Photo Crowdsourcing Based Privacy-Protected Healthcare

Long Hu, Yongfeng Qian, Jing Chen, *Senior Member, IEEE*, Xiaobo Shi, Jing Zhang, *Member, IEEE*, and Shiwen Mao, *Senior Member, IEEE*

Abstract—In this paper, the concept of crowdsourcing is applied to the medical field and a health monitoring mechanism based on photo crowdsourcing is proposed. Specifically, with photo crowdsourcing by many participators, the routine circumstances of users may be represented. However, these photos may include other people than the user, such as the visibility requestor, the invisibility requestor, and the passerby. The visibility and invisibility requestor are the participators in the system, whose identity can be set as visible or invisible, while the passerbys do not participate in the system. Hence, a privacy protection mechanism is proposed for this system, which includes two categories: i) The image fuzzy processing is provided for the invisibility requestor, while the original image is reserved for the visibility requestor. ii) The passerby's image is directly fuzzy processed for privacy protection.

Index Terms—Privacy protection, healthcare, photo crowdsourcing

1 Introduction

With the popularization of wearable devices, body data (blood oxygen, blood pressure, heartbeat, etc.) can be collected by smart clothes [1], smart wristbands and various other sensors, which can be used to provide users with fitness plans and falling detection, etc. With the health monitoring assisted by sensors, data analysis [2] and even real-time health monitoring services are available for users or their family members [3], [4].

However, there are some people, including senior citizens with Alzheimer's disease or children, may be unable to utilize a traditional health monitoring system with body sensors. Moreover, these people are easy to become lost, so it is essential that real-time health monitoring [5] must be provided to them [6]. However, it is a great challenge to provide them with monitoring by human resources, because it's very difficult and expensive to realize the real-time monitoring.

The popularity of crowd sensing is growing, which can be used for environmental monitoring, intelligent transportation, post-disaster reconstruction and other specific applications. As for the data obtained through crowd sensing, data storage and analysis may be conducted in the cloud for convenience [7], [8]. As stated previously, it is generally assumed that the cloud is "honest but curious". On one hand, the cloud provides users with computing and storage resources as per agreement [9]; on the other hand, cloud obtain users' data, thus compromising the privacy of users [10]. Various researches focus on the privacy protection [11], [12] in terms of trusteeship of the cloud. For example, number-based privacy protection is conducted through data confusion and encrypting storage, including storability certification and searchable encryption [13], [14]. In [14], a framework for safe cloud computing based on big data application is discussed, while the problem of secure storage on public cloud is described in [13]. The topic of search problems for encrypting data in a cloud is introduced. These works mainly focus on the search for keywords-based ciphertext of the text kind, but search problems involved with complicated content concerning images and so forth have not been studied. In [15], data confusion mechanisms including K-anonymity and differential privacy, etc., are studied. Image processing, security multi-party computation and homomorphic encryption, etc, are discussed in [16].

As far as security multi-party computation is concerned, participation in interaction is required in the whole process, so it is not available. Homomorphic encryption is too costly, even if the computing resource of a cloud is adopted, the computational cost would be too high, which increases the difficulty of specific implementation [17], [18]. In [19], automatic erasure of people who request privacy protection after they are automatically recognized in the case of photography with intelligent devices is introduced. However, if someone in a picture does not participate in the system, their privacy cannot to be protected. Furthermore, there are the following challenges for safe health monitoring mechanisms based on crowdsourcing: i) How to establish a health monitoring system based on crowdsourcing for special

- *L. Hu, Y. Qian, and X. Shi are with the School of Computer Science and Technology, HuaZhong University of Science and Technology, Wuhan 430074, China. E-mail: {longhucs, yongfeng}@hust.edu.cn, xiaoboshi.cs@qq.com.*
- *J. Chen is with the School of Computer, Wuhan University, Wuhan 430072, China. E-mail: chenjing@whu.edu.cn.*
- *J. Zhang is with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, Hubei, P. R. China. E-mail: zhangjing@mail.hust.edu.cn.*
- *S. Mao is the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849-5201. E-mail: smao@ieee.org.*

Manuscript received 5 Jan. 2017; revised 22 Mar. 2017; accepted 17 Apr. 2017. Date of publication 17 May 2017; date of current version 5 June 2019. (Corresponding author: Jing Zhang.)
Recommended for acceptance by M. Qiu, S.-Y. Kung, and Q. Yang.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TSUSC.2017.2705181

people and ii) how to accurately classify the people in the picture for corresponding privacy protection.

To addressing these challenges, this paper proposes a telemedicine monitoring system based on photo crowdsourcing. The method of photographing by different participants is utilized to restore the life state of the user. Persons involved in this system are divided into five kinds: users, participants, invisibility requestors, visibility requestors and passersby, while different safety policies are designed. Different from [19], photo crowdsourcing is taken into consideration, and safety protection measures are implemented for passersby, who do not participate in the system and whose identity tag is not available. In other words, different safety protection policies are assigned to different kinds of people. For example, fuzzy processing is conducted for an invisibility requestor or a passerby, but the original image information of a visibility requestor is reserved. Specifically, the main contributions of this paper are as follows:

- The health monitoring system based on photo crowdsourcing is proposed for the special people, with the detailed functions of various components.
- Group-oriented privacy policy is proposed to provide suitable privacy protection for different people.

The remainder of this article is organized as follows. Section 2 introduces the system architecture, safety problems and a threat model. Section 3 presents the key components. Section 4 describes the matching mechanisms based on privacy protection. Section 5 provides a simulation experiment, and Section 6 concludes the article.

2 System Description

2.1 System Architecture

One group, comprised of senior citizens with Alzheimer disease and children, receives special focus in this paper. In order to avoid unforeseen circumstances, such as a user becoming lost, a real-time monitoring service is required. Therefore, in this paper, photographing services are provided to users based on photo crowdsourcing, in order to restore the routine life status of the users. To be specific, the target population in the system i.e., persons who order the health monitoring service will be called users, and the persons who take photos for the users called participants. As for other persons in photos, some of them participate in the system and may mark their identities, and persons in this category are divided into invisibility requestor and visibility requestor; furthermore, there may be passersby who do not participate in the system but appear in the photos.

Participants are willing to play a role in the system and to take photos for the user, such as neighbors and friends. With the concept of crowdsourcing, the attributes of the crowd are collected so that photos for users can be taken. The photos taken will be sent to a cloud for storage, to restore the life state of users. The architecture of the system is as shown in Fig. 1. It can be seen from the figure that the user is Monica, participants are Tom, Annie, Tony and Jane, and the four participants are responsible for taking photos of Monica. It is shown in the photos of Monica that participants take photos of Monica in four situations: watching TV, attending class, playing outside and playing chess. After picking up the photos, Tom, Annie, Tony and Jane send them to a cloud for storage, so as to restore the life state of Monica in time if an accident occurs.

2.2 Application Scenes

In this paper, a health monitoring system applied to a special group is put forth and is based on photo crowdsourcing. As for its application scenes, there are the following circumstances:

- Health monitoring to prevent children or special senior citizens from being lost. Children are prone to be lost because they are at an early age, active and curious. Some children are lost because they are too fond of play or even because they are kidnapped. Unusual case senior citizens such as those with Alzheimer's disease can be in unforeseen circumstances, due to the features of a disease of this kind. For instance, these persons may become lost. In the proposed health monitoring system, several participants may be utilized to provide photographic services to users, with the goals of restoring routine life circumstance for users and to avoid the occurrence of accidents.
- Health monitoring for senior citizens living alone. Some senior citizens need to live alone because their children are not available or because their spouse is deceased. Because these senior citizens live by themselves, routing occurrences, such as going out alone can result in an accident. The system described in this paper could provide photographing of seniors living alone, and by recording their activities to avoid the occurrence of an accident. Even in the case of an accident, photos revealed by a health monitoring system of this kind may lead to the timely rescue.

2.3 Security Issues

The security issues considered in this paper are divided into two aspects: one aspect involves invisibility and visibility requestors who participate in the system, and the other aspect involves a passerby who does not actively participate in the system. The detailed introduction is as below.

- Invisibility requestor and visibility requestor, who participate in the system. Because these are system participants, they will send their image information to the cloud in advance. In this way, by utilizing matching mechanism, corresponding treatment can be applied to them as per tag information of invisibility or visibility.
- Passerby, who does not participate in the system. Because a passerby does not participate in the system, any information on a passerby is not received by the cloud in advance. If this kind of person is detected in the photos, direct treatment for privacy protection (such as fuzzy processing) is required.

2.4 Threat Model

It is assumed that clouds are "honest but curious" in this paper. Besides conducting data storage or processing, clouds may become interested in the data of a user, so the

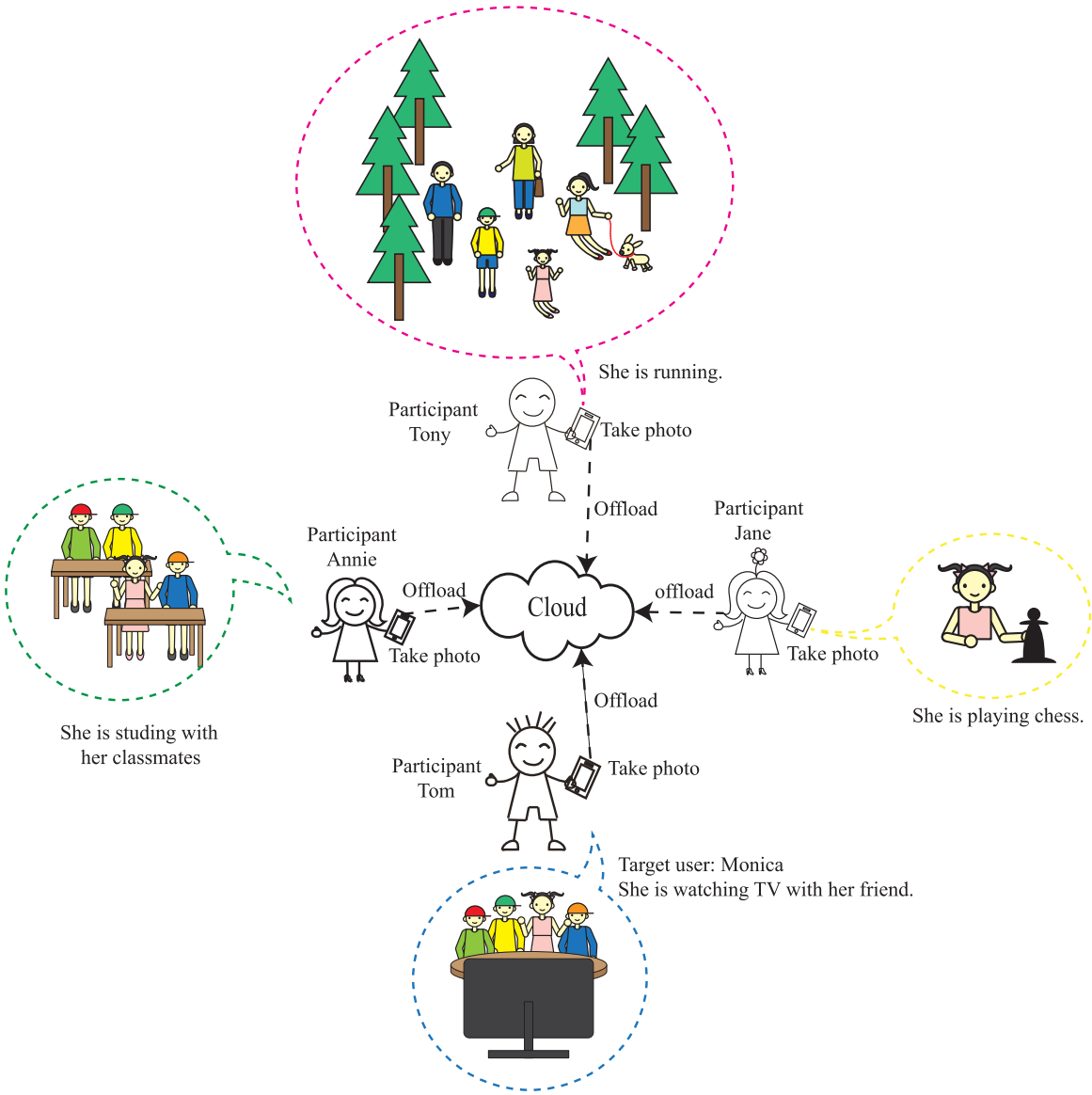


Fig. 1. Illustration of healthcare system based on photo crowdsourcing.

confidentiality during processing should be guaranteed, i.e., data processing should be conducted in a safe way. It is assumed that all participants serving users are honest and will directly send photos they're taken for users to the cloud. Because participants are almost all acquaintances of the user, it can be assumed that they are honest. Generally speaking, it can also be assumed that the channel is safe when users or participants send photos to the cloud and when the cloud delivers instructions to the user's end.

3 Key Components

This section focuses on the key components of the system and persons involved in the system, while the data source and outsourced cloud (cloud for short) are described in detail.

3.1 Persons Involved in the System

In this paper, a health monitoring mechanism for a specific group based on photo crowdsourcing is proposed. There are five kinds of persons who participate in the system, i.e., users, participants, invisibility requestors, visibility requestors and passersby. The five kinds of people will be introduced in detail as below.

- Users: "Users" represents the group who needs to order specialized health monitoring services and includes senior citizens with Alzheimer's disease, senior citizens living alone and children. Due to the particular circumstances of the users, they or their family members need this kind of health monitoring, which is based on photo crowdsourcing, for accident prevention. Even when user accidents occur, the photos of users recorded in the system may be utilized to track their daily habits, therefore help to find and assist them.
- Participants: Participants are persons who participate in the system by taking photos for users. Generally speaking, participants are acquaintances of users, such as neighbors, playmates or friends who

are able to see users frequently and who are also willing to participate in the system. Since the incentive mechanisms employed to attract participants into the system and thus to provide services to user is beyond the research scope of this paper, we provide a brief sketch of some such mechanisms roughly in section *D* of Section 3.

- Invisibility requestors: Photos taken by participants may include persons other than members of the special group. These system participants can choose to be visible or not. Those choosing to be invisible are called invisibility requestors.
- Visibility requestors: If those persons in photos (other than the user) who participate in the system choose to be visible, they are called visibility requestors.
- Passersby: If some persons in photos are passersby, they do not participate in the system at all and so cannot mark their identity. These "passive participants" (i.e., they have not chosen to participate in the system) who cannot mark their identities are called passersby.

It can be noted that users, participants, invisibility requestors, visibility requestors and passersby rely on specific situations, and the relationship among them is changeable. For example, two scenes will be considered, marked as scene A and scene B. There are five persons who are marked as $u_1, u_2, \ldots, u_5$; u_1 stands for the user who requires health monitoring, u_2, u_3, u_4 and u_5 are persons involved in scene A and scene B. It is assumed in scene A that u_1 is playing international chess with u_2, who participates in the system and marks himself or herself as a visibility requestor, and u_3 is the participant responsible for photographing. It is assumed in scene B that u_1, u_3 and u_4 are shopping in a mall; u_3 and u_4 participate in the system, and are marked as visible and invisible respectively, so that u_3 is visibility requestor, u_4 is invisibility requestor, and u_2 is the participant. There are u_1, u_3, u_4 and u_5 in the photo taken, but u_5 is a passerby. It can be seen from the two scenes above that u_2 is a visibility requestor and u_3 is a participant in scene A, while u_3 is visibility requestor and u_2 is participant in scene B. This shows that the identity of one person can vary in different scenes, i.e., the definition on identity relies on the specific scene.

3.2 How to Distinguish Five Types of People in the System

The participators of the system in this paper are divided into five types, i.e., user, participators, invisibility requestors, visibility requestors and passersby. However, how to distinguish these five types of people in the photos accurately is a challenge. As a matter of fact, the key to distinguish these five types of people is correctly matching their respective portrait information and privacy protection information. Specifically, for user, participators, invisibility requestors and visibility requestors, they are involved in the system and their identity tags are available, so the people in need of privacy protection can be separated from those without needing privacy protection. After gaining the photos, people in need of privacy protection can be automatically identified by the technologies such as face recognition, in order to detect the area in need of privacy protection in the photo automatically. In the case of small amount of photos, the people in the photos can be processed in the mode of manual marking. Thus, except for passersby in the photos, the others are marked. The visibility requestors do not need the protection of privacy area, but their identities can match with the corresponding images of the technologies such as face recognition, and the people without information in the photos can be directly deemed as passersby.

3.3 Sources of Data

There are the previously mentioned five kinds of people (i.e., users, participants, invisibility requestors, visibility requestors and passersby) involved in a health monitoring system based on photo crowdsourcing. Of them, invisibility requestors, visibility requestors and passersby do not provide data proactively and appear in photos passively; the main sources for image data are photos taken by participants or by users themselves. This kind of data is mainly used to restore the life state of users, and the corresponding descriptions are as follows.

- Data from users: Data from users refer to photos taken by users themselves. These photos may be taken when users stay alone indoors or when users go out alone. In this scene, there are at least two identities for the users, i.e., user and participant. This image information will be forwarded to a database in a cloud for storage.
- Data from participants: Data from participants are photos of users taken by participants and these photos will also be transmitted to the cloud for storage.

The data mentioned above are mainly used to record the life state of the user. Image information of invisibility requestors and visibility requestors who participate in the system would be collected by the system in advance, in order to enable the subsequent operation of the matching mechanism. Because there may be invisibility requestors and visibility requestors in these photos, there are special requirements for them to state a performance regarding whether or not they are to appear in the photos, so persons with requirements of invisibility shall be deleted in the photos at the cloud level, and persons with requirements of visibility shall have their images reserved in the photos. In order to match these requirements, image information of invisibility requestors and visibility requestors shall be used as the data source for the matching mechanism. These data will be stored on the cloud in advance, be marked as "visible" and "invisible" respectively, and be used to conduct matching of these data and photos of users, in which they may appear.

3.4 Outsourced Cloud

As works such as image storage and matching are involved in the system, a large amount of storage and computing resources are required and hence, the outsourced cloud is utilized for processing. Specifically, the main tasks of the outsourced cloud are as follows.

- To store photos of users and image information of invisibility/visibility requestors.
- To conduct matching between image information of invisibilit/visibility requestors and photos taken by participants.

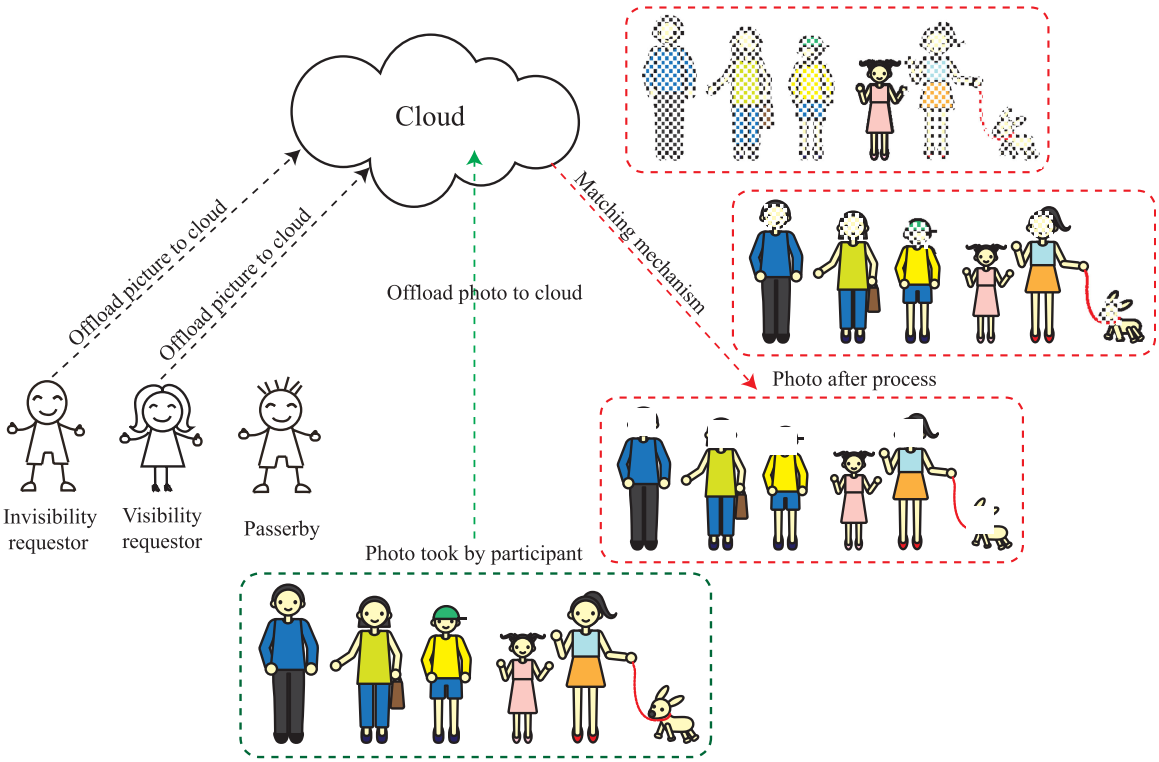


Fig. 2. Illustration of privacy protection mechinism.

- To directly conduct fuzzy processing to images of passersby, so as to protect image information of those persons who are only indirectly involved.

3.5 Incentive Mechanism

This paper proposes a health mechanism for a special group based on photo crowdsourcing and corresponding safety precautions. However, there is an issue regarding the way to attract participants into the system to take photos for users. The participants in the system may be acquaintances of the users, such as friends and neighbors, but they may also be volunteers, who are willing to participate in the system to help these special groups, or people who are attracted due to an incentive mechanism. How to attract them or the so-called incentive mechanism and the reasonable setup of said mechanism is one of the key factors for successful popularization of the system. Though it is not the key point of this paper, some suggestions on incentive mechanisms may be given: (i) setup of a reward in the system which corresponds to the size of one's contribution; (ii) setup of a credit rating in the system, where participants who abide by the system's guidelines (i.e., to not release pictures taken before these pictures are treated), enjoy a high credit rating. If a participant with a high credit rating appears in the system as an invisibility requestor, he or she would enjoy corresponding privacy protection and get more rewards.

4 Privacy Protection Mechanism

In photos of users collected by participants, there may be invisibility requestors, visibility requestors and passersby, as well as users. In fact, these three kinds of people can be divided into two categories: (i) persons who participate in the system; (ii) persons who do not participate in the system. The privacy protection policies vary for different kinds of people.

Fig. 2 systematically shows privacy protection policies that are in place. It can be seen from the figure an invisibility requestor, a visibility requestor, a passerby and a user to appear in photos taken by a participant. Invisibility requestor and visibility requestor transmitted their image information to cloud for storage in advance, but passerby did not transmit any image information in advance. After participant takes photos of user, invisibility requestor and visibility requestor will be detected by the cloud through matching mechanism, and fuzzy processing will be conducted to invisibility requestor in the meantime. As for passerby without image information, fuzzy processing will be directly conducted. To be specific, as for privacy protection mechanism, there may be hidden processing in allusion to faces and that in allusion to the whole body, and this hidden processing may be direct erasure or fuzzy processing. It can be seen from Fig. 2 that even the relationship between a dog and the user may be judged through context, thus to conduct corresponding privacy protection treatment to it. However, how to judge the relationship between a dog and the user is beyond the discussion range of this paper. Next, different privacy protection strategies will be introduced respectively from the above-mentioned two aspects.

Specifically, the photos of users should be pretreated prior to transmitting to the cloud. As previously mentioned, the people in the corresponding privacy demands in the photos can be distinguished by the face recognition technology, so as to gain the corresponding area in need of privacy protection. After selecting the privacy area, all photos can be divided into visible part and invisible part. The visible

TABLE 1
Notations

Variable	Explanation
u_i	people participated in this system
$q(u_i)$	Quantified expression of identity tags of persons who participate in the system
v_i	Node i
$e(v_i, v_j)$	Line between node v_i and v_j
V	Set of v_i
E	Set of $e(v_i, v_j)$
$s(\bar{V}, \tilde{V})$	Similarity between $\bar{V}$ and $\tilde{V}$

part is the direct public, and can be stored and shared directly in the cloud. But the invisible part can be put in the cloud after the privacy protection, and can be accessed only by authorized users. Here we consider some methods for treatment of privacy part, such as Mask, fuzzy processing, and P3.

4.1 Privacy Protection Matching Mechanism for Invisibility Requestor and Visibility Requestor

- Step 1: The system needs to obtain image information on invisibility requestors and visibility requestors in advance. For convenience, only one scene is taken into consideration, because treatment to multiple scenes relies on treatment to scenes one by one. Assume that there are u_1, u_2, $\cdots$ and u_m involved in a scene, and define function $q(u_i)$, wherein $i = 1, 2, \ldots, m$,

$$q(u_i) = \begin{cases} 1 & u_i \text{is invisibility requestor} \\ 0 & u_i \text{is visibility requestor.} \end{cases} \tag{1}$$

  This function is used to conduct a quantified expression of identity tags of persons who participate in the system. After u_i who participates in the system (with respect to a specific scene) chooses to be visible or not, this participant uploads image information to the cloud for storage, together with function value $q(u_i)$.
- Step 2: After image information is received by the cloud, feature extractions will be conducted. Since the image information taken into consideration in this paper is faces, a graph model may be used to stand for image information. In other words, let $G = (V, E)$ stand for image of the invisibility requestor or visibility requestor. Therefore, V stands for the collection of nodes, i.e., $V = \{v_1, v_2, \ldots, v_n\}$, and v_i stands for node i, and E stands for the collection of line segments between any two nodes. Record line segments between node v_i and node v_j as $e(v_i, v_j)$.
- Step 3: After participants take photos of users, they upload them to a cloud. For the convenience of matching between invisibility requestors or visibility requestors and photos taken by participants, adopt the face representation method similar to Step 2, extract the feature and make it be represented by graph model $G = (V, E)$, thereinto, the definition of V and E is as mentioned in Step 2.
- Step 4: After completion of Step 3 at cloud, matching between invisibility requestors or visibility requestors and photos taken by participants will be conducted, using the following two steps:

  (i) Adopt a matrix to stand for the image information of the faces. Make $\bar{G} = (\bar{V}, \bar{E})$ stand for face information of an invisibility requestor or visibility requestor, thereinto, $\bar{V} = \{\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n\}$, $\bar{E} = \{\bar{e}(\bar{v}_i, \bar{v}_j)\}_{i,j}$. As each node $\bar{v}_i$ stands for property of image in area i, so $\bar{v}_i$ may be represented as vector $(\bar{p}_{i1}, \bar{p}_{i2}, \ldots, \bar{p}_{il})$. Therefore, $\bar{G}$ may be represented by the following matrix $\bar{P}$:

$$\bar{\mathbf{P}} = \begin{bmatrix} \bar{p}_{11} & \bar{p}_{12} & \bar{p}_{13} & \cdots & \bar{p}_{1l} \\ \bar{p}_{21} & \bar{p}_{22} & \bar{p}_{23} & \cdots & \bar{p}_{2l} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \bar{p}_{n1} & \bar{p}_{n2} & \bar{p}_{n3} & \cdots & \bar{p}_{nl} \end{bmatrix}. \tag{2}$$

  There are n rows and l columns in matrix $\bar{P}$. Each row represents a node, and all vectors corresponding to that row are descriptive property of that node. Similarly, $\tilde{G} = (\tilde{V}, \tilde{E})$ stands for face information in photos taken by participant, thereinto, $\tilde{V} = \{\tilde{v}_1, \tilde{v}_2, \ldots, \tilde{v}_n\}$, $\tilde{E} = \{\tilde{e}(\tilde{v}_i, \tilde{v}_j)\}$. Correspondingly, there are l descriptive properties corresponding to each point $\tilde{v}_j$. For convenience, it is assumed that the number of descriptive properties for $\bar{v}_i$ and that for $\tilde{v}_j$ is identical, and they are denoted as $\tilde{v}_j = \{\tilde{p}_{j1}, \tilde{p}_{j2}, \ldots, \tilde{p}_{jl}\}$. Similarly, $\tilde{G}$ may be represented in a form similar to matrix $\bar{P}$, as shown below:

$$\tilde{\mathbf{P}} = \begin{bmatrix} \tilde{p}_{11} & \tilde{p}_{12} & \tilde{p}_{13} & \cdots & \tilde{p}_{1l} \\ \tilde{p}_{21} & \tilde{p}_{22} & \tilde{p}_{23} & \cdots & \tilde{p}_{2l} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \tilde{p}_{n1} & \tilde{p}_{n2} & \tilde{p}_{n3} & \cdots & \tilde{p}_{nl} \end{bmatrix}. \tag{3}$$

  Matrix $\tilde{P}$ is a matrix of $n \times l$, and node i is represented by vector $\tilde{p}_{i,:}$.

  (ii) Computation of similarity between image information of faces. After defining matrix $\bar{P}$ that describes image information of invisibility requestors or visibility requestors and matrix $\tilde{P}$ that describes image information in photos taken by participators, $\bar{P}$ and $\tilde{P}$ will be further represented in the form of a block matrix. To be specific, the matrix may be represented in the form of a vector, i.e., $\bar{P} = (\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n)^T$. Hence, the specific vector representation of row vector No. r in $\bar{P}$ (i.e., node $\bar{v}_r$ No. r for invisibility requestor or visibility requestor) is $\bar{v}_r = (\bar{p}_{r1}, \bar{p}_{r2}, \ldots, \bar{p}_{rl})$. Similarly, matrix $\tilde{P}$ may also be represented in the form of vector, i.e., $\tilde{P} = (\tilde{v}_1, \tilde{v}_2, \ldots, \tilde{v}_n)^T$; however, the specific vector representation of row vector No. q in matrix $\tilde{P}$ (i.e., node No. q for face information in photos taken by participant) is $\tilde{v}_q = (\tilde{p}_{q1}, \tilde{p}_{q2}, \ldots, \tilde{p}_{ql})$.

  Let $d(\bar{v}_r, \tilde{v}_q)$ stand for distance between node $\bar{v}_r$ and node $\tilde{v}_q$, and its value is

$$d(\bar{v}_r, \tilde{v}_q) = \|\bar{v}_r - \tilde{v}_q\|_p. \tag{4}$$

In Formula (4), the right item $\|\cdot\|_p$ stands for p-norm, and its common p values are $1, 2, \infty$ (respectively called as 1-norm, 2-norm and infinite norm). Represent $d(\bar{v}_r, \tilde{v}_q)$ with these three norms, as shown below:

$$d(\bar{v}_r, \tilde{v}_q) = \begin{cases} \sum_{j=1}^{l} |\bar{p}_{rj} - \tilde{p}_{ql}| & p = 1 \\ (\sum_{j=1}^{l} |\bar{p}_{rj} - \tilde{p}_{qj}|^2)^{1/2} & p = 2 \\ max(|\bar{p}_{r1} - \tilde{p}_{q1}|, \ldots, |\bar{p}_{rl} - \tilde{p}_{ql}|) & p = \infty. \end{cases} \tag{5}$$

Further, the distance between $\bar{P}$ and $\tilde{P}$ may be taken into consideration and recorded as $d(\bar{V}, \tilde{V})$. Similar to the instructions above, the computational formula is given directly as follows:

$$d(\bar{V}, \tilde{V}) = \begin{cases} \sum_{r,q} \sum_{j=1}^{l} |\bar{p}_{rj} - \tilde{p}_{ql}| & p = 1 \\ \sum_{r,q} (\sum_{j=1}^{l} |\bar{p}_{rj} - \tilde{p}_{qj}|^2)^{1/2} & p = 2 \\ \sum_{r,q} max(|\bar{p}_{rj} - \tilde{p}_{qj}|) & p = \infty. \end{cases} \tag{6}$$

So far, the definition of matching may be given, i.e., if $\tilde{v_j}$ is the matching of $\bar{v_i}$ in $\tilde{V}$, if and only if

$$\phi(\bar{v_i}, \tilde{v_j}) = \frac{d(\bar{v_i}, \tilde{v_j})}{min_{\tilde{v_k} \in \tilde{V} - \tilde{v_j}}(d(\bar{v_i}, \tilde{v_k}))} \leq \tau. \tag{7}$$

Thereinto, τ is the threshold value set up in advance. Only if $\phi(\cdot) \leq \tau$, does it hold that the two feature vectors are matching.

Define similarity between $\bar{V}$ and $\tilde{V}$ as $s(\bar{V}, \tilde{V})$,

$$s(\bar{V}, \tilde{V}) = \sum_{\tilde{V}, \phi(\cdot) \leq \tau} 1. \tag{8}$$

When the image information of invisibility requestors or visibility requestors is matched with photos taken by participants in the system, the threshold value η of similarity may be set up in advance. As for images of $s(\bar{V}, \tilde{V}) \geq \eta$, corresponding treatment shall be conducted, i.e., fuzzy processing is required when the result is invisibility requestors, while corresponding treatment is not required and the image information may be reserved when the result is visibility requestors.

- Step 5: Computation of distance of privacy protection. Based on Random Number Agreement and Scramble code generation put forth in article [19], it can be guaranteed that the computation on similarity mentioned in Step 4 (i.e., computation of distance) is conducted in a safe manner with privacy protection.

4.2 Privacy Protection Mechanism for Passerby

As far as passersby are concerned, because they do not actually participate in the system, the information about them is not stored on the cloud in the system; during the matching process in the previous section, there would be no identity information for some persons contained in photos taken by participant, i.e., there are some persons in a photo who are neither invisibility requestors nor visibility requestors. In fact, this phenomenon occurs due to the following two circumstances:

- (i) There is no passersby in a photo taken by participants, but due to the setup of threshold value τ and η, the portrait with low similarity would be directly considered dissimilar, i.e., there is passersby through system identification. However, the occurrence of this circumstance may be tolerant within a certain error range.
- (ii) There is passersby indeed in a photo taken by a participant, and their image information is not stored on the cloud.

No matter which circumstance mentioned above occurs, in order to prevent an image of a passersby from being invaded, fuzzy processing needs to be conducted directly, so as to protect the privacy of people in (or out of) the system to the maximum extent.

4.3 Discussion

The health monitoring mechanism for the special group involves protecting the privacy of group members of others indirectly involved. The advantages of safety precautions are as below. When conducting analysis for the special group, pictures taken by participants are needed. Since there would be people other than users in the pictures, some people may be willing to appear in the photos and to share their image information, but there would be others who regard shielding their image information and privacy protection as important and who need to be protected. The most intuitive practice is to erase this part of people from the photos. This paper proposes that users, participants and other people may mark whether or not their identities should be visible. Thus, after participants take photos of them and upload photos to the cloud, fuzzy treatment would be conducted to invisibility requestors. However, there may be people not participating in the system who are in the photos taken by participants, so there would be no identity marks for them. In this circumstance, the measure is to conduct fuzzy treatment for them directly. In this way, safety would be guaranteed as much as possible. However, there are some limitations for these kinds of safety precautions: for example, if an invisibility requestor wants to inquire about his or her photos put in the cloud, how to conduct a safe inquiry and how to restore the image is still an issue to be solved in future work.

5 Simulation Experiment

5.1 Experiment Setup

Our simulation experiment is set up as follows. The cloud is based on Linux system. The mobile devices selected by the client side include the portable computer and smart phone. Thinkpad X250 with CPU of 2.3 GHz and an internal storage of 8 GB and the window 10 system are utilized. At the end of a smart phone, HUAWEI 5s with CPU of 1.5 GHz and RAM of 2G is utilized. Three users are chosen. Generally speaking, each user would choose six scenes. For each user, there are six participants responsible for photographing each scene. But the number of invisibility requestors, visibility requestors and passersby is not limited. As for each scene chosen by the user, five photos will be taken, and thus there are thirty photos for one user each day, and user data collected over a week's time will be accumulated and analysed.

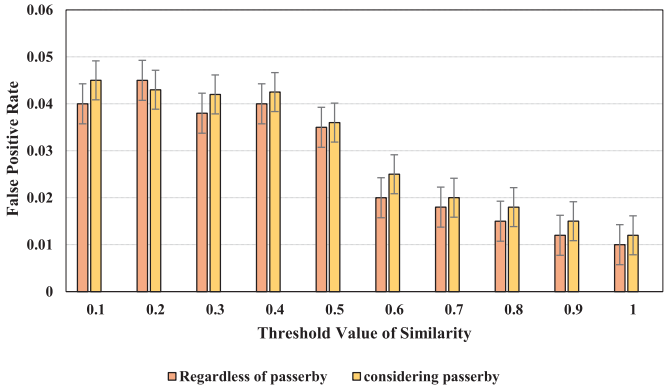


Fig. 3. False positive rate of system.

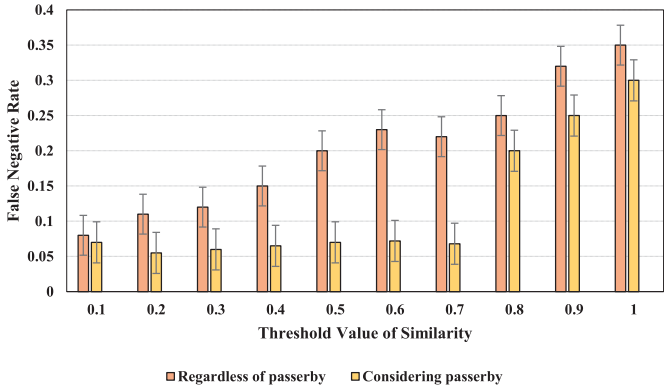


Fig. 4. False negative rate of system.

5.2 Performance Metric

In order to evaluate our health monitoring system, the measurement standards used are shown below.

- False positive rate α and false negative rate β. We use ture positive (TP), ture negative (TN), false positive (FP) and false negative (FN) to denote false positive rate, i.e., α and false negative rate, i.e., β, as follows

$$\alpha = \frac{FP}{FP + TN} \tag{9}$$

$$\beta = \frac{FN}{FN + TP} \tag{10}$$

5.3 Experiments Results

Figs. 3 and 4 illustrate the changes in false positive and false negative rates, with corresponding changes in threshold values. It can be seen from the figure that the false positive rate is generally controlled below 10 percent; in other words, the precision rate is higher than 90 percent. However, with changes in the threshold value, it can be seen that the false negative rate is generally controlled below 30 percent; in other words, the recall rate is at least 70 percent. Specially, if the threshold value is 0.5, the false positive rate reaches 0.07, and the false negative rate reaches 0.2.

6 Conclusion

This paper proposes a health monitoring mechanism based on photo crowdsourcing, for restoring the life state of the user and providing health monitoring for the special people. There are five kinds of people in the proposed system, including users, participants, invisibility requestors, visibility requestors and passersby. Invisibility and visibility requestors indicate their willingness for visibility or invisibility, while the image of passersby is fuzzy processed. Actual application scenes are taken into consideration in a simulation experiment, where three users are chosen as the target population, and image photographing of them is conducted for a week. False positive rates and false negative rates are evaluated, and the validity of the proposed system is verified through the simulations.

This work is a first step in the direction of safety protection for image crowdsourcing in the field of medical health monitoring. There are the following issues for further research and implementation.

1) More detailed incentive mechanisms. As the primary objective of this paper is to introduce the problem of privacy protection for a health monitoring mechnism based on photo crowdsourcing, incentive mechanisms do not receive focus. However, if this kind of application is to be implemented in earnest, a more reasonable incentive mechanism is required to attract more users and participants into the system, thus providing better health monitoring services. The participators in this system will consume their time and energy and provide the health supervision service for the user, and also will reveal their personal information (such as portrait information) to the system. Without the appropriate incentive mechanism, participators are unwilling to participate in the system, and further fail to provide the effective photographing service for the user for a long time, and fail to form the health supervision system based on photo crowdsourcing. In view of crowdsourcing incentive mechanism, Yang et al. [20] divided the incentive mechanism into two categories, i.e., crowdsourcer-centered, and user-centered. The former can be described by the stackelberg game theory, with the unique equilibrium point. The latter can be summarized as auction-based incentive mechanism. These different incentive mechanisms focus on different points. For the health supervision mechanism based on photo crowdsourcing proposed in this paper, it can be the user-based, and also participator-based. In the user-centered incentive mechanism, the user is a leader, while the participators are followers.
2) How to meet future searchability need when storage is conducted on the cloud for invisibility requestors. Users/participants may become interested in their photo information after fuzzy processing has been conducted. How to find their images among these invisible images and how to restore the images is a subject worth researching.
3) As the recognition of group members and others in pictures of users is based on facial recognition, when the recognition is not accurate enough, the implementation of the subsequent privacy protection mechanism would be directly influenced. We will continue to study these issues in subsequent works.
4) The suitable access control policy shall be formulated. For the health supervision mechanism based

on photo crowdsourcing proposed in this paper, the photos by participators are saved in the cloud. In the case of accessing the photos of users, the corresponding access control policy should be formulated, such as using the attribute-based confidential mechanism. Zhang et al. [17] proposed to deploy the access control policy by the ciphertext-policy attribute-based encryption (CP-ABE). Only the user meeting the definite attribute requirements can decrypt and accordingly get the access to photos.

ACKNOWLEDGMENTS

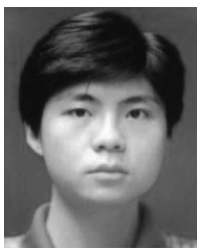
The authors would like to acknowledge the support from the Ministry of Science and Technology (MOST) of China under the grants 2016YFE0119000. Dr. Long Hu's work was supported by the National Natural Science Foundation of China (Grant No. 61572220). Prof. Jing Chen's work was supported by the National Natural Science Foundation of China under Grant No. 61272451 and No. 61572380.

REFERENCES

[1] M. Chen, Y. Ma, J. Song, C.-F. Lai, and B. Hu, "Smart clothing: Connecting human with clouds and big data for sustainable health monitoring," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 825–845, 2016.
[2] K. Hwang and M. Chen, *Big Data Analytics for Cloud/IOT and Cognitive Computing*. Chichester, U.K.: Wiley, 2017, ISBN: 9781119247029.
[3] Y. Zhang, M. Chen, D. Huang, D. Wu, and Y. Li, "idoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization," *Future Generation Comput. Syst.*, vol. 66, pp. 30–35, 2017.
[4] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn, "Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 54–61, Jan. 2017.
[5] M. Chen, J. Yang, Y. Hao, S. Mao, and K. Hwang, "A 5G cognitive system for healthcare," *Big Data Cognitive Comput.*, vol. 1, no. 1, pp. 2–16, 2017.
[6] M. Chen, P. Zhou, and G. Fortino, "Emotion communication system," *IEEE Access*, vol. 5, pp. 326–337, 2017.
[7] M. Qiu, Z. Ming, J. Li, K. Gai, and Z. Zong, "Phase-change memory optimization for green cloud with genetic algorithm," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3528–3540, Dec. 2015.
[8] J. Li, M. Qiu, Z. Ming, G. Quan, X. Qin, and Z. Gu, "Online optimization for scheduling preemptable tasks on IAAS cloud systems," *J. Parallel Distrib. Comput.*, vol. 72, no. 5, pp. 666–677, 2012.
[9] M. Chen, Y. Hao, C. Lai, D. Wu, Y. Li, and K. Hwang, "Opportunistic workflow scheduling over co-located clouds in mobile environment," *IEEE Trans. Service Comput.*, vol. 11, no. 3, pp. 549–561, May/Jun. 2018.
[10] K. Gai, L. Qiu, M. Chen, H. Zhao, and M. Qiu, "Sa-east: Security-aware efficient data transmission for its in mobile heterogeneous cloud computing," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 2, 2017, Art. no. 60.
[11] Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1339–1350, May 2016.
[12] W. Dai, M. Qiu, L. Qiu, L. Chen, and A. Wu, "Who moved my data? privacy protection in smartphones," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 20–25, Jan. 2017.
[13] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2010, pp. 136–149.
[14] W. Dou, X. Zhang, J. Liu, and J. Chen, "Hiresome-II: Towards privacy-aware cross-cloud service composition for big data applications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 2, pp. 455–466, Feb. 2015.
[15] Y. Zhang, W. Tong, and S. Zhong, "On designing satisfaction-ratio-aware truthful incentive mechanisms for k-anonymity location privacy," *IEEE Trans. Inform. Forensics Secur.*, vol. 11, no. 11, pp. 2528–2541, Nov. 2016.
[16] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy-preserving face recognition," in *Proc. Int. Conf. Inform. Secur. Cryptology*, 2009, pp. 229–244.
[17] L. Zhang, T. Jung, C. Liu, X. Ding, X.-Y. Li, and Y. Liu, "Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst.*, 2015, pp. 308–317.
[18] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 729–743, 2016.
[19] L. Zhang, K. Liu, X.-Y. Li, C. Liu, X. Ding, and Y. Liu, "Privacy-friendly photo capturing and sharing system," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2016, pp. 524–534.
[20] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *Biological Cybern.*, vol. 24, no. 3, pp. 1732–1744, 2016.

Long Hu received the BS and master's degrees from the Huazhong University of Science and Technology (HUST). He is working toward the PhD degree in the School of Computer Science and Technology, Huazhong University of Science and Technology (HUST). He was the publication chair for the 4th International Conference on Cloud Computing (CloudComp 2013). Currently, his research includes 5G mobile communication system, big data mining, marine-ship communication, internet of things, and multimedia transmission over wireless network, etc.

Yongfeng Qian received the MS degree from the Huazhong University of Science and Technology, China, in 2015. She is currently working toward the PhD degree in the Embedded and Pervasive Computing Lab led by Prof. Min Chen in the School of Computer Science and Technology, Huazhong University of Science and Technology. Her research includes internet of things, big data analytics, SDN, mobile cloud computing, healthcare, and security.



Jing Chen received the PhD degree in computer science from the Huazhong University of Science and Technology, Wuhan. He worked as an associate professor from 2010. His research interests in computer science are in the areas of network security and cloud security. He is the chief investigator of several projects in network and system security, funded by the National Natural Science Foundation of China (NSFC). He has published more than 60 research papers in many international journals and conferences, such as the *IEEE Transactions on Parallel and Distributed System*, the *International Journal of Parallel and Distributed System*, INFOCOM, SECON, TrustCom, and NSS. He acts as a reviewer for many journals and conferences, such as the *IEEE Transactions on Wireless Communication*, the *IEEE Transactions on Industrial Informatics*, *Computer Communications*, and GLOBCOM. He is a senior member of the IEEE.

Xiaobo Shi is currently working toward the DSc degree in the Embedded and PervasIve Computing Lab at the Huazhong University of Science and Technology. She is a associate professor at Henan Normal University where she worked as a teacher, since 1994. Her research interests include: body area network, cloud computing, internet of things, deep learning, etc.

Jing Zhang received the BS degree in electronic engineering from the Wuhan University of Technology, in 1997 and the PhD degree in communication and information engineering from the Huazhong University of Science and Technology (HUST), in 2010. He is currently an associate professor with the School of Electronic Information and Communications at Huazhong University of Science and Technology (HUST), China. He has worked at HUST since 1999. He was a visiting scholar with the University of Erlangen-Nuremberg, Germany, from November 2014 to November 2015. His research interest include the areas of mobile communications, green communications, and signal processing in wireless communications. He has published about 30 papers in refereed journals and conference proceedings and has been granted about 10 patents in China. He received the Best Paper Awards from IEEE GlobeCom Workshop 2014 and IEEE IWCMC 2015. He is leading several projects funded by NSFC, China MOST. He is also taking part in several international joint EU FP7 funded project. He is currently serving or has served as a reviewer for several international journals, such as the *IEEE Transactions on Vehicular Technology*, the *IEEE Journal of Selected Area on Communications*, *IEEE Access* et al. He also served as a reviewer for several international conferences, such as IEEE ICC2013, ICC2014, ICC2015, and IEEE GlobeCom 2014. He is a member of the IEEE ComSoc.

Shiwen Mao (S'99-M'04-SM'09) received the PhD degree in electrical and computer engineering from Polytechnic University (now New York University Polytechnic School of Engineering), Brooklyn, New York, in 2004. He is the Samuel Ginn Endowed Professor and director of the Wireless Engineering Research and Education Center (WEREC), Auburn University, Auburn, Alabama. His research interests include wireless networks and multimedia communications. He is on the Editorial Board of the *IEEE Transactions on Multimedia*, the *IEEE Internet of Things Journal*, the *IEEE Communications Surveys and Tutorials*, and the *IEEE Multimedia*, among others. He serves as a steering committee member for the IEEE ICME and AdhocNets, area TPC chair of IEEE INFOCOM 2016, technical program vice chair for information systems of IEEE INFOCOM 2015, and symposium/track co-chair for many conferences, including the IEEE ICC, the IEEE GLOBECOM, and the ICCCN. He is a Distinguished lecturer of the IEEE Vehicular Technology Society, and the vice chair—Letters and Member Communications of IEEE Communications Society Multimedia Communications Technical Committee. He was the recipient of the 2013 IEEE ComSoc MMTC Outstanding Leadership Award and the NSF CAREER Award in 2010, and also a co-recipient of the IEEE WCNC 2015 Best Paper Award, the IEEE ICC 2013 Best Paper Award, and the 2004 IEEE Communications Society Leonard G. Abraham Prize in the field of communications systems. He is senior member of the IEEE.