring the new normal there.

Introduction

The dramatic sophistication and miniaturization of augmented reality (AR) and mixed reality (MR) devices have brought a lot of success in industrial uses cases such as infrastructure maintenance, product design and assembly, and building construction where efficacy of work and the safety of workers have increased [1]. Generally, the abilities of people are augmented by the 2D/3D spatial sensing and recognition functions of AR devices, which are or will be equipped with RGB/depth cameras, inertial sensors, and 5G or faster wireless communications devices. Our idea is to leverage AR/MR devices with spatial computation functions supported by data-rich sensors to detect, share, and visualize risky situations involving surrounding humans, objects, and environments to prevent COVID-19 infection.

To this end, in this article, we first introduce our developed AR/MR application prototypes:

- Social distance measurement
- Fever detection
- Touched object detection

Second, leveraging these applications, we introduce a secure platform named Secure Connected AR Platform (SCARP) for sharing the situations in a privacy-aware, anonymous fashion if the detected information is privacy-sensitive. The platform has been tested in a lab environment to demonstrate its capabilities and effectiveness.

We assume use case scenarios where employees and owners of restaurants, security guards in shopping malls, and administrative staff in offices/schools wear AR/MR glasses. In the social distance measurement application, the state-of-the-art object recognition techniques such as YOLOv4 are exploited to recognize the surrounding persons and their locations in the wearer's vision. In the fever detection application, using plug-in thermography cameras, the body temperatures of the detected persons in the above social distance measurement application are measured, and those with high fever are identified. In these applications, the detected information is highlighted in the wearer's vision through the AR/MR glasses to allow the wearer to take appropriate actions. The touched object detection application is enabled by glasses with 3D depth-sensing functions (e.g., Microsoft Hololens). By detecting the wearer's hands and the objects in the surroundings from the depth data, the wearer's touching activities and the touched objects can be detected.

Based on these applications, we design SCARP, a secure platform to allow us to share the situations in the same space (Fig. 1). It contains a *spatial database*, which can store information about people and objects in the 3D space with their attributes. Examples of people-relevant information are people locations, distances among them, their densities, and their body temperatures, while those of object-relevant information are object locations, types, and touch frequencies. All this information is stored in the spatial database and are accessible via AR devices in the place. If a wearer detects personal information such as the body temperature of a nearby person, it should not be public to everybody in the space but be private to the person, to let her/him be aware of the situation. The wearer can set a *privacy level* to each information item to be posted to the database. We consider three privacy levels, *public*, *local*, and *private*, which are referred to as levels 0, 1, and 2, respectively (the details are explained later). To secure level 2 information, the wearer posts the private information to the spatial database with a *signature* that is unique to the target person. Then the platform allows only the person who owns the signature to access the information without revealing her/his private ID. We leverage the attitude of smartphones as a signature – matching the attitude signature of the target's smartphone estimated by computer vision techniques running on the wearer's AR device and that calculated by the smartphone's inertial sensors. Our platform also implements a protocol to send a message to notify the private information to the person's smartphone in a secure, anonymous fashion. Consequently, AR wearers can share public, local, and private information captured by the AR devices with the right people in the right way.

This article shows the proof of the above concept by designing and implementing those applications and the platform. We hope our platform is helpful for administrators who should prevent COVID-19 infections in their managed spaces such as restaurants, airports, and shopping malls, securing customers' and visitors' private information.

Digital Object Identifier: 10.1109/IOTM.0001.2000149

AR Applications for Situation Recognition

In this section, we introduce our applications for situation awareness by AR devices.

Social Distance Measurement

It has been widely recognized that social distancing is vital to prevent infection. However, people often forget it when they enjoy/concentrate on their activities such as shopping, eating, and talking. Measuring the distance between persons in public space and letting them be aware of it will help to prevent unintentional violations of social distancing.

As illustrated in Fig. 2a, a wearer of AR glasses (e.g., an employee of a restaurant, a shop owner, or a security guard) can measure the distance between herself and others, the gaps between them, and the level of overcrowding. This function is implemented using start-of-the-art object recognition like

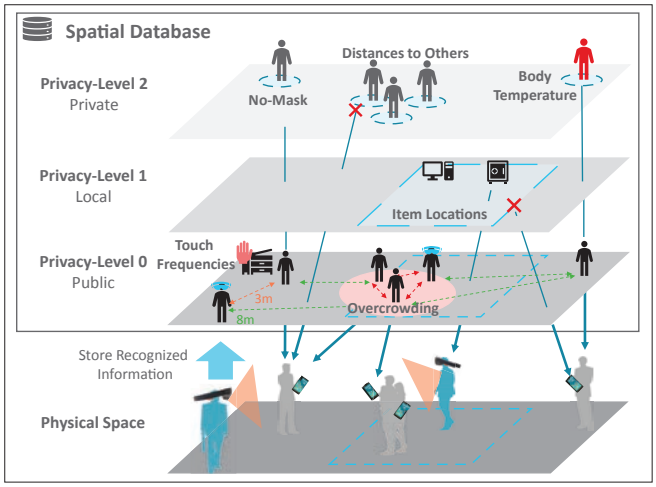


FIGURE 1. Secure platform involving AR glasses wearers and smartphone users. Information such as distance between persons, their fever (high body temperature), and touched objects are stored in a spatial database on a secure cloud server. Private data can only be accessed by the intended users.

YOLOv4. The locations of detected persons in the vision are transformed into spatial coordinates, relying on the angle and direction tracking function of the AR device. Such location information of persons will be shared via a spatial database.

Fever Detection

Detecting persons with high fever in public space will help to reduce the risk of infection. Notably, such a function will be required by administrative persons at stations, airports, and so on.

Leveraging the AR's person detection function described in the previous section, we assume the AR device has a thermography camera as a plug-in sensor. It tracks a detected person's body temperature, which adds a vital attribute to the person's information. As illustrated in Fig. 2b, we have demonstrated in our lab environment that a person wearing EPSON Moverio smart glasses and a FLIR ONE thermography camera detects persons in the space and their body temperatures. This also demonstrates part of our person identification function based on smartphone attitude matching, which is explained later.

Touched Object Detection

People intentionally and unintentionally touch their surrounding objects such as doorknobs, walls, desks, shelves, and many other items in offices, shops, and restaurants. Monitoring and visualizing what, where, and how often people touch will motivate the staff to sanitize their hands and things periodically.

Hand touch detection can be implemented using AR glasses with depth sensors (or MR glasses) like Microsoft Hololens. Figure 2c shows our Hololens application prototype that records the touched points and the number of touches. Hololens provides two crucial application programming interfaces (APIs), the spatial mapping API and the hand tracking API. These APIs provide the 3D location and 3D meshes of the surrounding objects and hands, and combining them makes it possible to detect the objects touched by the AR wearer. The application can also visualize the number of touches and the touched places in the wearer's vision. It also displays "dirty levels" of the hands based on the number of touches.

Secure Connected AR Platform

The core component of SCARP is a spatial database. The database contains the 3D model of a target space, where information on people and objects in the space and their attributes can be stored. As already explained, all the information recognized by the AR applications is sent to the spatial database on a secure cloud for information sharing purposes.

When an AR wearer posts information, one of the three privacy levels, 0 (*public*), 1 (*local*), and 2 (*private*) is set to control the access. As illustrated in Fig. 1, crowded locations, the average distance between persons and places where people frequently touch are level 0 information (*public*), which should be disclosed for public safety and convenience. Some information, such as locations of items and shelves, are level 1 information (*local*), which is not necessary to be public but is shared by those who reside in the place. *Spatial anchors*, which link a particular entry in the spatial database and the corresponding location in the physical space, enable this access control based on the physical space. Recent AR technologies, including Microsoft Hololens, Google ARCore, and Apple AR Kit, provide spatial anchor APIs. These APIs allow AR/mobile users to store spatial information to the database using spatial image features captured by cameras as keys. They also enable other people to use the anchors to retrieve the information. Finally, since person-relevant information such as abnormal body temperatures, social distancing violations, and not wearing masks are very personal, it should be level 2 (*private*) and be accessible only to the intended persons. To realize this, similar as with the spatial anchor concept, it is necessary to set a link between the target persons and their features. Using the features as keys, only these persons with keys can access the private information. Since using private features like facial information as keys causes severe privacy invasion, we design the concept of "*human anchor*," which is a privacy-preserving way of publishing and subscribing information anonymously. This is explained in the following section.

Human Anchor: Concept and Design

A human anchor works like a key to secure personal information (level 2 information), which is recognized by the AR applications but should be private to an intended individual. The necessary procedure of data storing/retrieving using a human anchor is the following:

- An AR wearer detects a person with her/his personal information, such as body temperature.
- The wearer also obtains her/his *human anchor* from the RGB camera as our AR applications assume computer vision to recognize the persons in the wearer's scenes.
- The wearer uploads the obtained information to the spatial database with the human anchor information.
- Assuming that only the target person has her/his human anchor information, she/he can access the stored data and others cannot.

Table 1 summarizes popular authentication methods that have been considered so far, and personal features such as faces, irises, and unique gaits are useful in the authentication of persons. However, revealing personal features to the system is not preferable. Wireless beacons such as Bluetooth Low Energy (BLE) beacons can be used as proof of presence. However, they do not fit with our purpose since our objective is to identify the persons in the AR wearer's vision. Instead, we focus on a smartphone held by a target person and use *smartphone attitudes* as a human anchor. The attitudes can be estimated from computer vision at the wearer side and calculated from its inertial sensors at a target person side. Assuming only the smartphone holder can obtain the inertial sensor readings, we guarantee that only the target person can access the information.

Figure 3 shows how the smartphone attitude is measured on the smartphone and is estimated from an AR device. In the proposed platform, the smartphone attitude is defined as its angles formed by three axes with the direction of gravity. Each AR wearer continues detecting and tracking persons in her/his vision, by combining a fast and accurate object detection algorithm, YOLOv4 [9], and an online real-time tracking algorithm, DeepSORT [10]. Once a person is detected, the

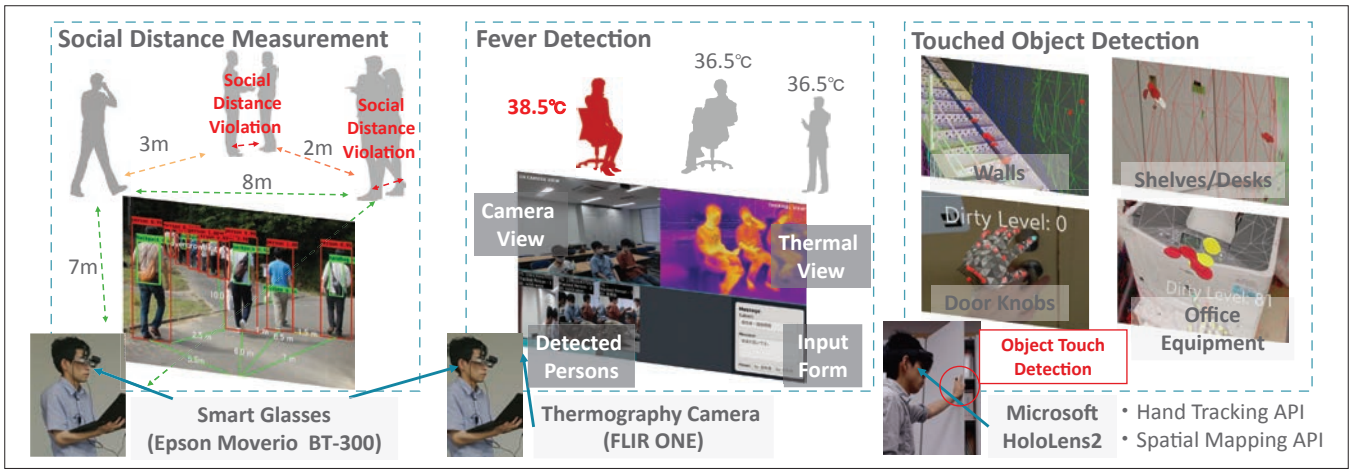


FIGURE 2. AR applications for situation recognition.

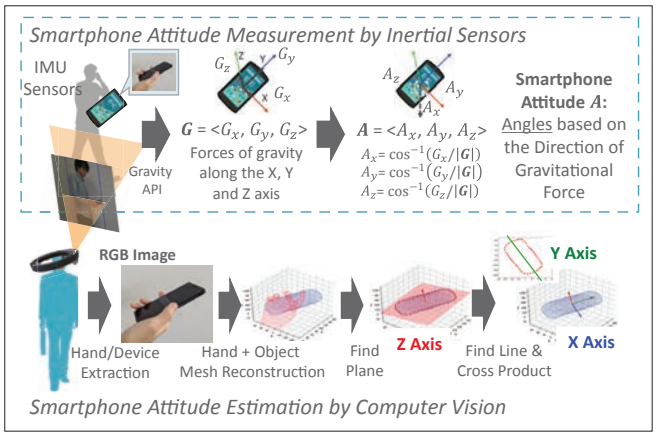


FIGURE 3. Smartphone attitude signature as a human anchor.

regions of her/his hands and the handheld smartphone are detected using YOLOv4. Then the shape mesh of the hand with the smartphone is generated from each captured image, utilizing the state-of-the-art deep neural network (DNN)-based hands and objects reconstruction method [11]. By identifying the smartphone's three axes in the obtained shape mesh and estimating gravity direction using the camera angle, the smartphone attitude can be estimated at the wearer side. Our preliminary experiment confirmed that the attitude estimation errors are mostly within 10° on each axis. Meanwhile, at the target person side, the smartphone attitude is captured by the Gravity Sensor API. This API provides the gravitational accelerations applied to each axis measured by acceleration sensors, and the smartphone attitude can be calculated by applying arccosine to the ratio of each axis's gravitational acceleration to the magnitude of gravitational acceleration.

For efficiency, each AR wearer transmits BLE beacons to let the surrounding smartphone users know her/his presence and activity. After knowing it, each smartphone that wishes to access the information continues capturing the smartphone attitudes by its accelerometers. By transmitting a series of attitudes with timestamps, access to an exactly matched entry is granted to the smartphone.

Access Protocol Using Human Anchor

Human anchors can be used to identify target persons' smartphones in the vision, but it is necessary to secure the platform when we employ the human anchor system. For example, if an AR device wearer is an attacker, she/he can post spam messages to a particular person, as many as she/he wishes. Even worse, the attacker can steal the posted private information of other persons as she/he can generate human anchors of persons in the scene. To cope with these situations, we design an access protocol exploiting human anchors and the public key infrastructure. In the following, an AR wearer who posts a person's information to the spatial database is referred to as *uploader agent* or simply *uploader*, and a smartphone user trying to obtain information posted by the uploader is referred to as *retriever agent* or *retriever* for simplicity of explanation.

Protocol Overview

The database access protocol between an uploader and a retriever is illustrated in Fig. 4. Besides these two players, there are a *spatial database*, and a trusted *identification server* with two databases called *ID store* and *key store*.

First, the retriever continuously generates a random ID with a timestamp. This is used as its *user ID* (denoted as *UID*). UID should be long enough to avoid ID collisions. The retriever records the UID on its local storage and also registers for the key store with its public key at regular intervals. When the uploader captures the situation, it generates a random ID (referred to as *AR ID* and denoted as *AID*) and broadcasts it via BLE or some proximity communication methods. Once the retriever receives the AID, and if it wants information that will be posted by the uploader, it measures the accelerometers to generate its human anchor and sends it to the ID store, with the received AID, the latest UID, and the timestamp. The uploader also captures the retriever's human anchors from a series of RGB images and sends it to the ID store as a query. In response to the submitted query, the ID store compares the received human anchors with stored ones and returns the corresponding UID to the uploader. The uploader queries the key store for the retriever's public key using the UID. After obtaining the public key, it encrypts the information with the key and uploads the encrypted information associated with the UID to the spatial database. The retriever can retrieve the information from the database anytime using the UID, and the information can be decrypted using the corresponding private key.

Protocol Validation

Given privacy concerns, the following three threats should be taken into account:

- Threat-I: *Spoofing*. An attacker mimics a retriever and retrieves her/his information from the spatial database.
- Threat-II: *Remote Spamming*. An attacker uploads a number of spam messages to the spatial database from a remote site.
- Threat-III: *Tracing/Stalking*. An attacker tracks a retriever in physical and cyber spaces by exploiting her/his human anchor.

In this section, we validate how the designed protocol resolves the above threats.

Feature	Authenticating device	Authenticated subject	Time	Temporary IDs
Face	Camera	Human	immediate	No
Fingerprint	Fingerprint Reader	Human	immediate	No
Iris	Camera	Human	immediate	No
		Human		No
Gait [2, 3]	Camera	Smartphone	10 seconds	Yes
Gesture [4, 5]	Wi-Fi Camera	Human	a few seconds	Yes
Trajectory [6]	LiDAR	Human	10 seconds	Yes
Proximity	BLE	Smartphone/Device	immediate	No
Radio [7, 8]	BLE	Smartphone	immediate	Yes
Device Attitude (Proposed)	Vision	Smartphone	immediate	Yes

TABLE 1. Identification/authentication features.

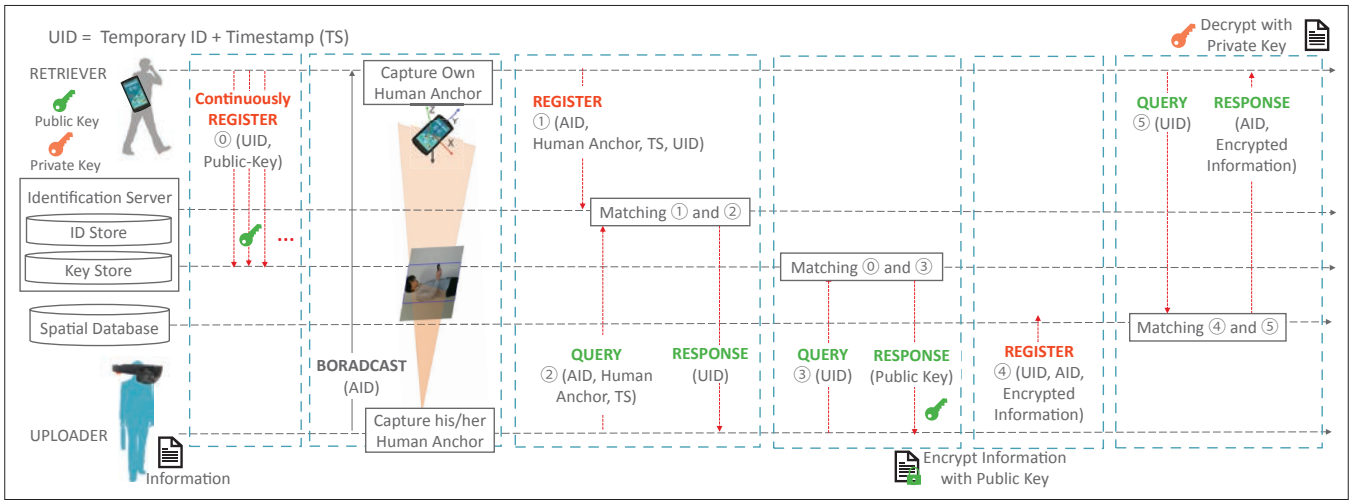


FIGURE 4. Database access protocol between an uploader and a retriever.

First, regarding spoofing (Threat-I), if there is a malicious retriever who can completely mimic the behavior of the surrounding victims' smartphone attitudes, it can steal the information intended for the victim. This can be avoided by using a more extended sequence of human anchors because it becomes harder to mimic the behavior as the sequence length becomes longer. Second, the protocol is protected from remote spamming (Threat-II) as it introduces a proximity detection and temporary UID. More concretely, when the uploader stores information about a retriever, we may set expiration time and dates to human anchors and UIDs so that the related messages and entries can be made invalid after a certain period. The retriever can also intentionally make them invalid at any time, depending on their privacy concerns. Finally, a UID's periodic change prevents the uploader, the identification server, and the database from tracking users in cyberspace (Threat-III). Public key cryptography can prevent any interception, man-in-the-middle attacks, and leaking information. For example, the identification server and key store know all user IDs and can retrieve the database, while they cannot decrypt any encrypted entities. Only the retriever that the uploader has intentionally specified via human anchors can decrypt them.

We note that passing the uploader's encrypted user ID via the database allows the retriever to obtain the uploader's public key. With passing the user ID and public key, uploaders can add a digital signature, which prevents the information from being tampered with.

Demonstration

Fever Detection in SCARP

We have prototyped the three applications, and have used the fever detection application to demonstrate SCARP. The demonstration video has been posted on our website [12].

As shown in Fig. 5, we have tailored Android-based smart glasses, EPSON Moverio BT-300, to be equipped with an RGB camera and a mobile thermography camera (FLIR ONE). The AR wearer can see both RGB and thermal views through the system, and can choose any person in the view as a retriever. Image processing is performed on the connected PC with NVIDIA GeForce GTX 1080 GPU and Intel Xeon E5-1680 v3@3.20 GHz CPU. The RGB frame rate was about 10 fps. In this environment, we asked three subjects in a room to hold their smartphones with an Android app to access the spatial database, detected these subjects in the RGB view, and measured their body temperatures using the thermal view.

The demonstrated scenario is that there was one with a high fever (target person) among three persons, and the detected temperatures are uploaded. Finally, only the target person receives a notification about the fever from the system to let her/him be aware of the fever and take appropriate action. This may be realized by the administrative staff of the space wearing AR glasses, who go around to detect those with high temperatures.

User Identification Accuracy

In the same experiment, we measured the ratio of successful and unsuccessful identifications for 5 minutes. About 3000 video frames were obtained as human anchors.

The identification failures are classified into three types. The first one is *identification denial*, which indicates that a pair of smartphones with the same attitudes exist, and hence, an AR wearer cannot distinguish them by their attitudes. The second one is *false rejection*, which means no attitude matching is found, although there is one. False rejection may occur due to the error of attitude estimation by an AR wearer. The last one is *false acceptance*, which indicates a matching is wrong. False

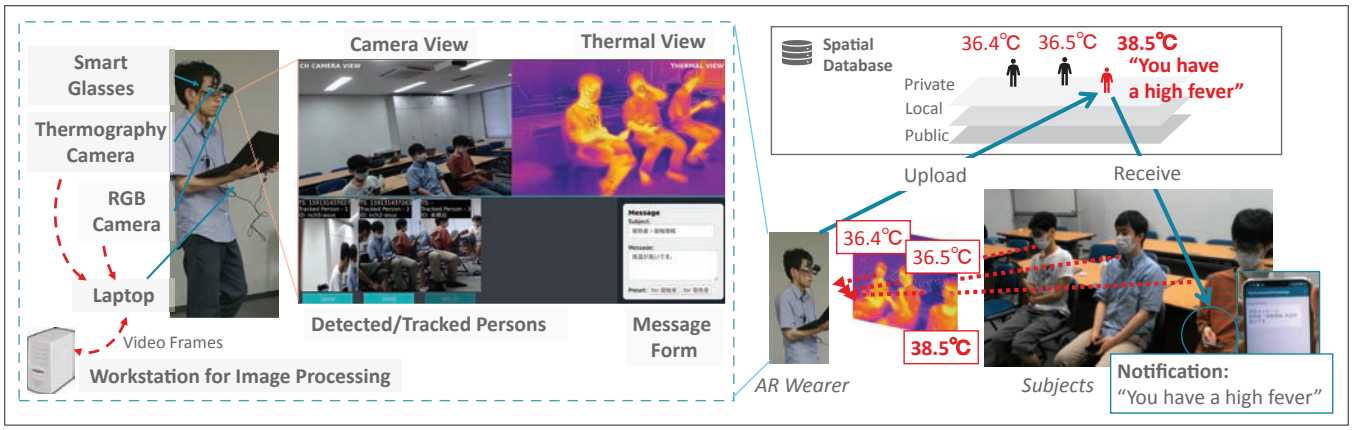


FIGURE 5. Demonstration of SCARP with fever detection application.

acceptance is fatal for SCARP since it results in disclosing private information to someone else.

These ratios may be affected by the "angular slack value" used in the smartphone attitude matching procedure. In this experiment, the smartphone attitudes are matched if the angular difference of the captured and measured axes is less than 10° in each axis. The smaller this slack value is, the identification denial and false acceptance ratios become more modest, while the false rejection ratio becomes larger.

From the experimental result, the human anchors of all three subjects were obtained by the AR wearer in 2190 frames, which means 73 percent of the total time was successful in user identification. As a breakdown of the failures, 10 percent were identification denial due to the collision of identification features, and 17 percent were false rejections. We would like to emphasize that false acceptance did not occur in this experiment. Achieving zero false acceptance while keeping a reasonable identification successful ratio is the most significant feature in privacy preservation.

Consequently, we have proved that the intended subject with a high fever could successfully obtain her/his information through the experiment. By investigating user identification success and failure ratios and the breakdown of the latter, we have also shown that the achieved success ratio was reasonable, and false identification did not occur with three subjects who acted similarly, sitting down nearby and using smartphones.

Research Challenges

Image Processing at Edge Devices

To pursue more privacy, the captured images should be processed in edge devices (i.e., AR glasses) without sending them to a cloud server. In our application demonstration, we used a workstation for image processing using DNNs such as Yolo and DeepSort. However, running them on small AR glasses is still a big challenge. Model compression approaches are promising to run DNNs in a resource-limited environment [13]. Moreover, dedicated hardware chips such as Goya/Gaudi by Habana Lab will help speed up the executions. By leveraging such hardware and software techniques, real-time detection should be realized to fully utilize AR devices' potential.

Leveraging Various Sensors

We may employ various types of sensors in our platform to enhance the capability of spatial recognition. For example, conversation levels can be detected by a microphone of the AR device to let those people be aware of the risk. A black-light can highlight environmental dirty levels in a dark place and is effective if it is co-used with our touch detection application. Enriching the spatial database by aggregating all such information related to COVID-19 will contribute to the analysis of potential risks of infection — how our living space is dirty and how it should be sanitized.

One of the advantages of SCARP is that it can recognize not only the environment but also the information about people in the space, being aware of privacy constraints. This means that SCARP can deal with any human-relevant private information. With more advanced sensors, it might be possible to recognize humans' biological information in the surroundings (e.g., heart sounds, fatigue, and headache) that cannot be seen by human eyes. Recently, wireless sensing has been more popular where millimeter waves can remotely monitor heartbeats and so on [14, 15]. Incorporating state-of-the-art sensing technologies will bring new applications and research issues to be addressed: stricter privacy preserving and consideration of social acceptance.

Conclusions

We have introduced an approach of recognizing and visualizing situations around us that cannot directly be seen by our eyes using AR technology. By collecting the information in a single spatial database, people can know the public information such as congestion levels of floors and shops, and the average social distance. The spatial database is a projection of the real world into cyberspace, and AR/MR devices can create a lot of useful information to prevent COVID-19 infection. The real-world phenomena and objects are associated with their physical positions via spatial anchors in the spatial database, and personal information is tagged by human anchors. To cope with issues such as tracking and stalker risks and privacy invasion by collecting more personal data, we have designed a platform named SCARP that enables secure access to the spatial database. We have prototyped three AR applications to incorporate physical world things and phenomena into cyberspace and demonstrated the fever detection system using a thermography camera. Again, we hope that our AR-based situation awareness system can be realized, and the proposals and proofs of concept in this article will help combat COVID-19.

Acknowledgment

This work was supported in part by Society 5.0 Realization Research Support Project funded by the Ministry of Education, Culture, Sports, Science and Technology (MEXT).

References

[1] P. Vávra *et al.*, "Recent Development of Augmented Reality in Surgery: A Review," *J. Healthcare Engineering*, vol. 2017, 2017.

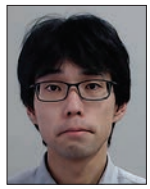
[2] Z. Wu *et al.*, "A Comprehensive Study on Cross-View Gait Based Human Identification With Deep CNNs," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 39, no. 2, 2016, pp. 209–26.

[3] M. Muaaz and R. Mayrhofer, "Smartphone-Based Gait Recognition: From Authentication to Imitation," *IEEE Trans. Mobile Computing*, vol. 16, no. 11, 2017, pp. 3209–21.

[4] J. Ranjan and K. Whitehouse, "Object Hallmarks: Identifying Object Users Using Wearable Wrist Sensors," *Proc. 2015 ACM Int'l. Joint Conf. Pervasive and Ubiquitous Computing*, 2015, pp. 51–61.

[5] X. Li *et al.*, "Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices," *Proc. 25th Annual Int'l. Conf. Mobile Computing and Networking*, 2019, pp. 1–17.
[6] T. Takafuji *et al.*, "Indoor Localization Utilizing Tracking Scanners and Motion Sensors," *2014 IEEE 11th Int'l. Conf. Ubiquitous Intelligence and Computing* and *2014 IEEE 11th Int'l. Conf. Autonomic and Trusted Computing* and *2014 IEEE 14th Int'l. Conf. Scalable Computing and Communications and Its Associated Workshop*s, 2014, pp. 112–19.
[7] H. Li *et al.*, "IDmatch: A Hybrid Computer Vision and RFID System for Recognizing Individuals in Groups," *Conf. Human Factors in Computing Systems — Proc.*, 2016, pp. 4933–44.
[8] Y. Park, S. Yun, and K.-H. Kim, "When IoT Met Augmented Reality: Visualizing the Source of the Wireless Signal in AR View," *Proc. 17th ACM Int'l. Conf. Mobile Systems, Applications and Services*, 2019, pp. 117–29.
[9] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "YOLOv4: Optimal Speed and Accuracy of Object Detection," 2020; http://arxiv.org/abs/2004.10934.
[10] N. Wojke, A. Bewley, and D. Paulus, "Simple Online and Realtime Tracking with a Deep Association Metric," *2017 IEEE Int'l. Conf. Image Processing*, 2017, pp. 3645–49.
[11] Y. Hasson *et al.*, "Learning Joint Reconstruction of Hands and Manipulated Objects," *CVPR*, 2019.
[12] T. Amano, H. Yamaguchi, and T. Higashino, "Connected AR for Combating COVID-19: Demonstration"; http://www-higashi.ist.osaka-u.ac.jp/tamano/connected-ar, 2020, accessed 19 July 2020.
[13] Y. Cheng *et al.*, "Model Compression and Acceleration for Deep Neural Networks: The Principles, Progress, and Challenges," *IEEE Signal Proc. Mag.*, vol. 35, no. 1, 2018, pp. 126–36.
[14] K. Chooruang and P. Mangkalakeeree, "Wireless Heart Rate Monitoring System Using MQTT," *Procedia Computer Science*, vol. 86, Supplement C, 2016, pp. 160–63.
[15] Z. Wang *et al.*, "Wi-Fi CSI-Based Behavior Recognition: From Signals and Actions to Activities," *IEEE Commun. Mag.*, vol. 56, no. 5, Mah2018, pp. 109–15.

Biographies



Tatsuya Amano received his B.E. and M.E. degrees in information and computer sciences from Osaka University, Japan, in 2016 and 2018, respectively. His research interests include mobile computing and applications.

Hirozumi Yamaguchi [M] received his B.E., M.E., and Ph.D. degrees in information and computer sciences from Osaka University in 1994, 1996, and 1998, respectively. He is currently an associate professor at Osaka University. His current research interests include design, development, modeling, and simulation of mobile and wireless networks and applications.

Teruo Higashino [SM] received his B.S., M.S., and Ph.D. degrees in information and computer sciences from Osaka University in 1979, 1981, and 1984, respectively. He joined the faculty of Osaka University in 1984. Since 2002, he has been a professor with the Graduate School of Information Science and Technology, Osaka University. His current research interests include design and analysis of distributed systems, communication protocol, and mobile computing. He is a Fellow of IPSJ.