EAI Endorsed Transactions
on Ambient Systems

Research Article EAI.EU

Access Control in Smart Homes by Android-Based Liveness Detection

Susanna Spinsante[1,*], Laura Montanini[1], Veronica Bartolucci[1], Manola Ricciuti[1], Danny Pigini[1], Ennio Gambi[1]

[1]Dipartimento di Ingegneria dell'Informazione, Universita' Politecnica delle Marche, Via Brecce Bianche 12 Ancona, 60131, ITALY,

Abstract

Technologies for personal safety and security play an increasing role in modern life, and are among the most valuable features expected to be supported by so-called smart homes. This paper presents a low-complexity Android application designed for both mobile and embedded devices, that exploits the available on-board camera to easily capture two images of a subject, and processes them to discriminate a true 3D and live face, from a fake or printed 2D one. The liveness detection based on such a discrimination provides anti-spoofing capabilities to secure access control based on face recognition. The limited computational complexity of the developed application makes it suitable for practical implementation in video-entry phones based on embedded Android platforms. The results obtained are satisfactory even in different ambient light conditions, and further improvements are being developed to deal with low precision image acquisition.

Keywords: liveness detection, spoofing, face recognition, Android, stereo vision

Received on 28 February 2017; accepted on 11 May 2017; published on 17 May 2017

doi:10.4108/eai.17-5-2017.152546

1. Introduction

The Smart Home (SH) domain encompasses a huge variety of technologies, applications, and services, aimed at providing intelligence to an environment in which people spend most of their lifetime. Intelligent capabilities in SH aim at improving the quality of life of the resident people, by facilitating routine operations, and anticipating the users' needs, by learning and understanding their behaviours [1, 2]. The advantages to live in a SH can be expressed in terms of: simplicity and comfort, reliability, energy saving, cost reduction, and security. In order to fulfill such requirements, the design of SHs relies on a wide variety of other fields, like, for example: sensing, reasoning, actuating, security, and Human-Computer Interaction (HCI9) [3]. Pervasive sensing is extremely useful in SHs, as well as wireless technologies, enabling the connection among heterogeneous devices, and creating the conditions for new integrated functionalities [4]. Dedicated interfaces can be used to access the system, including remote controls and touch screens. Other devices, such as smartphones, tablets and PCs, can be also used to remotely control the SH state [5], or to execute operations through acting systems. Reasoning functions can be seen as the necessary link connecting sensing and actuation. Reasoning is an umbrella term that includes user modeling, activity prediction and recognition, decision making, and spatial-temporal reasoning [3]. Personal safety and security play a critical role [6] in SH design, and many different devices and applications have been developed to address such needs. At the same time, regardless of how safe individual devices are or claim to be, new vulnerabilities may arise when different hardware devices are networked and set up to be controlled remotely.

Regarding safety, the most important aspect concerns the detection of alarming events, such as flooding, gas and smoke leaks. Systems able to detect these events allow the user to be warned on time, promptly intervene, or ask for help from someone else, and avoid potentially more dangerous situations.

*Corresponding author. Email: s.spinsante@univpm.it

Access control is another key point when dealing with security. Intrusion detection systems are becoming gradually more common [7]. They exploit different technologies in order to detect the presence of unauthorized people at home. Most widespread technologies include magnetic sensors on doors and windows, motion sensors and cameras [8–10]. Anyway, in this field, the ability to distinguish between authorized and unauthorized subjects represents a primary objective.

Reliable methods for biometric personal identification, called Automatic Identification and Data Capture (AIDC) systems, exist, both based on iris [11, 12] or retinal scans [13], and fingerprint analysis [14, 15]. Nevertheless, they are still quite expensive [16] and have to gain acceptance by the general consumers. Among them, face recognition [17] is a long-established research area that recently became very popular in consumer applications. Thanks to advances in electronics and sensor technologies, that make high quality image sensors available in commercial devices, at a reasonable cost, it is becoming one of the most successful image analysis and understanding application. However, despite biometry is helpful to improve security, anti-spoofing techniques should be implemented [18], in order to ensure they cannot be breached.

In this paper, we address the design of a low-complexity Android-based application for liveness detection, relying on image processing techniques, to be implemented in embedded Android platforms for video entry-phones. The aim of the project is to counteract face spoofing, one of the prominent threats to face recognition systems. The main idea is to discriminate a 2D face image, such as a photo, from a real 3D face belonging to a live subject, by means of stereo vision techniques. Stereo vision enables the reconstruction of the scene three-dimensional shape, providing a so-called *disparity map*, in which the areas of the image are differently colored, based on their relative distance from the camera. This way, the proposed application is able to discriminate a picture from a live face.

The paper is organized as follows: Section 2 shortly introduces the basic concepts upon which the application design has been conceived, whereas Section 3 presents an overview of related works about liveness detection methods. Basics of stereo vision are briefly described in Section 4. The design of the Android mobile application is discussed in Section 5, and Section 6 presents the experimental results obtained by testing the application in real conditions. Finally, Section 7 concludes the paper.

2. Basic Concepts

For the human brain, binding an identity to a face is an automated and immediate task, despite its complexity. However, it is virtually impossible to reduce this operation to a search for objective parameters, that instead are essential to form the basis of an efficient biometric system. From a biometric point of view, we must consider that many factors can make it difficult to recognize a face. Light conditions, facial expressions, face rotations, age, physical radical changes, as well as the presence of partial occlusions, such as glasses, facial hair, or hair, covering part of the face, are just some of the elements which make the automatic face recognition challenging. Despite these issues, algorithms that allow to obtain satisfactory results of personal identification have been proposed in the literature [19–21].

A generic face recognition process applied to anti-intrusion systems is summarized in Figure 1, and consists of five principal phases [22]:

- *Image Acquisition*: the face recognition process starts with the image acquisition, usually exploiting an RGB camera sensor.
- *Pre-processing phase*: such a phase ensures that the image recognition process meets the established requirements. For example, it implements the localization of subject on the image and the distinction of him/her from the background, moreover it checks the optimum brightness, or a specific subject-to-lens distance.
- *Face detection phase*: in order to be recognized, the face should be first detected on the image frame.
- *Features extraction phase*: each face can be coded by a subset of numerical information, called *features*, and represented by a mathematical model, useful for face identification and discrimination from others.
- *Recognition or verification phase*: thanks to the mathematical representation, it is possible to compare different images, in order to recognize the captured subject's identity or verify that he/she is a real person.

If the face has been recognized from the captured static image or video sequence, and the subject belongs to authorized users, then the access will be allowed.

Some critical aspects recently emerged in access control systems based on face recognition, such as the vulnerability to spoofing attacks. They can be divided in three categories [23]:

- photo attack: when the counterfeiter presents a picture (printed or displayed on a digital device) of the authorized user to the recognition system;
- video attack: when the attacker replays a video of the authorized user;

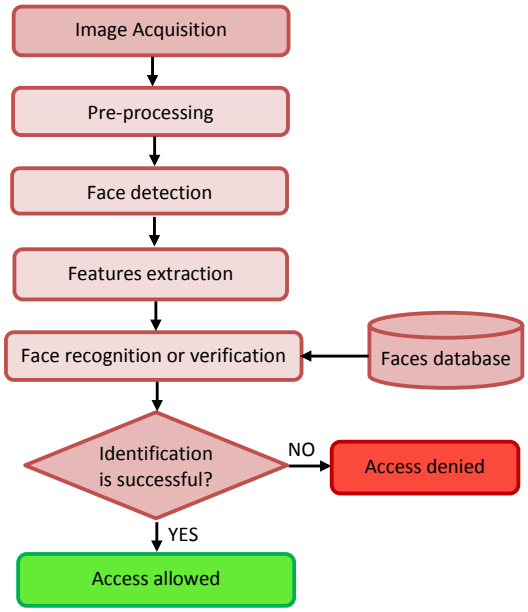


Figure 1. Flow chart of a face recognition process applied in an anti-intrusion system.

- mask attack: when the opponent wears a 3D mask of the authorized user.

Anti-spoofing, liveness detection and vitality detection are equivalent terms used in the literature to describe the same concept, that is: any technique aimed at verifying if the captured biometric information belongs to a live subject, or to an artificial and synthetic copy of him/her.

Anti-spoofing techniques shall be unobtrusive, user-friendly, fast, low cost and well performing, e.g. able to avoid both false negative and false positive identifications. As stated by Galbally et al. in [23], these techniques may be classified into three groups:

- sensor-level techniques: exploiting specific sensors in order to identify particular living traits (blood pressure, facial thermogram, etc);
- feature-level techniques: in which the biometric data are acquired via a standard sensor and the distinction between fake and real faces is software-based;
- score-level techniques: much less common than the others, and focused on the study of biometric systems at a score-level.

The choice among one of the three groups should always balance advantages and disadvantages. Typically, hardware-based techniques have the best performance since they extract information directly from the human body. Nevertheless, they are quite intrusive and expensive. Conversely, the score-level techniques have limited performance, while maintaining low costs and intrusiveness. Among them, a compromise solution is represented by the feature-level group: it combines sufficient performance with low cost and less intrusiveness.

3. Related Works

In recent years many anti-spoofing techniques have been proposed in the literature.

A study by Pravallika and Prasad exploits SVM classification to differentiate between real and fake samples [24]. It relies on the assumption that a fake image captured in an attack attempt has different quality than a real sample acquired in the normal operation scenario. Such a method is applicable to iris, palm print and face. Another quality-based algorithm has been proposed by Galbally and Marcel [25]. As affirmed by authors, by visually inspecting real and fake face images of the same person, even the human eye may find it difficult to make a distinction. Nevertheless, some disparities may become evident by translating images into a proper feature space. Anyway, the performance of such anti-spoofing methods degrades when the quality of the spoofing attempts increases.

In a recent paper [26] the gaze direction estimation has been implemented for the liveness detection analysis. While Pan et al. [27] investigate eye-blinks as a liveness detection clue. Both solutions provide high performance against photo spoofing, but are vulnerable to video attacks. In this view, promising results have been obtained by Komulainen et al. [28]: they propose a reliable spoofing detection method based on the available scene and context information.

A further study addresses the spoofing issue by analyzing the feasibility of low-cost attacks with self-manufactured three-dimensional printed models to 2D (photo attacks), 2.5D (video attacks) and 3D (mask attacks) face recognition systems [29]. However, 3D face recognition technology may fail the challenge posed by more sophisticated type of attacks based on the presentation of a 3D face reproduction to the acquisition sensor used. In [30], the authors inspect the spoofing potential of subject-specific 3D facial masks for 2D face recognition. Additionally, they analyze LBP-based countermeasures using both color and depth data, obtained by Kinect. Instead, Liu et al. propose to use remote Photoplethysmography (rPPG) as an intrinsic liveness cue for 3D mask face anti-spoofing [31].

As stated by authors in [23], an anti-spoofing solution should always balance security against convenience, demonstrating that it is important to keep in mind the final product within which the system must be integrated, and its related constraints. With respect to the described methods, in this paper the use of a binocular vision through a single camera

as an anti-spoofing system for liveness detection, provides simplicity, cost and practical advantages and remarkable performance even under bad illumination conditions. The most practical aspect is that the depth analysis is lower complexity and immediate operation. Furthermore, the Android application presented in Section 5 can be implemented and adopted even on smartphones, providing high portability and facility of distribution.

4. Stereo Vision

The term stereo computer vision refers to the extraction of 3D information from digital images. By comparing the information captured from two different points of view, the 3D information can be extracted by examining the relative positions of objects in the two shots. Traditionally, in stereo vision, two different views of a scene are captured by horizontally disposed cameras: this mode is inspired by the binocular human visual system.

The problem of converting 2D information in 3D can be reduced substantially in two sub-problems: correspondence and reconstruction. The correspondence problem consists in identifying matched points in the images such that there are no ambiguities. In fact, ambiguous correspondences lead to different interpretations of the scene.

Figure 2 shows two simplified models of reality in order to better understand the concepts behind the stereo vision problem. In Fig. 2(a), two points P and Q on the same line of sight of the left image plane have been considered. Thanks to epipolar geometry the correspondence issue can be easily addressed. In fact, the epipolar constraint states that the projection of points P and Q in the right image plane must belong to the same line (dotted line) of their projection in the left side. The search in the space of corresponding points can then be narrowed from a 2D to a 1D search.

As regards the reconstruction, once the matching points have been identified, it is necessary to calculate their disparity. Referring to Fig. 2(b), the disparity can be defined as follows:

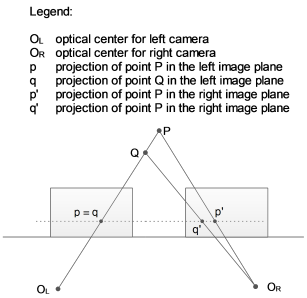
$$d = x_r - x_l. \tag{1}$$

It represents the difference between the x coordinate of the two corresponding points and allows to calculate the depth. In fact, through some simple steps, it is possible to obtain the relationship between the disparity d and the depth Z:

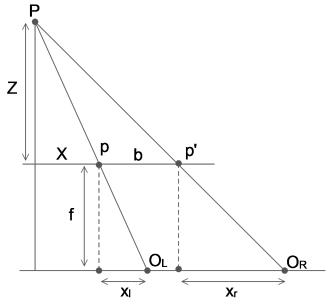
$$\begin{aligned} \frac{x_l}{f} = \frac{X}{Z} \quad , \quad \frac{x_r}{f} = \frac{X+b}{Z} \\ d = x_r - x_l \quad = \quad \frac{f(X+b)}{Z} - \frac{fX}{Z}, \end{aligned} \tag{2}$$

whence:

$$d = \frac{fb}{Z}. \tag{3}$$



(a) Epipolar constraint for correspondence: matches for p and q in the right plane must lie on the epipolar line (dotted line)



(b) A simplified model of reality in the top-view perspective

Figure 2. Graphic representations of the stereo vision concepts

Therefore, the disparity of a point is proportional to focal length f and baseline b, and inversely proportional to its depth. Since f and b are constant over the whole image, a disparity map provides a direct encoding of the scene depth.

5. Design of the Android Mobile Application

Currently, thanks to the progressive spreading of social networks, to retrieve pictures or videos of an individual is very simple. Conversely, to acquire information on the 3D shape of the face and reproduce it as a mask is more complicated. For this reason, in the proposed application, the liveness detection problem is approximated as a problem of discriminating 2D from 3D objects, i.e. considering just photo and video attacks. This is obtained basically by resorting to the stereo vision concept, according to which by comparing the images of the same subject captured from two different perspectives, the 3D information may be extracted, analyzing the relative positions of the same elements in the two captured images. Since the application exploits a standard RGB camera and all the features are extracted by image processing, the technique used can be classified as a *feature-level* technique.

A first version of the software application has been designed in Java language, for a desktop execution,

exploiting the availability of the *BoofCV* libraries for stereo vision. Later, in order to get a portable code for Android devices, the *OpenBeans* library has been used. Using the camera sensor embedded in almost all the current mobile devices (smartphones), the application needs a couple of images gathered from two different perspectives (left and right), and processes them according to Section 4, to output a point-cloud of the detected subject, denoting if a live (3D), or a fake (2D) picture, has been processed.

The stereo vision implies a number of pre-requisites the captured images need to satisfy, such as: any image distortion due to the capturing sensor shall be compensated, in order to get pinhole camera - like images, and each image in the couple shall be rectified, to be comparable. To this aim, two fundamental operations must be performed before starting the stereo matching and reconstruction processes: camera calibration and image rectification.

Calibration is a process for estimating the camera's intrinsic and extrinsic parameters. The former concern the internal characteristics of the camera, such as focal length or parameters of lenses distortion, while the latter describe the spatial position and orientation of the camera, i.e. the relative translations and rotations between the two images. The knowledge of the intrinsic parameters is an essential first step for the 3D reconstruction, because it enables the derivation of the scene structure in the space and removes the distortion of the lens, which leads to optical errors, degrading the accuracy.

The calibration process must be repeated if the camera resolution changes [32], and consists of the following six steps:

1. to print a grid pattern, that becomes the camera calibration model;
2. to mount the model on a flat rigid surface.
3. to take a lot of pictures (at least 8), locating the target at different orientations and distances from the lens;
4. to examine the captured images, keeping only those that are in focus;
5. to use the algorithm to automatically detect the calibration target and generate reference parameters;
6. to save the file generated from images processing and containing the calibration parameters.

The *BoofCV* library provides a calibration feature. To calculate the calibration parameters, it is possible to use planar chessboards, as explained above. Figure 3 shows a sample subset of the chessboard grids used to calibrate the device camera in our experiments.

The image rectification step is required when the considered image planes are not coplanar: thanks to this operation the images become coplanar, and the matching and reconstruction procedures will be faster and more efficient, since they will run on a single dimension, as mentioned in Section 4.

The image rectification process consists of a sequence of operations that, starting from two images representing a common scene, allow to generate several images, by rotating them in the same coordinate system. During this process, the detection of corresponding points between the two starting images is fundamental. This operation, known as *keypoint matching* [33], consists of three steps:

1. *Key-point detection*: the key-points are searched in all images. They could be pixels corresponding to the shapes angles, in which there is a color discontinuity between neighbors pixels.
2. *Key-point description*: each key-point detected is identified and marked.
3. *Key-point matching*: in such a phase, the actual association of the key-point with the two images, takes place. It is based on the Hamming distance between the strings which describe them; if such a distance is less than a specific threshold, the match is considered valid.

Once the rectification process is concluded, by exploiting stereo vision concepts, a 3D representation of the captured environment is obtained, and can be expressed in two ways:

- using a disparity picture, where different colors represent different image depths; the hottest hues represent the closest points, while the coldest are the most distant from the camera;
- through a dense 3D PC, in which, using drag-and-drop, the figure three-dimensionality is recognized and perceived.

The algorithm here presented can be summarized as follows:

- Camera calibration: the calibration file and the pair of photographed images are loaded.
- Keypoint matching: the images features are detected, described and associated.
- Rectification process of the pair of images.
- Disparity picture: dense stereo disparity is calculated.
- 3D PC conversion: the disparity picture is converted in a 3D PC, that is the alghoritm output.

Figure 3. Sample subset of calibration chessboards

The Android version of the algorithm described so far is schematized in Figure 4. The most important step is the *Stereo Reconstruction* one. As shown Figure 4, by clicking on the *"Stereo reconstruction"* button, a camera function, that allows to capture the photo sequence, is called. Automatically, a new interface appears, and, by pressing the *"Stereo reconstruction"* button again, the images are processed and the 3D scene reconstructed. It is worth noticing that the Android application described above has been developed as a tool to experimentally prove the feasibility of the proposed approach to liveness detection. In fact, the final aim of the project is to have the algorithm implemented on an Android embedded platform, with limited computational capabilities, typically used to design video-entry phones.

The final graphical interface contains four buttons, i.e:

- *Initial Pictures*, which visualizes the initial pictures;
- *Rectified Images*, which displays the rectified images;
- *Disparity*, which shows the resulting disparity map;
- *Back*, to return to the home screen and restart the process.

Finally, once the scene has been reconstructed, the robustness of the liveness detection process is further increased through a number of verification steps:

- check if the subject's nose is the element of the face at the shortest distance from the camera;
- check if different areas captured by the sensor (like nose and eyes, or face and background) are located at different distances from it;
- check if expected areas, like the face, the nose or the eyes, can be located in both the captured images;
- check if some kind of involuntary eye movements is detected.

6. Experimental Results

In order to verify the proper functioning of the adopted method, several preliminary tests have been performed using a desktop PC. The objective of such tests is to identify the optimal resolution value which allows to correctly reconstruct the image. In fact, as the resolution increases, computational problems (processing time) increase or calibration inaccuracies appear. Test results show that the best resolution value is 0.3 megapixels. By using this value, the results are obtained in a very short time (about one second) and a correct calibration process is ensured. As already stated, this is a fundamental operation to properly carry out the stereo reconstruction.

Additional factors influencing the results are:

- subject distance from the camera;
- relative distance between the two pictures;
- brightness.

For each of them, three different conditions have been considered, as shown in Table 1, and every possible combination of them has been considered. Results suggest that using as input pictures taken at a great distance produces worst results, at any brightness condition. For minimum and medium distances, the low-light condition does not provide acceptable results in any circumstance, while in the normal light case the face is entirely detected and reconstructed, both for extremely close-up, close-up and half-length photos. For the intense brightness case, acceptable results are obtained only if the two shots are very close together. In summary, in order to obtain a proper 3D reconstruction of the face:

- it should be well lit;
- the use of flash should be avoided, unless the two shots are taken at a distance smaller than 5 mm;
- the pair of photos should have a relative distance varying from 3-5 mm to 15 mm;
- within the limits of the considered situations, the distance of the subject from the camera is indifferent for a correct result.

Following preliminary tests, the Android application has been tested on different devices (Samsung Galaxy S3, S5 and S6, LG G4, Huawei P8 Lite), equipped with diverse Android OS versions. The app execution runs smooth, if the device has at least 1 GB RAM available, but in any case it is necessary to downscale the camera resolution by a factor of at least 8, to enable a real-time processing of the captured images.

Also in this case, despite the not full precision of the acquisition process, the mobile application is able to discriminate faces shown in pictures (spoof) from live ones. Figure 5 visually summarizes some of the results obtained from lab experiments, run by capturing up to 30 pairs of pictures.

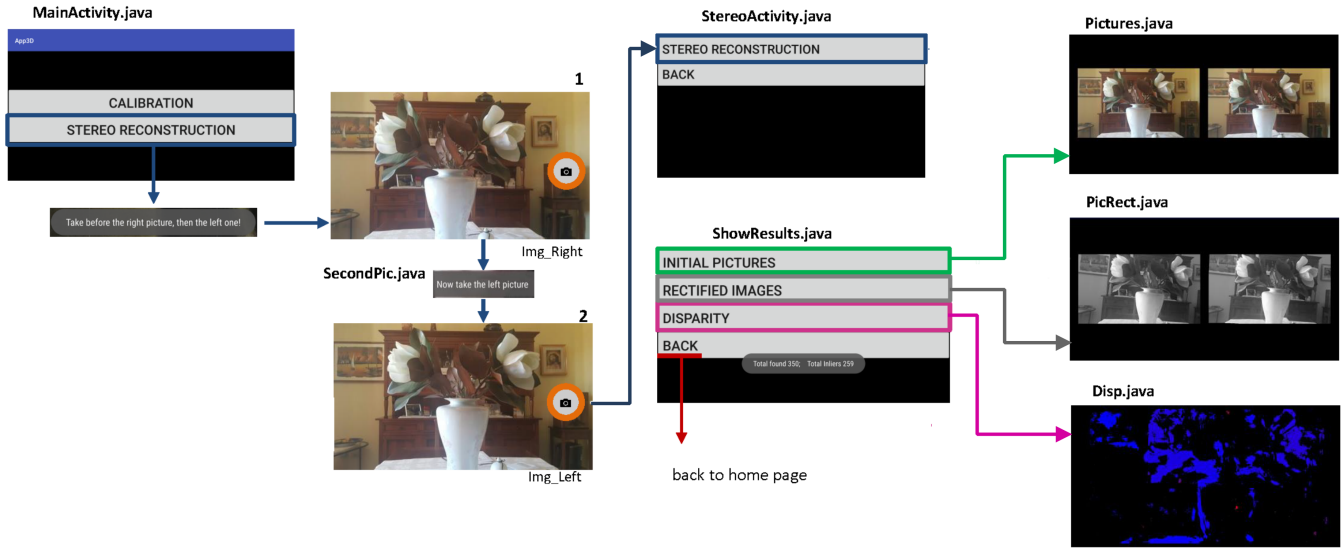


Figure 4. Global flow diagram of the application steps

Table 1. Summary of the situations envisaged in the test phase, for each analyzed factor.

Factor	Possible conditions	Description
Distance between subject and camera	extreme close-up photos	The pictures contain just part of the face and neck
	close-up photos	The pictures contain not only face and neck, but also the shoulders
	half-length photos	The picture is cut at chest level
Distance between the two pictures	minimum distance	The photos are almost coincident and the distance between the two shots is about 3-5 mm
	medium distance	There is a slight shift between the two pictures (~ 15 mm)
	great distance	The two pictures are far apart more than 30 mm
Brightness	minimum brightness	The subject is illuminated by a low light (for example an abatjour)
	medium brightness	The subject is illuminated by a common, warm light bulb
	intense brightness	The subject is illuminated by a common, warm light bulb and in addiction by a flash

Problems and inaccuracies encountered during the processing phase can be summarized as follows:

- the presence of noise, unavoidable even in the high-quality cameras, can lead to variations in intensity also in pairs of corresponding pixels;
- the presence of occlusions, possibly visible only from one of the two cameras, causes errors in the calculation of the disparity map;
- the reflection and translucency of some objects, causes a key-point matching failure.
- the presence of uniform or repeated surfaces, such as many points with very similar intensity, is another key-point matching problem.

7. Conclusion

The Android application for mobile and embedded devices presented in this paper demonstrates the feasibility of a real-time liveness detection process, which implements anti-spoofing by detecting the 2D or 3D nature of the captured face images. The application requires initial calibration of the device camera, and suffers from limitations due to possible imperfections

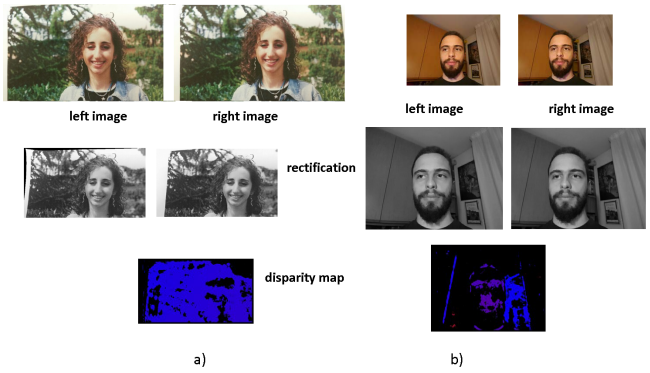


Figure 5. Output of the liveness detection mobile app in the case of: a) spoofed face images, b) live and complex face image. The output disparity map in b) clearly features the face profile distinguishable from the background.

in the image capturing process, however, it shows very promising results.

The proposed application is able to generate a disparity graph associated to the subject in front of the smartphone camera, obtaining different results in cases of liveness detection or spoofing. When the graph mainly consists of a single color, such a condition is associated to a spoofing attempt; when areas of different colors are detected, like the background and the subject in foreground, then it is assumed to have a real person in front of the camera, and therefore their liveness is detected successfully.

Further developments are currently ongoing to increase the robustness of the application and test it on a larger variety of subjects, in real-life conditions.

References

[1] Makonin, S., Bartram, L. and Popowich, F. (2013) A smarter smart home: Case studies of ambient intelligence. *IEEE Pervasive Computing* **12**(1): 58–66. doi:10.1109/MPRV.2012.58.

[2] Wu, S., Rendall, J., Smith, M., Zhu, S., Xu, J., Yang, Q., Wang, H. *et al.* (2017) Survey on prediction algorithms in smart homes. *IEEE Internet of Things Journal* **PP**(99): 1–1. doi:10.1109/JIOT.2017.2668061.

[3] Cook, D.J., Augusto, J.C. and Jakkula, V.R. (2009) Ambient intelligence: Technologies, applications, and opportunities. *Pervasive and Mobile Computing* **5**(4): 277–298.

[4] Spinsante, S., Cippitelli, E., De Santis, A., Gambi, E., Gasparrini, S., Montanini, L. and Raffaeli, L. (2015) *Multimodal Interaction in a Elderly-Friendly Smart Home: A Case Study* (Cham: Springer International Publishing), 373–386. doi:10.1007/978-3-319-16292-8_27, URL http://dx.doi.org/10.1007/978-3-319-16292-8_27.

[5] Raffaeli, L., Montanini, L., Gambi, E. and Spinsante, S. (2016) User interfaces in smart assistive environments: Requirements, devices, applications. In Rodrigues, J., Cardoso, P., Monteiro, J. and Figueiredo, M. [eds.] *Handbook of Research on Human-Computer Interfaces, Developments, and Applications* (Hershey, PA: IGI Global), chap. 17, 420–443.

[6] Ur, B., Jung, J. and Schechter, S. (2013) The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)* (HUPS 2014). URL https://goo.gl/H9V9He.

[7] Robles, R.J., Kim, T.h., Cook, D. and Das, S. (2010) A review on security in smart home development. *International Journal of Advanced Science and Technology* **15**.

[8] All-in-one wireless security system - piper. URL https://getpiper.com.

[9] Uses-monitoring & security - smartthings. URL https://www.smartthings.com/uses/monitoring-security.

[10] Ring video doorbell for your smartphone - ring. URL https://ring.com/.

[11] Gragnaniello, D., Sansone, C. and Verdoliva, L. (2015) Iris liveness detection for mobile devices based on local descriptors. *Pattern Recognition Letters* **57**: 81 – 87. doi:http://dx.doi.org/10.1016/j.patrec.2014.10.018, URL http://www.sciencedirect.com/science/article/pii/S0167865514003511. Mobile Iris {CHallenge} Evaluation part I (MICHE I).

[12] Thavalengal, S., Nedelcu, T., Bigioi, P. and Corcoran, P. (2016) Iris liveness detection for next generation smartphones. *IEEE Transactions on Consumer Electronics* **62**(2): 95–102. doi:10.1109/TCE.2016.7514667.

[13] Azemin, M.Z.C., Kumar, D.K., Sugavaneswaran, L. and Krishnan, S. (2011) Supervised retinal biometrics in different lighting conditions. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*: 3971–3974. doi:10.1109/IEMBS.2011.6090986.

[14] Callaly, F., Cucu, C., Cucos, A., Leyden, M. and Corcoran, P. (2007) Real-time fingerprint analysis authentication for embedded appliances. In *2007 Digest of Technical Papers International Conference on Consumer Electronics*: 1–2. doi:10.1109/ICCE.2007.341416.

[15] Patil, A.A. and Dhole, S.A. (2016) Image quality (iq) based liveness detection system for multi-biometric detection. In *2016 International Conference on Inventive Computation Technologies (ICICT)*, **1**: 1–5. doi:10.1109/INVENTIVE.2016.7823297.

[16] Arslan, B., Yorulmaz, E., Akca, B. and Sagiroglu, S. (2016) Security perspective of biometric recognition and machine learning techniques. In *Machine Learning and Applications (ICMLA), 2016 15th IEEE International Conference on* (IEEE): 492–497.

[17] Zhao, W. and Chellappa, R. (2002) *Image-based Face Recognition: Issues and Methods*. Tech. rep., IMAGE RECOGNITION AND CLASSIFICATION.

[18] Akhtar, Z. and Kale, S. (2011) *Security Analysis of Multimodal Biometric Systems against Spoof Attacks* (Berlin, Heidelberg: Springer Berlin Heidelberg), 604–611. doi:10.1007/978-3-642-22714-1_62, URL http://dx.doi.org/10.1007/978-3-642-22714-1_62.

[19] Wang, J., Lu, C., Wang, M., Li, P., Yan, S. and Hu, X. (2014) Robust face recognition via adaptive sparse representation. *IEEE Transactions on Cybernetics* **44**(12): 2368–2378. doi:10.1109/TCYB.2014.2307067.

[20] Wagner, A., Wright, J., Ganesh, A., Zhou, Z., Mobahi, H. and Ma, Y. (2012) Toward a practical face recognition system: Robust alignment and illumination by sparse representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **34**(2): 372–386. doi:10.1109/TPAMI.2011.112.

[21] Liao, S., Jain, A.K. and Li, S.Z. (2013) Partial face recognition: Alignment-free approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **35**(5): 1193–1205. doi:10.1109/TPAMI.2012.191.

[22] Chao, W.L. (2007) Face recognition. *GICE, National Taiwan University* .

[23] Galbally, J., Marcel, S. and Fierrez, J. (2014) Biometric antispoofing methods: A survey in face recognition. *IEEE Access* **2**: 1530–1552. doi:10.1109/ACCESS.2014.2381273.

[24] Pravallika, P. and Prasad, K.S. (2016) Svm classification for fake biometric detection using image quality assessment: Application to iris, face and palm print. In *2016 International Conference on Inventive Computation Technologies (ICICT)*, **1**: 1–6. doi:10.1109/INVENTIVE.2016.7823189.

[25] Galbally, J. and Marcel, S. (2014) Face anti-spoofing based on general image quality assessment. In *Pattern Recognition (ICPR), 2014 22nd International Conference on* (IEEE): 1173–1178.

[26] Adamiak, K., Åżurek, D. and ÅŽlot, K. (2015) Liveness detection in remote biometrics based on gaze direction estimation. In *2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*: 225–230. doi:10.15439/2015F307.

[27] Pan, G., Sun, L. and Wu, Z. (2008) *Liveness detection for face recognition* (INTECH Open Access Publisher).

[28] Komulainen, J., Hadid, A. and Pietikainen, M. (2013) Context based face anti-spoofing. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on* (IEEE): 1–8.

[29] Galbally, J. and Satta, R. (2016) Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models. *IET Biometrics* **5**(2): 83–91. doi:10.1049/iet-bmt.2014.0075.

[30] Erdogmus, N. and Marcel, S. (2013) Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on* (IEEE): 1–6.

[31] Liu, S., Yuen, P.C., Zhang, S. and Zhao, G. (2016) 3d mask face anti-spoofing with remote photoplethysmography. In *European Conference on Computer Vision* (Springer): 85–100.

[32] Kim, S., Yu, S., Kim, K., Ban, Y. and Lee, S. (2013) Face liveness detection using variable focusing. In *2013 International Conference on Biometrics (ICB)*: 1–6. doi:10.1109/ICB.2013.6613002.

[33] Markus, N., Pandzic, I.S. and Ahlberg, J. (2016) Learning local descriptors by optimizing the keypoint-correspondence criterion. *CoRR* **abs/1603.09095**. URL http://arxiv.org/abs/1603.09095.