IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MISSION CRITICAL PUBLIC-SAFETY COMMUNICATIONS: ARCHITECTURES, ENABLING TECHNOLOGIES, AND FUTURE APPLICATIONS

Received August 20, 2017, accepted September 8, 2017, date of publication September 18, 2017, date of current version November 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2752176

A Proposal to Improve the Authentication Process in m-Health Environments

FRANCISCO D. GUILLÉN-GÁMEZ[1], IVÁN GARCÍA-MAGARIÑO[2,3], JAVIER BRAVO-AGAPITO[4], RAQUEL LACUESTA[2,3], (Student Member, IEEE), AND JAIME LLORET[5], (Senior Member, IEEE)

[1]Department of Research and Diagnostic Methods, Faculty of Education, Pontificia University of Salamanca, 37007 Salamanca, Spain
[2]Department of Computer Science and Engineering of Systems, University of Zaragoza, Escuela Universitaria Politécnica de Teruel, 44001 Teruel, Spain
[3]Instituto de Investigación Sanitaria Aragón, University of Zaragoza, 50009 Zaragoza, Spain
[4]Department of Computer Science, Madrid Open University, Madrid 28400, Spain
[5]Integrated Management Coastal Research Institute, Universitat Politècnica de València, 46022 València, Spain

Corresponding author: Jaime Lloret (jlloret@dcom.upv.es)

ABSTRACT One of the challenges of mobile health is to provide a way of maintaining privacy in the access to the data. Especially, when using ICT for providing access to health services and information. In these scenarios, it is essential to determine and verify the identity of users to ensure the security of the network. A way of authenticating the identity of each patient, doctor or any stakeholder involved in the process is to use a software application that analyzes the face of them through the cams integrated in their devices. The selection of an appropriate facial authentication software application requires a fair comparison between alternatives through a common database of face images. Users usually carry out authentication with variations in their aspects while accessing to health services. This paper presents both 1) a database of facial images that combines the most common variations that can happen in the participants and 2) an algorithm that establishes different levels of access to the data based on data sensitivity levels and the accuracy of the authentication.

INDEX TERMS Security, facial authentication, database, face images, m-health.

I. INTRODUCTION

The security on m-health services is relevant to ensure the appropriate usage of different applications through networks. In particular, the applications of distance services are based on the assumption that participants correctly indicate their identities when logining to the system. A possible way to validate the identities of participants is to apply facial authentication through the use of a webcam [1], [2]. In particular, facial authentication has already been suggested to be used in health and social services.

Our medical records contain a great deal of information about Privacy, Information Technology, and Health Care [3]. These records also contain confidential information about who and what we are—about topics such as fertility, abortions, emotional problems and psychiatric care. These data must not be disclosure and the access to the information must be controlled. The importance of identifying patients within m-health systems has been increasing not only for protecting privacy but also for controlling the right access to the service (if a fake user is not authenticated, the insurance company could be providing the service to another person). Typical security requirements of m-health systems should include among others confidentiality, effective user authentication and access control. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be [4]. Authentication systems must ensure that the data collected are associated with the correct participant and that only authorized individuals have access to these data and tools. Two-factor authentication (2FA) is used by the cybersecurity community in some cases [5]. Specially, it should be considered when sensitive data are accessed. Some authors use as the second category eye scans or voice recognition [6]. In our case, we work with face recognition, establishing a three-level algorithm that lets users access to the data depending on the authentication accuracy.

In online health services, the authentication of patients has become a need for preventing patients from making frauds and ensuring that the virtual patients are who they claim to be [7]–[9]. Therefore, each user plays an important role in his/her care process, where (s)he must be diagnosed, identified and verified correctly [10], [11]. Nowadays, m-health systems only provide the authentication of the user using the username and password at the beginning of the session.

However, during the rest of the access users are without supervision, what can increase the susceptibility to fraud [12]. Furthermore, this type of access provokes disadvantages to control the privacy in the access to the system. Therefore, a solution for this disadvantage could be the use of facial authentication systems in real time.

Jain and Nandakumar [13] assert that biometrics is one of the methods of individual authentication. It means the automatic recognition of a person based on their physiological features or behavior. In comparison with other biometric systems like the iris, fingerprint or the retina, facial authentication has a better acceptance by users [14] and does not require specialized equipment for the data acquisition.

In general, the operations of biometric systems are normally similar, and can be defined with two phases. The first one is that the person must be registered in the system. During the process of registration, the system captures the characteristic feature of the person (e.g. facial image), and it processes it to create an electronic representation called ''reference model'' or ''training model''. The training model must be stored in a database. The second phase of the biometric system consists in recognizing the person. The user does not inform the system what are their identity and it processes it to create the ''live model''. After that, the biometric software compares both models (reference model and live model) to determine the identity of the person in the database.

Improving the security of the m-health systems is an important requirement with the purpose of giving greater trust to the stakeholders involved in the process: doctors, insurance companies, patients, and so on. This aligns with our previous works that present different ways of including security in m-health systems. We proposed a mechanism to include data encryption in mobile-health applications [15]. We also presented an architecture for improving security in m-health services based on cloud storage and services [16]. In addition, we have developed m-health applications, such as SapoFitness app [17], which monitors the weight of users and suggests them daily exercises and some diets, in order to reduce their obesity or keep them with a healthy life style.

The application of biometric technologies could be useful for improving the security of m-health systems. However, some existing biometric authentication systems omit the appropriate security mechanisms for some kinds of malicious opponents. Some authors state that there is still a series of problems that must be resolved before achieving a totally anonymous identity in biometric authentication and the protection from some common attacks [18], [19].

In order to improve this situation, Mayron *et al.* [20] and He *et al.* [21] proposed a series of techniques and ways to be robust for some common kinds of attacks. Das *et al.* [22] proposed a light-weight biometric-based authentication scheme for hierarchical wireless body area networks that prevented attacks such as denial of service, privileged insider, and man in the middle. Ohana *et al.* [23] introduced 'honey faces': the concept of adding a great group of synthetic faces (indistinguishable from real) in the biometric password file. This password protects the privacy of users and increases the security of the system without affecting the accuracy of the authentication.

In this line, Cherrat *et al.* [24] proposed a learning system for facial authentication algorithm based on a system called 3SD ''Security and Surveillance System for Drivers''. This system is based on intelligent sensors and cameras which constantly monitor the vehicle environment and the driver behavior to detect potentially dangerous situations. The learning system of face recognition facilitates the early detection of sleep among other situations. Specifically in the field of Mobile Healthcare (mHealth), Wazid *et al.* [25] carried out a taxonomy of security protocols for mHealth systems that is based on the supported characteristics, possible attacks, and computation and communication costs.

Focusing on this research field, this work proposes the design and evaluation of a database of facial images. This database could be used to validate and ensure the precision of different software applications for facial authentication. Moreover, an open-source facial authentication application called OpenFace was used in order to determine the level of effectiveness in the identification and verification of the user. Furthermore, we propose an algorithm to establish different data privacy levels depending on their sensitivity.

In brief, the contribution of this work is two-fold. First, a novel database of photos has been collected to train facial authentication algorithms to be robust for variations in rotations, distance, expressions and accessories. This can be the basis for improving facial authentication algorithms in the next years. Second, this work presents a proposal for including facial authentication for conforming a 2FA mechanism for improving the security in the access to health data in m-health environments.

The rest of this article is structured as follows. Section II reviews facial databases proposed in the literature. Section III describes the details of the database ''FACEIMAGES'' that we have created. Section IV introduces the experiments of the presented database with an existing facial authentication application. Section V proposes a security approach for m-health systems. Finally, section VI outlines the conclusions and future research lines.

II. RELATED WORKS

In the field of the biometrics and in the case of the facial authentication, the databases of facial images have got a relevant place, and are focused on the evaluation of different algorithms of facial authentication. Some of the databases cannot be considered as superior to others, since each of them is designed to test different aspects of recognition and consequently has their own strengths and weaknesses.

One of the biggest databases was FERET with 1,199 participants with a maximum of 20 poses per user, considering two different expressions and two different lighting conditions [26]. Others, for example, are focused specifically on the variation of the capture conditions of the pose and the lighting [27].

TABLE 1. Specfic features of the OST relevant facial image databases.

	ORL	AR FACE	M2VTS	YALEB	FRAV2D	CASPEAL	KINECT FACE	NCKU
Year	1994	1998	1999	2001	2004	2008	2014	2014
Users	40	126	37	10	109	1040	52	90
Resolution (pixels)	92x 112	768x 576	286x350	640×480	320x 240	640×480	640x480	640×480
Lighting changes	✓	✓		✓	✓	✓	✓	
Rotations			✓		✓	✓	✓	✓
Different backgrounds	✓					✓	✓	
Different facial expressions	✓	✓		✓	✓	✓	✓	
Gender							✓	
Age							✓	
With or without glasses	✓	✓		✓		✓	✓	
With or without scarf		✓						
With or without cap		✓				✓		
Distance variation						✓		

For instance, Du [28] decided to use three databases. (1) 896 images of 126 people of the database AR Face Database [29]; (2) 600 images of the database M2VTS (Multi Modal Verification for Teleservices and Security applications) [30], and (3) 530 images of facial expressions of the American sign language.

At the same level, Lin [31], decided to use photographs of two databases already existing: on one hand, the database of Olivetti Research Laboratory (ORL), and on the other hand, the database of facial detection of NCKU (National Cheng Kung University). The ORL database contains pictures that have been taken under some controlled lighting conditions and background. The size of all these pictures is 92 × 112 pixels, with 256 levels in the gray scale for each pixel. NCKU database contains 660 different pictures of 90 people. These databases used five different images with the same type of lighting, different facial expressions, and twirls on the face. As a characteristic feature, these databases used a gray scale of color in their pictures.

Furthermore, Zou *et al.* [32] used two databases already created in their experiments: on one hand, the CASPEAL database contains 99,594 pictures of 1,040 people with different poses, expressions, accessories and lighting [33] and on the other hand, the database YALEB, with images of 10 people with 63 different types of lighting [34].

However, most of the existing databases have different limitations, like the amount of images per person. Normally, researches opt to create databases with lots of people, but the number of images of each person is low. By contrast, Min *et al.* [35] created a new database of photographs (KINECT FACE) with a sample of 52 users, using a meta-data file, with different information data about the participants, like for example: (1) the gender information; (2) year of birth; (3) with or without glasses. The authors state that all the images were taken under the same conditions, but there are not restrictions on clothes, make-up or hairstyle of the participants. Among other conditions taken into account to capture the photographs, they decided to put a white board behind each user with a distance of 1.25m, with the purpose of producing a simple background, which it can be filtered easily.

In this line, Conde *et al.* [36] built a database with 2D and 3D images with metadata, which was called FRAV2D [37]. In its first version, a group of 51 subjects were scanned with 14 different captures of images per subject, depending on the type of rotation and lighting. The total of captures of images was 714. Later, the database was made with 105 people with 16 different captures per person: four front images, eight different rotations with different directions and grades, two gestures and two different lighting conditions. The participants were chosen between students, teachers and staff who worked at university.

Moreover, other authors have investigated about the resolution of the photographs that the database must have, with the purpose of achieving a successful facial recognition. For instance, Farshchi *et al.* [38], carried out different analyses about the average time for detecting a user in the picture with different types of resolutions. The results showed that for a resolution of 460 × 680, the average time of detection was 0.8s; for a resolution of 800 × 600, the average time was 0.9s; for a resolution of 1,024 × 768, the average time was 1s; and for a resolution of 1,152 × 864, the average time was 1.2s. The average level of authentication was 92,7%. With the purpose of classifying the characteristics and options that each database offers, table 1 determines the most relevant features of the aforementioned databases.

A. FACIAL AUTHENTICATION VS. OTHER BIOMETRIC METHODS

While some biometric methods can require certain voluntary action from the patient, the facial authentication can be used passively. Braz *et al.* [39] compared different biometric methods, including the facial authentication, fingerprint and iris. Lassmann [40] performed different field tests about these methods and determined that the fingerprint recognition was the most used, followed by the iris detection and the facial recognition. However, some of these methods present some deficiencies in comparison with facial authentication.

Regarding the data acquisition, it is easier to obtain high quality facial images than appropriate fingerprints. For example, there are some disadvantages when using the recognition through fingerprints. Some of those reasons include cut skin, bandaged fingers, callosity, dry or wet skin, use of moisturizing creams, sweat and transmission of germs [41], [42].

The iris scanner can provide a high effectiveness for the recognition of users, however, due to the iris is quite small, it needs a high-resolution camera in order to be able to be captured. Furthermore, the camera should be close in order to capture the iris and all this process is highly sensitive to the body movements [43]. These systems can fail when contact lenses are used, or when blinking at the time of taking the image. Moreover, there is a range of ocular diseases that affect the capacity of the iris recognition system to capture the proper image of the eye [44].

By contrast, a system about facial authentication only requires the front camera of a smartphone and without the need of a specialized equipment, because the field of view of the webcam is big enough to cover the range of facial faces of people [45]. The perception of a user about the usability of a biometric method is also an important factor. Jain *et al.* [46] highlighted the facial authentication as one of the best biometric methods which was thought to have a ''high'' acceptance from users, while the digital fingerprint recognition was thought to have a ''medium'' acceptance from users. Table 2 presents levels of accuracies of some of the existing research works about these three biometric methods.

Taking into consideration the results and conclusions from the different research works analyzed and compared, the facial authentication systems are presented as a possible alternative for the identification of patients with great results in accuracy, being a non-intrusive method and with the ease of data acquisition since nowadays most users have smartphones, normally with front cameras.

III. FACEIMAGES DATABASE

The design of a database for the facial authentication is a complex task, due to the big amount of factors that influence the conditions while getting the data. For this reason, a protocol is required to ensure that all the images of the people are comparable. A proof of this complexity is the large variety of existing two-dimensional facial databases and the absence of homogeneity between them [59], [60].

TABLE 2. Accuracies of some research works of three different biometric methods.

	Research by authors	Accuracy
Facial	Owayjan, Dergham, Haber et al., [47]	90.0 %.
	Farshchi & Toosizadeh [38]	92.7 %.
	Lata, Tungathurthi, Rao et al., [48]	85.0 %.
Iris	Ali [49]	99.9 %
	Sim, Asmuni, Hassan et al., [50]	98.6 %
	Raja, Raghavendra, Vemuri et al., [51]	85.0%
	Galdi, Nappi & Dugelay [52]	97.0 %
	Raja, Raghavendra, Busch et al., [53]	81.0 %
Fingerprint	Raghavendra, Busch & Yang [54]	97.0 %
	Xu, Zhou & Lyu [55]	75.0 %
	Hammudoglu, Sparreboom, Rauhamaa et al., [56]	67.0 %
	Khalil [57]	78. 2 %
	Bo, Zhang, Jung et al., [58]	77.0 %

In this work, we present a database as an addition to the rest of the existing facial databases, taking into account a novel set of combinations of characteristics of each of them, and deepening in those aspects that were not used by them and can also be useful for the facial identification and authentication. We have designed a database called ''FACEIMAGES'', and sections A and B respectively present its characteristics and structure.

The sample of participants of the database was composed of 23 potential users of m-health systems, who have signed an agreement to allow the use of their photos for creating FACEIMAGES and later on performing their corresponding biometric analysis.

Data security and privacy protection are two main factors that need to be taken into account for our database. In order to get it, some authors recommend different tips to avoid possible attacks [61], [62], [63]. For example, some researchers highlight the need for a dynamic security model and cryptographic algorithms that point to different levels of security and privacy for cloud computing [64]. Lodha and Dhande [65] and Akanji *et al.* [66] proposed to eliminate the threats of the system by some advices such as encryption, user identification, and access control, which ensure that all communications with databases and other objects of the system are in accordance with defined policies and controls.

A. CHARACTERISTICS

1) Webcam

In order to capture images of the participants with different poses, expressions, accessories and lighting conditions, we used a cam with a resolution in pixels of 630 × 475. Figures 1 and 2 show two examples of the different ways of capturing images in relation to the rotation of the face (25 degrees at rotation angles).

2) ACCESSORIES

In the facial authentication process, the use of accessories as glasses, hats, caps of scarves could cause great difficulties for

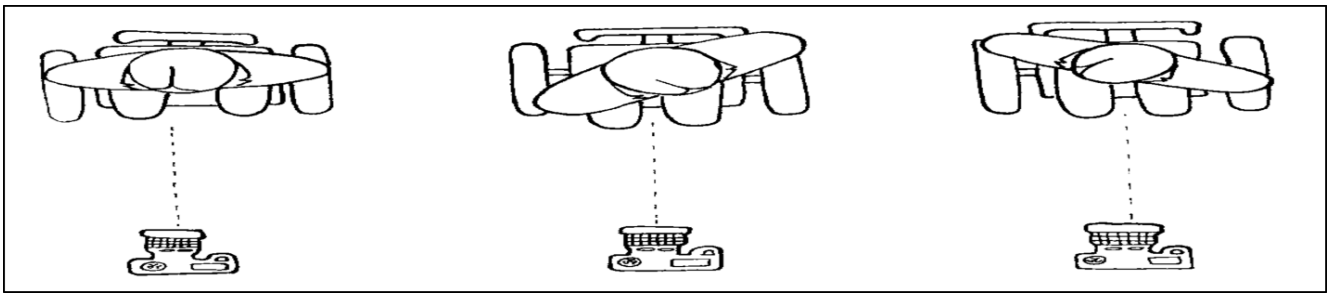

FIGURE 1. Example of how images have been taken with different face rotations.

FIGURE 2. Example of face participant rotation. Images taken from the FACEIMAGES database. (a) right position, (b) frontal position, (c) left position.

FIGURE 3. Example of a user images taken from FACEIMAGES database with different accessories: (a) wearing a scarf, (b) wearing a cap, and (c) wearing glasses.

face detection, because they could sometimes provoke facial occlusion. In this work, we have carefully used different types of accessories with the purpose of increasing the diversity of our database. With regards to glasses, the database used two types: normal glasses and sunglasses. It also used different hats or caps with different sizes and shapes. In addition, it considered either wearing a scarf or not. Figure 3 shows some examples of these kinds of variations.

3) FACIAL EXPRESSIONS

In order to capture the images, we took four types of facial expressions into consideration. Apart from the neutral expression, the participants were asked to show other three types of expressions: (a) smiling, (b) shouting and (c) closing the eyes, and opening the mouth (see examples in Figure 4). Friendly patients may smile while contacting through m-health services. The second type of expression could happen if the patient is in great pain. The last type of expression was carried out to consider emergency demands during the night, when they can be tired and sleepy. Different distances from the webcam

Other factor to take into consideration is that the participant is located in a correct distance from the camera. Thinking about this problem in the facial authentication, we have collected some images of the participants with different distances. Two distances were used: 0.5 and 1 m. Examples of these pictures are presented in Figure 5.

B. STRUCTURE OF THE DATABASE

A database of facial images must include different variations in order to try how reliable the algorithm of the software of facial authentication is in different conditions. Due to this, thirty variations were used in order to build our facial database. Table 3 shows all the combinations considered in this database for each participant.

FIGURE 4. Example of a user images taken from FACEIMAGES database with different facial expressions: (a) smile, (b) scream, and (c) yawn.

TABLE 3. Combination of features of face images in the database faceimages.

User									
Rotation - Neutral pose									
Distance	Left					Right			
Close (0,5m)	✓					✓			
Far (1m)	✓					✓			
Expressions – Central rotation									
Distance	Neutral			Smile			Scream		Yawn
Close (0,5m)	✓			✓			✓		✓
Far (1m)	✓			✓			✓		✓
Accessories									
Distance	Glasses			Scarf			Cap		
	Left	Center	Right	Left	Center	Right	Left	Center	Right
Close (0,5m)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Far (1m)	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 5. Example of a user images taken from FACEIMAGES database with different distances from the webcam: (a) close, and (b) far.

IV. RELIABILITY OF OPENFACE MEASURED WITH THE DATABASE FACEIMAGES

Nowadays, OpenFace is one of the most popular free applications for facial authentication. Amos*et al.* [67] have been the creators of OpenFace through Carnegie Mellon University (CMU) under the license of Apache 2.0. OpenFace is an open-source based project in a researching project of Google.

Baltrušaitis *et al.* [68] explain that it is necessary to introduce the information of each person in OpenFace previously (name and a minimum of ten pictures of the person) so that OpenFace could learn how to distinguish each person in base of their features. In this way, once the information of several people is introduced, the system is able to find out who is who in real time.

It is worth mentioning that the same database of images should be used for comparing several tools in order to ensure the reliability of comparisons. For this reason, we have created our own facial database, so it could be used in the identification and facial verification of any experiment.

In general terms, a system of biometric identification uses any of the physiological characteristics to identify a person, in our case, the face of a person. In the classifying tools, we could distinguish different types of percentages which determine its quality. Specifically, these parameters could be applied to the systems of facial authentication. Due to this fact, it is defined as (1) true positive (TP), the images where the right user appeared in the picture and the system identified him correctly, as (2) false positive (FP), the photos where a false user appeared and the system authenticated him erroneously, as (3) true negative (TN) where there was another false user and the system detected the usurpation effectively and (4) false negative (FN) where there was the right user but the system detected a usurpation.

For our analysis, we have used different measures: (1) sensitivity, the percentage of times that the user was authenticated correctly in the true cases; (2) specificity, percentage of cases which the system detected usurpations in the false cases; and (3) accuracy, the percentage of times that the system provided a correct result in all the

TABLE 4. Percentages obtained in relation to the face rotation.

Rotation - Neutral pose			
Distance	Parameters	Left	Right
Close	Analyzed	78.26	86.96
	Sensitivity	88.89	100
	Specificity	89.47	70.00
	Accuracy	89.19	85.00
Far	Analyzed	86.96	86.96
	Sensitivity	85.00	100

TABLE 5. Percentages obtained in reltion to different facial expressions.

Expressions – Central rotation					
Distance	Parameters	Neutral	Smile	Scream	Yawn
Close	Analyzed	100	100	100	100
	Sensitivity	100	100	100	69.57
	Specificity	56.52	60.87	56.52	82.61
	Accuracy	78.26	80.43	78.26	76.09
Far	Analyzed	100	100	100	100
	Sensitivity	100	95.65	95.65	65.22
	Specificity	56.52	73.91	69.57	82.61
	Accuracy	78.26	84.78	82.61	73.91

TABLE 6. Percentages obtained in relation to different accessories.

Accessories										
		Cap			Scarf			Glasses		
Distance	Parameters	Left	Right	Center	Left	Right	Center	Left	Right	Center
Close	Analyzed	52.17	56.52	82.61	82.61	91.30	100	43.48	60.87	95.65
	Sensitivity	50.00	84.62	100	89.47	100	100	60.00	50.00	59.09
	Specificity	100	76.92	47.37	77.78	70.00	52.17	81.82	69.23	68.18
	Accuracy	75.00	80.77	73.68	83.78	85.37	76.09	71.43	59.26	63.64
Far	Analyzed	52.17	47.83	82.61	95.65	100	100	65.22	56.52	100
	Sensitivity	75.00	100	100	90.91	100	100	26.67	46.15	56.52
	Specificity	100	81.82	68.42	80.95	77.27	65.22	87.50	84.62	86.96
	Accuracy	87.50	90.91	84.21	86.05	88.89	82.61	58.06	65.38	71.74

possible cases. In some cases, OpenFace was not able to detect a face in the image, so it outputted an error message without classifying the image. We reported this fact by indicating the percentages of images that OpenFace was able to analyze in each case (denoted as ''analyzed'' in the corresponding tables).

In tables 4 to 6, one can observe the different features obtained taking into consideration the different combinations of our database. All these tables consider two values related to the distance from where the pictures were taken (close-far).

With regards to face rotation, in the table 4 we could highlight how OpenFace presents a higher percentage of sensitivity in right rotation of the face than in the left rotation, both in close and far distance (100 against 88.89, and 100 against 85.00 respectively). However, OpenFace has a higher level of accuracy in the left rotations than in the right rotations, although both percentages are very close for both distances (between 85 and 90%).

With regards to the facial expressions, it could be observed in table 5 how the biometric software has percentages of sensitivity and ability of analyzing close or the same as 100% for close distances, although for far distances the sensitivity has a percentage much lower in the photos with yawn expression face. With regards to the level of accuracy of OpenFace for all kind of expressions and for both distances, all levels showed results around 74-85% approximately.

Taking the accessories into consideration, in table 6 we can do several analyses. For example, in relation to the level of accuracy, it is observed that if the user wears a cap or a scarf, the level of accuracy is higher in far distances than in close distances for both rotations (percentages between 83% and 91%). However, if the user wears glasses, the level of accuracy is slightly better in close distance than far distance. Also, the lowest accuracy is experimented if the user is situated far to the webcam, his face is rotated to the left, and he wore glasses.

TABLE 7. Means obtained in relation to differet measurement values.

	Average
Analyzed	83.48
Sensitivity	82.95
Specificity	74.66
Accuracy	78.87

Table 7 shows the average of the four measures. It is worth indicating that OpenFace detects better TP than FN. However, the accuracy of this system is close to 80%, which is an appropriate level for this kind of system.

V. SECURITY SYSTEM IN THE ACCESS TO THE HEALTH DATA

This work presents a security system for the access of health data. Section A presents the security model of this system. Section B introduces the mechanisms to access the data regarding three different levels of data. Section C integrates the use of FACEIMAGES in this proposal, and discusses some illustrative examples.

A. Security model

The confidentiality and invasion of privacy are two aspects of great importance when working in health-related scenarios. The CIA triad of confidentiality, integrity, and availability is at the heart of information security. Among these aspects, we center our study in the proposal of a protocol to maintain data confidentiality and user's privacy, considering attacks similar to the ones proposed by Simoens *et al.* [18]. Our protocol uses a two-factor authentication that allows authorized users to access to the data. Also, a privacy algorithm is presented in the next subsection in order to protect sensitive data with a strongest level of authentication

The proposed protocol establishes three phases in the authentication process. In the first one, the user must be physically identified. Therefore, the user goes physically to the place where the identification and user register are done. Once the user has been physically identified, an account is created for that user. This account registers among others the following user's data: user's identification id, personal data such as telephone number, first level authentication user's data (user and password), and second level authentication user's data (facial images with variations). The ''necessary photos'' for following authentications are taken physically by the system. This protocol step can be viewed in Figure 6.

When the user's account has already been created, they can send new facial variations of them using the online system, always after going through the three phases protocol and with a right strong authentication process.

The second phase is carried out by the user when they want to access to their data or health-services. In this moment, a 2FA process begins. In order to exchange the authentication first level user's data, a session key is established. In our protocol, the server must own a server's certificate certified

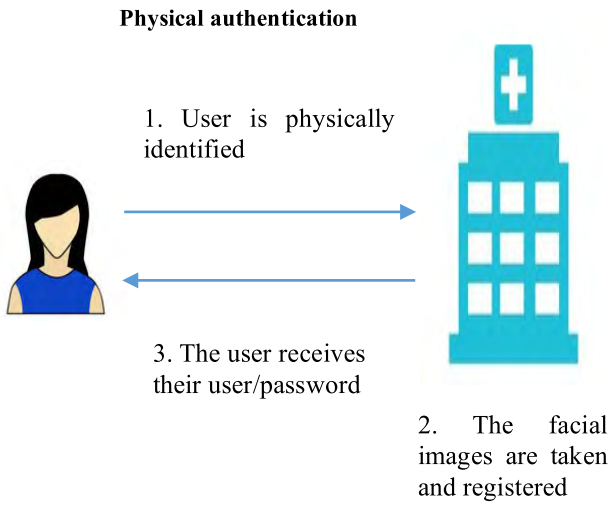

FIGURE 6. Initial physical authentication.

by approved entities of recognized prestige. That certificate is sent to the client. The client verifies server's identity and generates the session key. The session key is cyphered by the public server's key and sent to the server. From this moment, all communications among server and client are cyphered with this key. One this process has been carried out, the user will send their first level authentication data, that is, user and password. This process can be observed in Figure 7. If the process is right, the second authentication level process begins.

In the third phase, the second level authentication process is done. In order to provide a strong authentication system, this asks the user to validate two different facial images variations (example: right position and left position). These variations are analyzed with the biometrical model of the user stored in the database. The user may change a variation to validate, only if this involves accessories (for example they do not wear glasses in that authentication and want to try another variation). If the value of the comparison of one photo with the database is higher than an 'x' threshold and the other one is at least above a ''z'' threshold then, access to level 2 data is provided for that user. If the level is higher than the 'y' threshold for one photo an at least above a ''w'' threshold, the system grants access to level 1 data. Thresholds x, y, w and z can be calibrated after the system is deployed and tested with some users. Figure 8 shows the process of this third phase. The data levels are introduced in the next subsection.

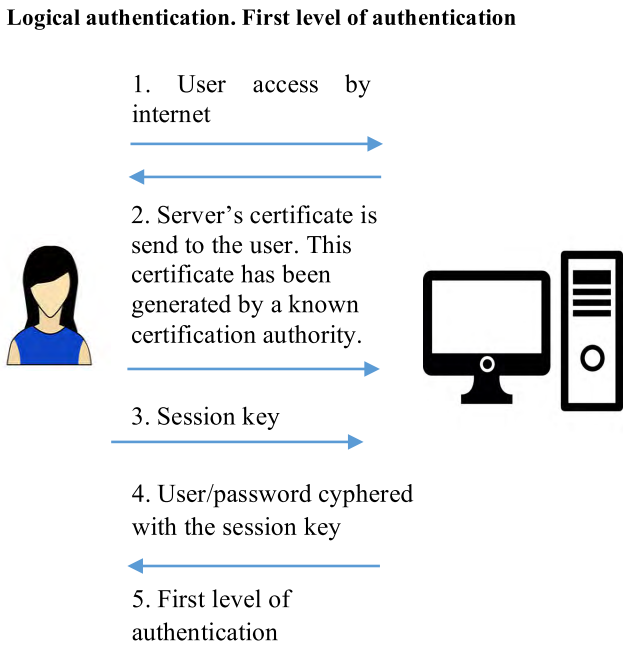

FIGURE 7. First level of logical authentication.

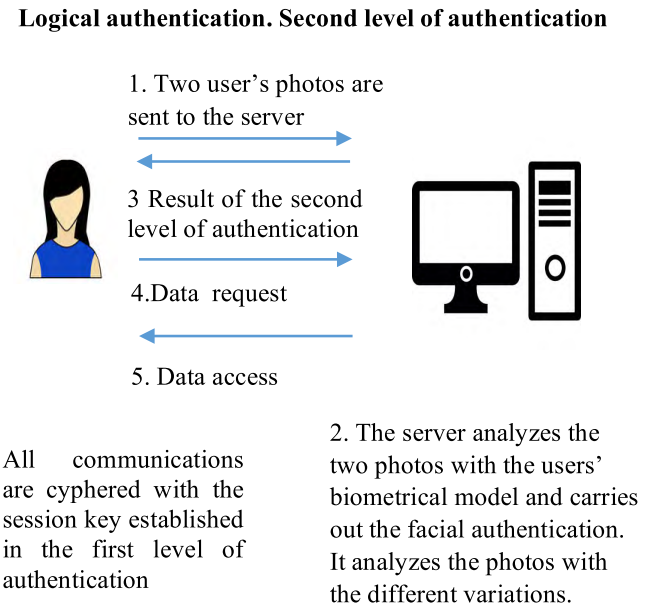

FIGURE 8. Second level of logical authentication.

Our system is protected from attacks based on insufficient authentication. For that purpose, it denies the access to sensitive content or functions depending on the authentication result. Also, if the authentication is not valid in three tries the system blocks the possibility of new tries. In this case, in order to protect the system against brute force attack, we propose a protocol similar to the user with credit cards. The user will receive an alert informing them, as "some illicit" access could have been tried in their name. Then, the user could call to the medical center or access to their online account to take the proper measures to avoid illegal access and to protect their privacy.

Moreover, in order to protect the system against weak password recovery validation, we established a protocol of challenges based on two rounds. The first round is a list of questions that the user registered when creating their account and profile, the second round of challenges is based on a facial image authentication, where some variations are proposed to the user in order to validate at least two different profiles. In that way, again, a two-factor validation process is established in order to recover the password.

Privacy and integrity in the transmission are guaranteed by both using a hash function generated over the transmitted data and using symmetric cryptography to protect the data sent. In this way, some of the attacks against which the system is protected are (1) eavesdropping, as the data are cyphered; (2) data modification, identity spoofing and password-based attacks, as the system uses strong authentication; (3) denial of service, considering that only three consecutive authentications are allowed; (4) man in the middle, through the use of server's certificate and strong authentication process; (5) compromised key attack as the session key is re-generated in each connection, and (6) sniffer attack, since the data are protected. Strong cyphered algorithms are used in order to avoid attacks based on algorithms' weaknesses.

The current approach stores all the images in a secure way. For this purpose, the PNG photo files are encrypted with the mechanism proposed by Yuang *et al.* [69]. Notice that with this mechanism, the faces cannot be recognized in the photo files after the corresponding encryption. The decryption requires multiple keys that are sent in different messages. Users registers its initial true images double-checked by human in a face-to-face meeting in which the use shows its national identity card. These images are stored in the server of the health center, and then these photos are transferred to another server that actually checks the access of users. In this way, the original photos are duplicated in two different servers in case some errors happen. The transmission from server to server is performed following the approach introduced by Boopathi *et al.* [70], whose authors demonstrated its robustness against collision attack, the chosen prefix collision attack, and the plaintext attack.

B. SECURITY LEVELS FOR DIFFERENT KINDS OF DATA

In order to maintain users' privacy in the access to the health system services and information, and depending on the accuracy of the authentication we have designed an algorithm in which personal data access is established based on several levels. When accessing to health data, our approach performs a strong authentication process. We define strong authentication as a way to ensure that each person who identifies themselves in a system is actually who they claim to be by, verifying their identity in an accurate way [5]. Among the three ways of identifying the users: (a) something the person know, (b) something the person own and (c) something that the person is, we have selected two authentication processes corresponding to (a) and (c) factors. In our proposal, any system's user must carry out at least an identification based

on the introduction and validation of user/password data. Moreover, if they require to access to more sensitive data, a facial authentication must be carried out.

In our model, data are classified depending on their sensitivity. We establish three levels. In order to determine the sensitivity of the data, we have studied the Spanish organic law on the protection of personal data [71]. From the study carried out, we have selected and classified the different types of health data and those that can be treated within a public health system into the following levels:

Level 1 Data:

- Data related with ideology, health or sexual life that are not possible to be including in the level 3.
- Data arising from acts of gender-based violence.

Level 2 Data:

- Data that offer a definition of the personality and allow evaluating certain aspects of it or related with people behavior.

Level 3 Data:

- Data that are used for the sole purpose of making a money transfer to entities, in which the person is an associate or a member.
- Data containing health data, which refers exclusively to the degree or condition of disability or the simple declaration of invalidity, due to the fulfillment of public duties.

Both patients and doctors or any person involved in the health process that need to access to the data and services, is authenticated in order to set the proper permissions. Authentication made by user and password data allows access to level 3 data. To access 1 or 2 levels data, a second authentication is required. This second authentication level implies a facial authentication. In this way, the authentication requirements are the following ones:

Privacy level 1 and 2: password and facial authentication.

Privacy level 3: password authentication

Figure 9 shows the diagram about the process of authentication, in which the following terms have been used:

Pu1 (t): password authentication of user u1 in a time t

Fu1 (t): facial authentication of user u1 in a time t

As we have shown in previous sections and due to the different user's variations in the process, different results can be obtained from performing a facial authentication. The current approach considers that a robust m-health system should provide an appropriate accuracy in the authentication for accessing the data of the different levels, considering different combinations of circumstances. For this purpose, we have presented a database of facial images that can assist designers of m-health systems in developing or selecting an appropriate facial authentication application.

C. INTEGRATION OF FACEIMAGES IN THE SECURITY SYSTEM FOR m-HEALTH AND ILLUSTRATIVE EXAMPLES

A different target threshold can be established for each of the first two data levels. As an example, we respectively propose

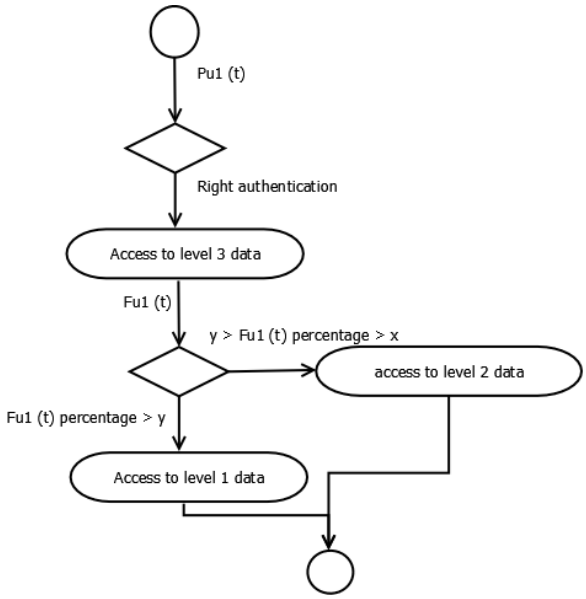

FIGURE 9. Process of authentication.

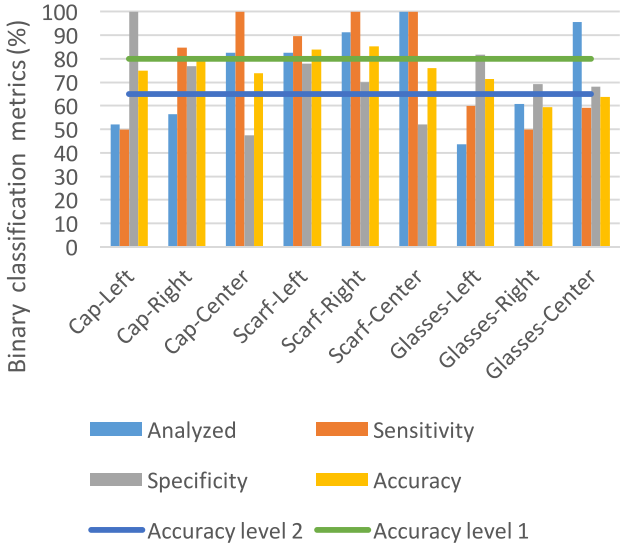

FIGURE 10. Access allowed when working in close-distance scenarios, with different accessories and rotations.

the following thresholds of accuracy for the second and first levels of security: x = 65% and y = 80%.

Figures 10 and 11 respectively present these thresholds in the charts of the average results of OpenFace application with the proposed FACEIMAGES database, in the different scenarios. More concretely, figure 10 presents the average results for some close-distance scenarios, and figure 11 does it for some far-distance scenarios, in both cases considering different rotations and accessories.

In order to better illustrate the application of the current approach, we illustrate the whole process with an example. When a private or public health organization has decided to integrate m-health on their services, a system must be developed and deployed for providing this service. One of the

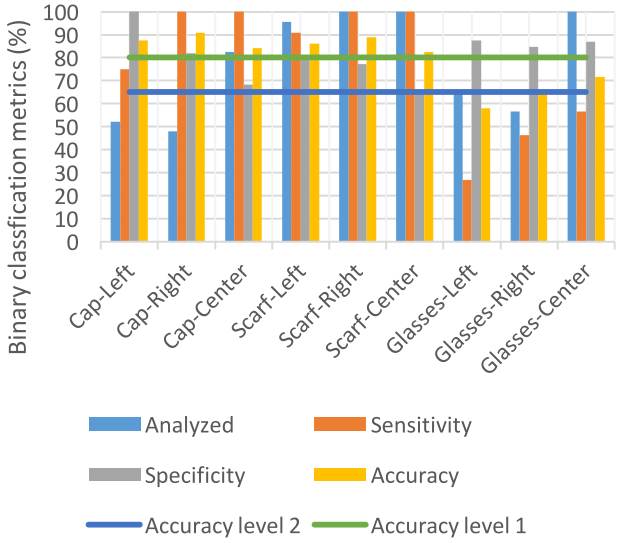

FIGURE 11. Access allowed when working in far-distance scenarios, with different accessories and rotations.

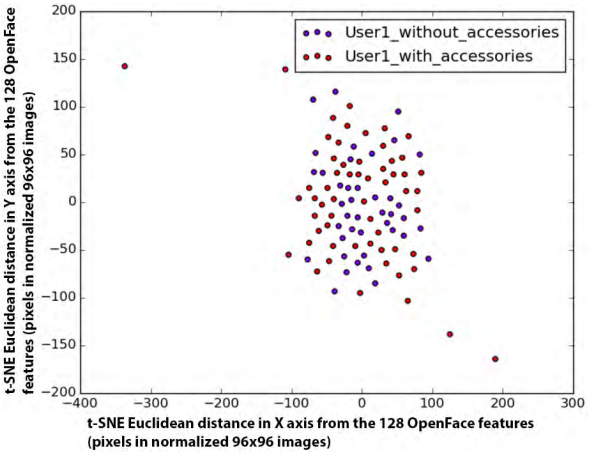

FIGURE 12. The t-SNE chart of the same user logged with two different usernames (the latter used when wearing accessories).

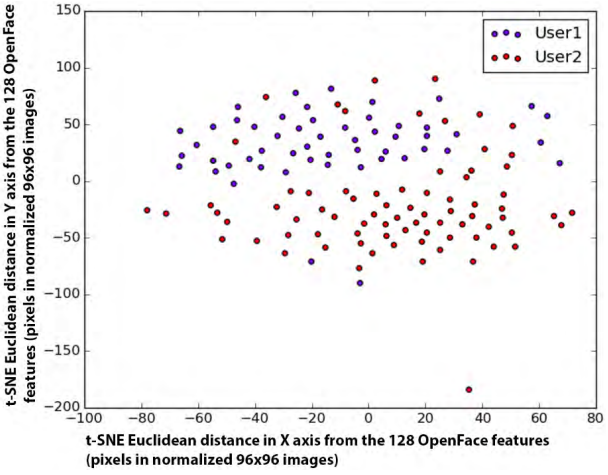

FIGURE 13. The t-SNE chart of two different users.

crucial aspects is to ensure the authentication security due to the high levels of confidentiality of their data. In this case, this work proposes a 2FA system, in which the second authentication mechanism is based on facial photographs taken from the cam of the corresponding mobile device. However, the system is recommended to be robust regardless of hindering aspects such as different rotations, expressions, accessories and distances. The engineer of the m-health system can assess the quality of the facial authentication application in all these possible scenarios with the proposed FACEIMAGES database. When the m-health system has been deployed, patients can start using it. First, they should register and provide some true face images for creating the reference model. Then, each time the user accesses, it introduces their user and password data, and show their face to the cam of their mobile device. The system takes a picture and analyzes it for granting access. In some cases, the system may need to take several pictures to decide whether to grant access, generally if the conditions are different from the ones in which the reference images were taken. If the system works properly, it will grant the user with access to the three levels. If there are some mismatches, the system may need more time for granting the user with access to the data of the highest level of security (i.e. level 1). If the system detects an attempt of usurpation after analyzing an enough large number of pictures, the system will alert the administrator and/or the real user so they can take the proper actions.

In order to show the effectiveness of this example, we simulated two different new scenarios. In the first scenario, a person accessed the system adopting different distances, accessories, rotations and expressions. We logged this user with two different usernames. The first username was used when he was not wearing accessories. The second username was used when he had some accessories on (i.e. cap, sun glasses, and scarf). OpenFace provided the t-SNE (t-Distributed Stochastic Neighbor Embedding) chart of Figure 12 for these two usernames. T-SNE is the dimensionality reduction technique that OpenFace uses to visualize the 128 dimensional features it analyzes. As one can observe, the system did not distinguish between the two usernames, as both belonged to the same person.

In the second scenario, we logged into the system two different users with different usernames. Both subjects were male and were close relatives (i.e. brothers). This may be a difficult scenario for the proper classification, since close relatives may have facial similarities. In addition, the system analyzed pictures of them, with different rotations, distances, accessories and expressions. OpenFace provided the t-SNE chart of Figure 13. One can observe that even for this scenario, the system properly classified most of the pictures. The spatial results of these different users were mostly allocated in different areas.

D. SECURITY ANALYSIS

In online systems, security can be compromised by either web attackers and network attackers. Each security system

can suffer different kinds of attacks regarding its type. The current approach is composed of two factors of authentication, the encrypted password and facial authentication. Since we use known encryption algorithms already validated, this discussion focuses on the possible attacks related with the facial authentication.

In facial authentication, the most relevant attack is the stealing of facial images. For example, a network attacker could try to intercept a facial image for later using it in the authentication. The presented system is secured from this attack in the following ways:

- The face images are encrypted to be sent through the network, so the stealer cannot intercept these during the network communication, as it would need to break the secure encryption algorithm.

- Even if the stealer could steal a facial image, the proposed authentication process could ask the user to adopt several specific poses from a large set. In other words, the proposed facial authentication mechanism could use different combination of poses as partial solutions, and then the stealer cannot enter by just stealing one of these partial solutions.

- The system can check whether the images are exactly the same from the one previously received, and only grant access to the new facial images different from the ones previously received. Normally, two real images are not usually exactly the same, as these normally vary. This approach is similar to detection of fake written signatures by assessing their duplicity. In this manner, the system needs to take a new original photo from the user each time. In this way, it prevents from the attack of intercepting and reusing stolen images.

Another possible attack is the extraction of facial images from social media and social networks. From this attack, the system can be protected with the following mechanisms:

- The user can upload a set of forbidden images. In case that the system detected any of these images, it would alert immediately the user. In this way, the user can upload all the images that they use in their social networks or appear in the social media.

- The previous mechanism could be compromised if for example a friend uploads an image of the user to a social network without him/her knowing, or simply the user forgets to upload certain images. For protecting from these situations, the system could incorporate an automatic search engine that searches for facial images of the user online and includes all these images in the list of forbidden images.

- In this kind of attack, the attacker would also need a complete set of different poses, since the system can ask for different poses, and the aforementioned mechanism of partial access solution would also increase the security.

- In all the wrong attempts, the system notifies the user so that they are aware of the these to take further security measures (e.g. resetting the password and updating the list of forbidden images).

Furthermore, the system includes the following protection mechanism for the illegitimate use of facial images:

- The user app only admits photos directly taken from the camera device for the authentication. Thus, for attempting to any of the two aforementioned kinds of attacks, the attacker would need to hijack the app, for being possible to correctly send images that are not directly taken from the camera of the device.

Finally, it is worth reminding that the system uses 2FA, so for entering the system, the attacker would need to break not only the aforementioned facial authentication protection mechanisms but also the encrypted password-based validated authentication.

VI. CONCLUSIONS AND FUTURE WORK

On the whole, the current work has presented a database of facial images for testing and comparing facial software applications and algorithms. This database has focused on the common variations of face images taken from potential patients. In particular, it considers different combinations of features such as the distance to the camera, the rotation, the different facial expressions (e.g. yawning) and accessories (e.g. scarf and glasses). This particular set of combinations is novel to the best of authors' knowledge in comparison to the existing databases of facial images. The current work has used this facial database to propose a secure approach for m-health systems. This approach incorporates a security model considering some of the most common attacks. This approach establishes different security levels for allowing patients to access to the health data based on data sensitivity levels.

This database was initially designed for comparing facial authentication applications for security in m-health environments. However, this database can be used for comparing this kind of applications for different purposes, such as (1) the customization of mobile applications regarding the user facially identified by the camera, and (2) the analysis of the trust models of cameras of mobile devices. This facial database is planned to be applied to compare a large set of facial authentication applications to determine which can be the most appropriate one for each domain.

In the future, the current work is planned to be extended in several ways. First, the proposed database of facial images is planned to be used to test 2FA mechanisms with facial authentication in the internet of things, for making the communication of certain kinds of health data more secure in this context. In the long-term, we also plan to add facial recognitions of emotions in the presented health access system. This can be useful for doctors to track the emotional evolution of their patients to detect side effects of some treatments from the psychological viewpoint and to know whether the patients may need psychological support. Furthermore, the database of facial images will be extended to include images with very low resolutions. In this way, the database will be useful for assessing the accuracy of facial authentication algorithms in analyzing images from very low-end and old devices, which are common in the developing world.

REFERENCES

[1] F. D. Guillén-Gámez, J. Bravo-Agapito, and I. Garcia-Magarino, "Students' perception of the importance of facial authentication software in moodle tools," *Int. J. Eng. Edu.*, vol. 33, no. 1, pp. 84–90, 2017.

[2] F. D. Guillén-Gámez, I. Garcia-Magarino, J. Bravo, and I. Plaza, "Exploring the influence of facial verification software on student academic performance in online learning environments," *Int. J. Eng. Edu.*, vol. 31, no. 6A, pp. 1622–1628, 2015.

[3] T. C. Rindfleisch, "Privacy, information technology, and health care," *Commun. ACM*, vol. 40, no. 8, pp. 92–100, 1997.

[4] N. Kalogeropoulos, I. Tzigounakis E. A. Pavlatou, and A. G. Boudouvis, "Computer-based assessment of student performance in programing courses," *Comput. Appl. Eng. Edu.*, vol. 21, no. 4, pp. 671–683, 2013.

[5] S. Arora, J. Yttri, and W. Nilsen, "Privacy and security in mobile health (mHealth) research," *Alcohol Res., Current Rev.*, vol. 36, no. 1, p. 143, 2014.

[6] P. Varchol, D. Levicky, and J. Juhar, "Multimodal biometric authentication using speech and hand geometry fusion," in *Proc. IEEE 15th Int. Conf. Syst., Signals Image Process. (IWSSIP)*, Jun. 2008, pp. 57–60.

[7] L. Shin, "How biometrics could improve health security," Fortune, Time Customer Service, Tampa, FL, USA, Tech. Rep., 2015.

[8] J. Drexler and C. J. Dyball, "Anti-fraud verification system using a data card," U.S. Patent 5 457 747, Oct. 10, 1995.

[9] A. E. F. Zuniga, K. T. Win, and W. Susilo, "Biometrics for electronic health records," *J. Med. Syst.*, vol. 34, no. 5, pp. 975–983, 2010.

[10] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[11] J. Bringer, H. Chabanne, and B. Kindarji, "Identification with encrypted biometric data," *Secur. Commun. Netw.*, vol. 4, no. 5, pp. 548–562, 2011.

[12] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: A grand challenge," in *Proc. 17th Int. Conf. Pattern Recognit. (ICPR)*, vol. 2. Aug. 2004, pp. 935–942.

[13] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *IEEE Comput.*, vol. 45, no. 11, pp. 87–92, Nov. 2012.

[14] P. J. Phillips, P. Grother, R. Micheals, D. M. Blackburn, E. Tabassi, and M. Bone, "Face recognition vendor test 2002," in *Proc. IEEE Int. Workshop Anal. Modeling Faces Gestures (AMFG)*, Oct. 2003, p. 44.

[15] B. M. C. Silva, J. J. P. C. Rodrigues, F. Canelo, I. M. C. Lopes, and J. Lloret, "Towards a cooperative security system for mobile-health applications," *Electron. Commerce Res.*, vol. 14, pp. 1–27, Oct. 2014, doi: 10.1007/s10660-014-9154-3.

[16] J. Lloret, S. Sendra, J. M. Jimenez, and L. Parra, "Providing security and fault tolerance in P2P connections between clouds for mHealth services," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 5, pp. 876–893, 2016.

[17] I. M. Lopes, B. M. Silva, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proença, "A mobile health monitoring solution for weight control," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, vol. 9. Nanjing, China, Nov. 2011, pp. 1–5.

[18] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 833–841, Apr. 2012.

[19] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[20] L. M. Mayron, Y. Hausawi, and G. S. Bahr, "Secure, usable biometric authentication systems," in *Proc. Int. Conf. Univ. Access Hum.-Comput. Interact.*, Jul. 2013, pp. 195–204.

[21] D. He, Y. Zhang, and J. Chen, "Robust biometric-based user authentication scheme for wireless sensor networks," *IACR Cryptol. ePrint Arch.*, vol. 203, pp. 1–15, 2012.

[22] A. K. Das, S. Chatterjee, and J. K. Sing, "A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks," *Adhoc Sensor Wireless Netw.*, vol. 28, nos. 3–4, pp. 221–256, 2015.

[23] M. Ohana, O. Dunkelman, S. Gibson, and M. Osadchy. (2016). "HoneyFaces: Increasing the security and privacy of authentication using synthetic facial images." [Online]. Available: https://arxiv.org/abs/1611.03811

[24] L. Cherrat, M. Ezziyyani, A. El Mouden, and M. Hassar, "Security and surveillance system for drivers based on user profile and learning systems for face recognition," *Netw. Protocols Algorithms*, vol. 7, no. 1, pp. 98–118, 2015.

[25] M. Wazid, S. Zeadally, A. K. Das, and V. Odelu, "Analysis of security protocols for mobile healthcare," *J. Med. Syst.*, vol. 40, no. 11, p. 229, 2016.

[26] P. J. Phillips, H. Wechsler, J. Huang, and P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image Vis. Comput.*, vol. 16, no. 5, pp. 295–306, 1998.

[27] T. Sim, S. Baker, and M. Bsat, "The CMU pose, illumination, and expression (PIE) database," in *Proc. 5th IEEE Int. Conf. Autom. Face Gesture Recognit.*, May 2002, pp. 46–51.

[28] S. Du, Y. Tao, and A. M. Martinez, "Compound facial expressions of emotion," *Proc. Nat. Acad. Sci. USA*, vol. 111, no. 15, pp. E1454–E1462, 2014.

[29] A. M. Martinez, "The AR face database," Computer Vision Center, Univ. Autonoma de Barcelona, Spain, Tech. Rep. 24, 1998.

[30] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, "XM2VTSDB: The extended M2VTS database," in *Proc. 2nd Int. Conf. Audio Video-Based Biometric Pers. Authentication*, vol. 964. 1999, pp. 965–966.

[31] W. H. Lin, P. Wang, and C. F. Tsai, "Face recognition using support vector model classifier for user authentication," *Electron. Commerce Res. Appl.*, vol. 18, pp. 71–82, Aug. 2016.

[32] W. W. W. Zou and P. C. Yuen, "Very low resolution face recognition problem," *IEEE Trans. Image Process.*, vol. 21, no. 1, pp. 327–340, Jan. 2012.

[33] W. Gao *et al.*, "The CAS-PEAL large-scale chinese face database and baseline evaluations," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 1, pp. 149–161, Jan. 2008.

[34] A. S. Georghiades, P. N. Belhumeur, and D. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 6, pp. 643–660, Jun. 2001.

[35] R. Min, N. Kose, and J.-L. Dugelay, "KinectFaceDB: A Kinect database for face recognition," *IEEE Trans. Syst., Man, Cybern. A, Syst.*, vol. 44, no. 11, pp. 1534–1548, Nov. 2014.

[36] C. Conde, R. Cipolla, L. J. Rodríguez-Aragón, Á. Serrano, and E. Cabello, "3D facial feature location with spin images," in *Proc. IAPR Conf. Mach. Vis. Appl. (MVA)*, May 2005, pp. 418–421.

[37] *FRAV2D: Face Recognition and Artificial Vision*. Accessed: Jul. 1, 2017. [Online]. Available: http://www.frav.es/

[38] S. M. R. Farshchi and S. Toosizadeh, "A safe authentication system for distance education," *Comput. Appl. Eng. Edu.*, vol. 22, no. 4, pp. 593–603, 2014.

[39] C. Braz and J. M. Robert, "Security and usability: The case of the user authentication methods," in *Proc. 18th Conf. Interact. Homme-Mach.*, Apr. 2006, pp. 199–203.

[40] G. Lassmann, "Some results on robustness, security and usability of biometric systems," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, vol. 2. Aug. 2002, pp. 577–579.

[41] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710–724, Feb. 2014.

[42] R. Saini and N. Rana, "Comparison of various biometric methods," in *Proc. Int. J. Adv. Sci. Technol. (IJAST)* vol. 2. 2014, pp. 1–7.

[43] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015.

[44] J. Daugman, "Results from 200 billion iris cross-comparisons," Comput. Lab., Univ. Cambridge, Cambridge, U.K., Tech. Rep. UCAM-CL-TR-635, 2005.

[45] Visidon Applock. (2017). *Visidon Ltd Teknologiantie 2*. Accessed: Jul. 29, 2017. [Online]. Available: http://www.visidon.fi/en/Home

[46] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[47] M. Owayjan, A. Dergham, G. Haber, N. Fakih, A. Hamoush, and E. Abdo, "Face recognition security system," in *New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering*. Cham, Switzerland: Springer, 2015, pp. 343–348.

[48] Y. V. Lata, C. K. B. Tungathurthi, H. R. M. Rao, A. Govardhan, and L. P. Reddy, "Facial recognition using eigenfaces by PCA," *Int. J. Recent Trends Eng.*, vol. 1, no. 1, pp. 587–590, 2009.

[49] M. A. M. Ali, "Biometric identification and recognition for iris using failure rejection rate (FRR)," Ph.D. dissertation, Faculty Elect. Eng., Univ. Teknologi MARA, Shah Alam, Shah Alam, 2016.

[50] H. M. Sim, H. Asmuni, R. Hassan, and R. M. Othman, "Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images," *Expert Syst. Appl.*, vol. 41, no. 11, pp. 5390–5404, 2014.
[51] K. B. Raja, R. Raghavendra, V. K. Vemuri, and C. Busch, "Smartphone based visible iris recognition using deep sparse filtering," *Pattern Recognit. Lett.*, vol. 57, pp. 33–42, May 2015.
[52] C. Galdi, M. Nappi, and J. L. Dugelay, "Multimodal authentication on smartphones: Combining iris and sensor recognition for a double check of user identity," *Pattern Recognit. Lett.*, vol. 82, pp. 144–153, Oct. 2016.
[53] K. B. Raja, R. Raghavendra, C. Busch, and S. Mondal, "An empirical study of smartphone based iris recognition in visible spectrum," in *Proc. 7th Int. Conf. Secur. Inf. Netw.*, Sep. 2014, p. 239.
[54] R. Raghavendra, C. Busch, and B. Yang, "Scaling-robust fingerprint verification with smartphone camera in real-life scenarios," in *Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2013, pp. 1–8.
[55] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Proc. Symp. Usable Privacy Secur. (SOUPS)*, vol. 14. Jul. 2014, pp. 187–198.
[56] J. S. Hammudoglu. *et al.* (2017). "Portable trust: Biometric-based authentication and blockchain storage for self-sovereign identity systems." [Online]. Available: https://arxiv.org/abs/1706.03744
[57] M. S. Khalil, "Reference point detection for camera-based fingerprint image based on wavelet transformation," *Biomed. Eng. Online*, vol. 14, no. 1, p. 40, 2015.
[58] C. Bo, L. Zhang, T. Jung, J. Han, X. Y. Li, and Y. Wang, "Continuous user identification via touch and movement behavioral biometrics," in *Proc. IEEE Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2014, pp. 1–8.
[59] P. J. Phillips *et al.*, "Overview of the face recognition grand challenge," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, vol. 1. Jun. 2005, pp. 947–954.
[60] P. Flynn, K. Bowyer, and P. Phillips, "Assessment of time dependency in face recognition: An initial study," in *Proc. Int. Conf. Audio-Video-Based Biometric Person Authentication*, Jun. 2003, pp. 44–51.
[61] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data security and privacy in cloud computing," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, p. 190903, 2014.
[62] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Proc. Int. Comput. Sci. Electron. Eng. (ICCSEE)*, vol. 1. Mar. 2012, pp. 647–651.
[63] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.
[64] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing," *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, 2013.
[65] S. R. Lodha and S. Dhande, "Web database security techniques," *Int. J. Adv. Res. Comput. Sci. Manage. Studies*, vol. 2, no. 3, pp. 1–6, 2014.
[66] A. W. Akanji, A. A. Elusoji, and A. V. Haastrup, "A comparative study of attacks on databases and database security techniques," *African J. Comput. ICTs*, vol. 7, no. 5, pp. 1–8, 2014.
[67] B. Amos, B. Ludwiczuk, and M. Satyanarayanan, "OpenFace: A general-purpose face recognition library with mobile applications," School Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-CS-16-118, 2016.
[68] T. Baltrušaitis, P. Robinson, and L. P. Morency, "OpenFace: An open source facial behavior analysis toolkit," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Mar. 2016 pp. 1–10.
[69] L. Yuan, P. Korshunov, and T. A. Ebrahimi, "Privacy-preserving photo sharing based on a secure JPEG," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2015, pp. 185–190.
[70] M. Boopathi and M. Aramudhan, "Secure server-server communication for dual stage biometrics–based password authentication scheme," *Alexandria Eng. J.*, vol. 48, no. 5, pp. 415–435, 2017. [Online]. Available: https://doi.org/10.1016/j.aej.2017.01.031
[71] Spanish Agency of Data Protection. *Guide for the Security of Data*. Accessed: Jul. 1, 2017. [Online]. Available: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

FRANCISCO D. GUILLÉN-GÁMEZ received the Ph.D. degree from the Madrid Open University, in 2016. He is currently with the Faculty of Education Pontificia, University of Salamanca. In journals and conferences, he has several publications in the area of biometric authentication applied to distance education.

IVÁN GARCÍA-MAGARIÑO received the Ph.D. degrees in computer science engineering from the Complutense University of Madrid, in 2009. He was a Lecturer with Madrid Open University from 2010 to 2014. He has been a Lecturer with the University of Zaragoza from 2014. Among journals, book chapters, conferences, and workshops, he has over 90 publications (30 in journals with ISI Thomson JCR). His most relevant publications belong to international journals with a high impact, such as *Engineering Applications of Artificial Intelligence*, *Expert Systems with Applications*, *Information Sciences*, *Knowledge-based Systems*, *Information and Software Technology*, *Simulation Modelling Practice and Theory*, *Journal of Systems and Software*, *Personal and Ubiquitous Computing*, *International Journal of Medical Informatics*, *Medical and Biological Engineering and Computing*, *Journal of Biomedical Informatics and Computer Standards and Interfaces*. He belongs to the EduQTech Research Group. He had a FPI Researcher Scholarship from 2006 to 2010.

JAVIER BRAVO-AGAPITO received the Ph.D. degree in computer Science from the Universidad Autónoma de Madrid. He collaborated with recognized institutions including Telecom Bretagne (Brest, France) and University of Pittsburgh PA, USA. He is currently an Associate Professor with the Madrid Open University and his research interests are focused in E-learning and data mining areas.

RAQUEL LACUESTA received the degree in computer science engineering and the Ph.D. degree (Dr.Ing.) in computer science engineering from the Polytechnic University of Valencia, in 1999 and 2008, respectively. She has been the Lecturer of Computer Science with Zaragoza University, for over 12 years. She currently teaches human–computer interaction, security, and databases subjects. She has authored or co-authored over 30 scientific papers published in national and international conferences. She also has had over 15 papers about education published in national and international conferences and several papers published in international journals. Her main topics of research are security and auto-configuration on *ad hoc* and spontaneous networks, design and evaluation of routing algorithms, computer–human interaction and education. She has been involved as an Organizer and Chair for several important program committees of international conferences. She is an Associate Editor and Reviewer of the *International Journal Networks Protocols and Algorithms* and member of different national research projects.

JAIME LLORET (M'07–SM'10) received the M.Sc. degree in physics in 1997, the M.Sc. degree in electronic engineering in 2003, and the Ph.D (Dr.Ing.). degree in telecommunication engineering in 2006. He is currently an Associate Professor with the Polytechnic University of Valencia. He is also the Chair of the Integrated Management Coastal Research Institute and the Head of the Active and Collaborative Techniques and Use of Technologic Resources in the Education Innovation Group. He is the Director of the University Diploma Redes y Comunicaciones de Ordenadores and of the University Master Digital Post Production. He has been the Internet Technical Committee Chair (the IEEE Communications Society and Internet Society) for the term 2013–2015. He has authored 22 book chapters and has had over 360 research papers published in national and international conferences and international journals (over 140 with ISI Thomson JCR). He has been involved in over 320 program committees of international conferences, and over 130 organization and steering committees. He leads many national and international projects. He an IARIA Fellow. He is currently the Chair of the Working Group of the Standard IEEE 1907.1. He has been the General Chair (or Co-Chair) of 39 international workshops and conferences. He has been the Co-Editor of 40 conference proceedings and the Guest Editor of several international books and journals. He is an Editor-in-Chief of *Ad Hoc and Sensor Wireless Networks* (with ISI Thomson Impact Factor), the *International journal Networks Protocols and Algorithms*, and the *International Journal of Multimedia Communications*, IARIA Journals Board Chair (eight journals) and he is (or has been) an Associate Editor of 46 international journals (16 with ISI Thomson Impact Factor).