Soft Comput
DOI 10.1007/s00500-015-2019-4

METHODOLOGIES AND APPLICATION

Face recognition performance comparison between fake faces and live faces

Miyoung Cho[1] · **Youngsook Jeong**[1]

Abstract Face recognition is a widely used biometric technology because it is both user friendly and more convenient to use than other biometric approaches. However, naïve face recognition systems that do not support any type of liveness detection can be easily spoofed using just a photograph of a valid user. Face liveness detection is a key issue in the field of security systems that use a camera. Unfortunately, it is not easy to detect face liveness using existing methods, assuming that there are print failures and overall image blur. With the development of display devices and image capturing technology, it is possible to reproduce face images similar to real faces. Therefore, the number of attacks using a photograph or video displayed on a screen rather than paper will increase. In this study, we compare test results using live faces and high-definition face videos from light-emitting diode (LED) display devices and analyze the changes in face recognition performance according to the lighting direction. Experimental results show that there is no significant difference between live faces and not live faces under good lighting conditions. We suggest the use of gamma to reduce the performance gap between the two faces under poor lighting conditions. From these results, we can provide key solutions to resolve the issues associated with texture-based approaches.

Keywords Fake face · Face video · Display device · Face recognition · Face authentication

Communicated by V. Loia.

✉ Miyoung Cho
mycho@etri.re.kr

Youngsook Jeong
ysjeong@etri.re.kr

[1] Electronics and Telecommunications Research Institute, 218 Gajeongno, Yuseong-gu, Daejeon 34129, Korea

1 Introduction

Biometrics is the technology of establishing the identity of an individual on the basis of one or more intrinsic physiological or behavioral characteristics, such as faces, fingerprints, irises, and voices. One biometric technology, face recognition technology, has rapidly developed in recent years. This technology is more direct, user friendly, and convenient compared to other methods.

Face recognition is a task that humans routinely and effortlessly perform in our daily lives (Li and Jain 2011). The wide availability of powerful and low-cost desktop and embedded computing systems has created an enormous interest in the automatic processing of digital images in a variety of applications, including face identification, access control, security, surveillance, smart cards, law enforcement, and human–computer interaction.

Recently, face recognition has become increasingly important owing to rapid advances in image capture devices (e.g., surveillance cameras and camera in mobile phones), the availability of a very large number of face images on the internet, and the increased demands for higher security (Li and Jain 2011). Sometimes, facial data are stolen or duplicated in a face recognition system. That is, one or more photographs of a valid user can be easily obtained without even physically contacting the user through downloading via the internet or simply capturing them using a camera. A 2D image-based facial recognition system can be easily spoofed by these simple tricks and some poorly designed systems. Actually, it is a very challenging task to guard against spoofs based on a static image of a face, and most effort in face recognition research has currently focused on the image matching part of the system without caring whether the matched face is from a live human or not (Tan et al. 2010).

Published online: 19 January 2016

Generally, there are three ways in which face recognition can be spoofed: a photograph, video, and 3D model of a valid user (Pan et al. 2008). A photograph attack is both the cheapest and easiest spoofing approach. The imposter can rotate, shift, and bend the photo in front of the camera to simulate a live person in an attempt to fool the authentication system. Video spoofing is another major threat to face recognition systems because it is very similar to a live face. Finally, a 3D model has the 3D information of a face, yet it is rigid and lacks physiological information. In addition, it is difficult to create a realistic 3D model of a live person. Because of this, photographs and video are the most common spoofing approaches for attacking a face recognition system. With the improved color gamut of display devices and the development of image capturing, it is easy to deceive a face recognition system with images of faces displayed on a screen or monitor.

To overcome these problems, researchers have considered using extra sensors as well as visual cameras. Andrea et al. distinguished between 2D photographs and real human faces using 3D vector scans (Lagorio et al. 2013). Sooyeon Kim et al. proposed the technique of face liveness detection using the in-focus and out-of-focus functions of a camera (Kim et al. 2013). For live faces, the focused regions are clear, and the others are blurred owing to the depth information. In contrast, there is little difference between an image taken at different levels of focus from a printed copy of a face, because they are not solid. Despite the success of the above methods in some cases, nonintrusive methods without additional devices and human involvement are preferable in practice because they can be easily integrated into an existing face recognition system, where usually only a generic webcam is equipped. Their methods are also disadvantageous in terms of cost and commercialization.

Figure 1 shows an example of spoofing with a face video. In general, a human is able to distinguish between a live face and a fake face without any effort because humans easily recognize the physiological clues of liveness. However, face recognition systems without any additional devices are not able to differentiate a live face from a not live face. In this study, we focus on naïve face recognition systems that do not use any type of liveness detection and are easily spoofed by a face video of a valid user. We compare live faces with face videos from display devices and present the changes in face recognition performance according to lighting conditions.

This paper is organized as follows: In Sect. 2, we give a brief overview of the ways in which a face recognition system can be spoofed. Section 3 explains the challenges for face recognition. Section 4 describes how to construct a live face database and an imposter video database. In Sect. 5, we present an analysis of the experimental results. Finally, some issues are discussed in Sect. 6 along with the conclusions.

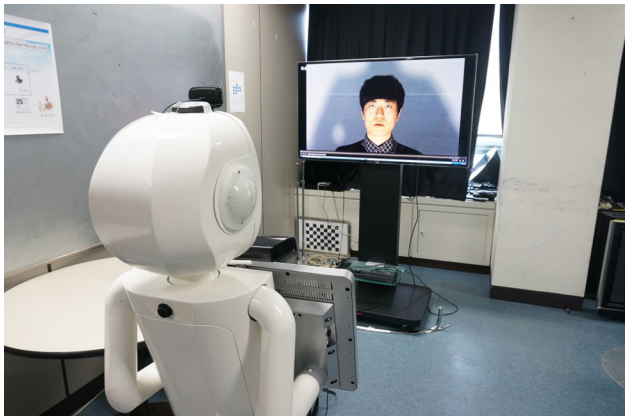

Fig. 1 Example of spoofing with video

2 Related work

There are many approaches implemented in face liveness detection. Approaches for detecting liveness are categorized according to the indicators of motion, signs of life, and texture (Chakraborty and Das 2014).

Motion analysis mainly differentiates the motion patterns between 3D and 2D faces. Planar objects move in a significantly different way than real human faces, which are 3D objects. Motion analysis usually depends on the optical flow calculated from video sequences. Bao et al. analyzed the differences and properties of the optical flow generated from 3D objects and 2D planes (Bao et al. 2009). The optical flow allows the reference field to be deduced, thereby allowing the face recognition system to determine whether the test region is planar or not. Kollreider et al. introduced a method combining the detection of face parts and the estimation of an optical flow field for face liveness detection (Kollreider et al. 2005). The basic idea of this method is the assumption that a 3D face generates 2D motion more so at central face region than at the outer face regions such as the ears. Therefore, the parts of the face farther from the camera move differently than parts that are nearer. However, a photograph generates an equal amount of motion for all of the different face regions. Motion analysis may not perform well when there is little motion information. This can occur because the behavior of the user may be different, resulting in highly noisy images and a low resolution. This approach might also fail when a spoof attack is performed using a more sophisticated method, such as a 3D sculpture face model.

Signs of life are categorized into two types depending on the interaction from the user. The first type requires a certain known interaction to be performed by the user. In this situation, the user performs a certain task to verify the liveness of their face image. This can be considered as a challenge response or a motion password. The second type focuses

on certain movements without user interaction, such as eye blinking or lip movement. These movements are considered as signs of life; therefore, the face is real. H. K. Jee proposed a method for detecting the eyes in sequential input images, and it could be determined whether the input face was real by calculating the variation in each eye region (Jee et al. 2006). Kollreider et al. proposed the use of lip movement and lip reading as face landmarks for liveness detection (Kollreider et al. 2007). Sun et al. introduced a blinking-based approach for liveness detection using conditional random fields (CRFs) (Sun et al. 2007). A sign-of-life approach is very hard to spoof using 2D face images and 3D sculptures and is independent of textures. However, this approach may require user collaboration and depends largely on the detection of facial features.

The last approach, texture analysis, takes advantage of detectable texture patterns such as print failures and the overall image blur to detect attacks. Tan et al. introduced the Lambertian reflection model to discriminate genuine and fake faces (Tan et al. 2010). G. H. Kim tried to exploit the frequency and texture information by using the power spectrum and local binary pattern (LBP) (Kim et al. 2012). They assumed that the images taken from the 2-D objects tended to suffer from a loss in texture richness compared to the images taken from the 3-D objects. Moreover, the difference in the level of detail results in a difference in the micro-texture. Unlike the other two methods, the texture-based approach is easy to implement and does not require user collaboration. This approach works on the assumption that fake faces are printed on paper, and the printing process and paper structure produce texture features that differentiate printed faces from real face images (Yang et al. 2013). However, these assumptions may be false in many cases. At the Black Hat 2009 conference, Duc and Minh (2009) showed how attackers could break into laptops from Lenovo, Toshiba and Asus featuring face-recognition technologies, simply by using digitized images of legitimate users. The results presented by Maatta et al. using micro-textures have shown that the misclassified samples mainly consist of overexposed and very blurry images of a clients face (Mtt et al. 2011). Moreover, with the development of ultrahigh definition (UHD) displays and capturing devices, it is possible that the color reproduction through a UHD display is similar to real color. Therefore, an attack may be performed using a photograph displayed on a screen rather than on paper, which produces very little texture information. Thus, spoofing attacks using high-definition face video will become more common. In this study, we focus on spoofing attacks using high-quality face videos displayed on UHD display devices. In this paper, we provide the key ideas for resolving the main issues for liveness detection using face videos from a high-definition display.

3 Challenges for face recognition

A face recognition system generally consists of four modules: face detection, normalization, feature extraction, and matching.

Face detection segments the facial regions from the background. In addition, face normalization is performed to normalize the face geometrically and photometrically. Skin colors are often used to determine the face area because of the ease of implementation, but its performance is easily degraded by illumination changes. View-based methods achieve a very high performance for detecting faces against complicated backgrounds (Rowley et al. 1998; Sung and Poggio 1998). However, these methods consume a considerable amount of time owing to the exhaustive search of facial regions over the image. To solve these problems, some commercial engines used the generalized matching face detection method (GMFD), a modified generalized learning vector quantization (GLVQ) algorithm, which searches and selects face area candidates after the generation of potential eye pairs. GLVQ is based on a neural network and is not easily fooled by attempts to conceal identity via the usage of caps, hats, sunglasses, etc (Sato et al. 2005).

Face feature extraction is performed on the normalized face to extract the salient information that is useful for distinguishing the faces of different persons and is robust with respect to geometric and photometric variations. The extracted face features are used for face matching.

Last, in face matching, face recognition is performed by calculating the similarities or scores between a queried facial image and the enrolled facial images. Several methods have been proposed: extraction of the effective features from entire facial images based on a principal component analysis (Turk and Pentland 1991), extraction of the local features based on a local feature analysis (Penev and Atick 1996), and extraction of the relative positions of facial landmarks (Wiskott and Fellous 1997). However, local and global image variations are not explicitly taken into account in the previously discussed methods. Recently, one commercial engine has developed a standard face model to generate various facial appearances using the perturbation space method (PSM) algorithm. This face model consists of a 3D facial surface and a set of illumination bases. Moreover, the general range of facial poses and illumination has ceased to present major problems. However, the range of variation in different facial parts is still a challenge. To reduce the impact of adverse local changes (e.g., a varying facial expression caused by smiling and blinking eyes and intentional changes caused by wearing caps, hats, and glasses), the engine utilizes the adaptive regional blend matching (ABRM) algorithm, which reduces the impact of such local changes during the matching process (Sato et al. 2005).

Most face recognition engines focus on pose or lighting changes. Some engines are interested in live face detection. VeriLook is able to prevent this type of security breach by determining whether a face in a video stream is live or a photograph. The liveness score can be maximized with these actions carried out separately or together: moving the head around a bit, tilting the head, moving the head closer to or further from the camera, or slightly changing the facial expression. However, it is weak to spoofing attacks by face videos including motion.

Although VeriLook is considering live face detection, most of the existing commercial engines focus on the development of robust face recognition technology in the presence of lighting or pose changes and to account for the time difference between the probe image and the gallery image(s). In this paper, we compare the recognition performance of some existing commercial engines using live and fake faces according to the lighting direction. In addition, these results will help identify future research directions with regard to fake faces for the face recognition community.

4 Face databases

4.1 Existing fake face database

There are many fake face databases used for research on liveness face detection. The NUAA Photograph Imposter Database is a collection of face images for 15 subjects taken by generic, cheap webcams (NUAA Photograph Imposter Database 2010). This database contains various appearance changes commonly encountered by a face recognition system (e.g., gender, illumination, and with/without glasses). The photographs of live humans were taken using a digital camera and then developed into photographs. To collect various imposter photos, the photographs were moved, rotated, or bent horizontally or vertically. Unlike the NUAA database, the CASIA Face Anti-Spoofing Database focuses on a variety of collected data, providing a comprehensive collection from 50 subjects. Three fake face attacks were implemented, including a warped photo attack, cut photo attack, and video attack. This database also contains three imaging qualities: low, normal, and high quality. Another database, the Replay-Attack Database by the Idiap Research Institute consists of 1300 video clips of photograph and video attack attempts on 50 clients, taken under different lighting conditions (Chingovska et al. 2012). All videos were generated by having a real client try to access a laptop through a built-in webcam or by either displaying a photograph or a video recording of the same client.

Despite the fact that the existing fake face databases include video attacks, the quality of the images and videos were not sufficiently high to display through UHD monitors.

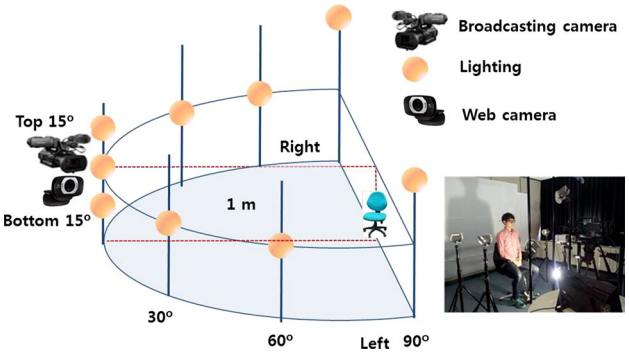

Fig. 2 Environment for capturing face videos

Therefore, ultrahigh-resolution face videos are needed so we can display fake faces similar to live faces.

4.2 Capturing face videos from live faces

Our database is a collection of face videos taken by a 2K broadcasting camera and cheap webcam. To eliminate the influence of outside light, we covered the windows in a small studio room with dark curtains. Nine lights were used as directional light sources to achieve various lighting conditions. The locations of the lights are shown in Fig. 2 (Cho and Jeong 2014). All light sources are a subject located 1 m away.

We captured UHD videos using a 2K broadcasting camera. A webcam was simultaneously used to capture images of a live face so we could compare the performance because most face recognition systems use a generic webcam. The face took up at least two-thirds of the entire area of the sequences. The height of the camera was fixed, and we controlled the height of the chair depending on the subjects height. We asked each subject to sit on this chair, look into the camera, and perform natural movements such as speaking, smiling, or blinking. We captured images with the camera and webcam while turning one light on at a time.

The face database is divided into two groups according to purpose: registration and test purposes. The faces for registration purposes were captured under normal lighting conditions without motion. The faces for test purposes were collected under various directional lighting sources conditions with natural motion. There were 60 registration-purpose video clips and 540 test-purpose video clips from a total of 60 subjects. Figure 3 shows face videos from live faces.

For each configuration, the video clips from the 2K broadcasting camera were captured at a rate of 30 fps and a resolution of 1920×1080 pixels, and each clip lasted approximately 5 s. Live face video clips from the webcam were captured a resolution of 864×480 pixels. Compared to other databases, our database is more challenging because it includes images captured under various lighting conditions,

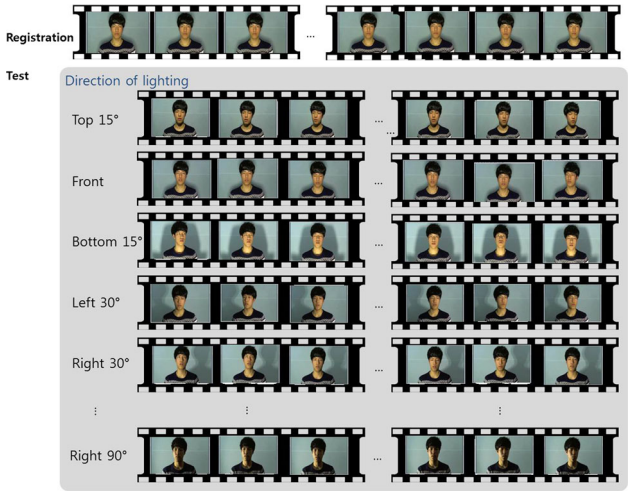

Fig. 3 Face videos from live faces

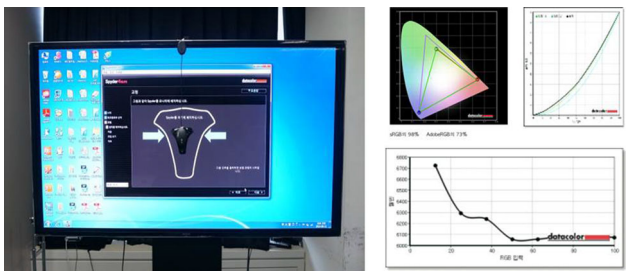

Fig. 4 Calibration of the UHD monitor

including poor lighting conditions such as the light source positioned 90° to the left/right of the subject.

4.3 Fake face database

To test the strength of face recognition systems against video imposters, high-quality face videos captured with the 2K broadcasting camera were displayed on a high-definition monitor and then recaptured via a web camera that was the same as the web camera used for capturing live faces. We displayed the original video on a 50-inch LED monitor to provide an output with a face size similar to a live face.

To ensure a proper display output similar to a live face, the UHD monitor has to be calibrated according to the criteria for color management and standard image reproduction stated in ISO 15076-1:2010 (2010). Further, the UHD monitor was characterized using a 2.2 gamma tone reproduction curve and a D65 white-point color temperature according to IEC 61966-2-1:1999 (1999), which contains the sRGB and HDTV color-space standards. Figure 4 shows the setup for the calibration of the UHD monitor using Spyder in a dark room and the characterized features such as the color gamut, gamma, and white point.

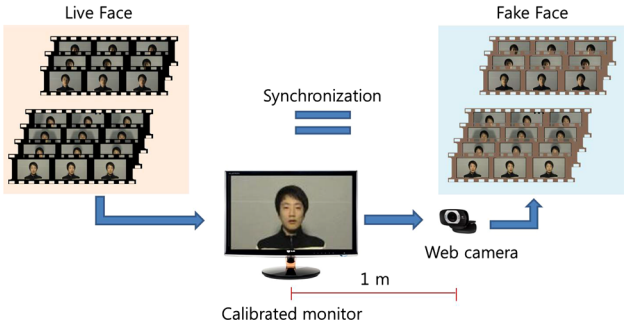

Fig. 5 Synchronization and recapturing fake faces

The color gamut refers to the range of colors a device can reproduce. Usually, a larger or wider gamut means that more rich saturated colors are available, and we recommend the use of a monitor that satisfies over 98 % of the sRGB color gamut. The gamma is important factor for representing the highlighted and shadowed regions. We will describe this in detail in the Sect. 6. The standard monitor white point is D65, which means that the color temperature is 6500 K in daylight.

The calibrated monitor displayed face videos similar to a real face size. The web camera recaptured the face videos from the UHD monitor located 1 m away in the same environment used for capturing real faces. Each video clip was recaptured at 30 fps at the original resolution (864 × 480 pixels), with each clip lasting approximately 5 s (the same length as the original live face video). Before we conduct the performance comparison experiment, we synchronized both the live and fake face videos. The synchronization of both live and fake face videos is shown in Fig. 5.

5 Experiment

5.1 Overview

In previous work, we registered live face images and then compared the recognition results of live faces with the results of high-definition fake face videos from LED display devices (Cho and Jeong 2014). However, the previous work missed the spoofing attack of registration due to stolen or duplicated facial data. In this study, we expand on our previous work and compare the cross-recognition test results from the perspective of face recognition performance.

Figure 6 shows the cross-recognition test method using live faces and fake faces. The face recognition system consists of two parts: registration and recognition. There are four cases depending on which images are registered or recognized. For example, the result L-F means that the face recognition system registered live faces and then obtained recognition results from fake faces.

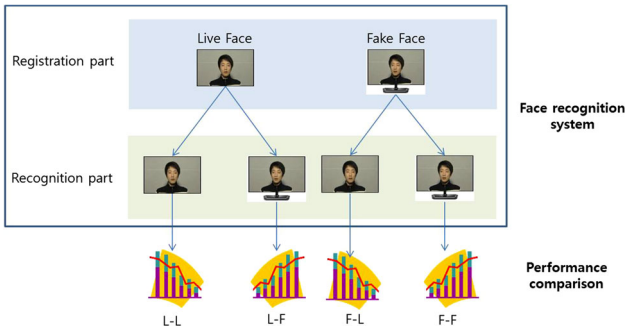

Fig. 6 Experiment overview

Table 1 Overall face recognition performance comparison

Engine	Recognition rate (%)				Variation
	F-F	F-L	L-F	L-L	
A	78.75	74.12	75.13	73.80	5.16
B	93.39	96.79	94.02	97.47	4.05
C	54.70	57.13	53.57	58.79	5.54
D	33.71	36.32	35.56	31.06	5.47

5.2 Results

We tested four different face recognition engines used for commercial purposes. Each engine registered five face images from the registration-purpose videos. Each test engine obtained recognition results from every frame in the live and fake face videos, and we calculated the recognition rate from the detected faces only. Table 1 summarizes the overall performance comparison for each engine.

Each engine exhibited similar recognition results, regardless of whether the face was live or fake, with all engines having a variation less than 5.54. Engine B and Engine C exhibit the highest results in the L-L test. On the other hand, Engine A exhibits higher results in the tests using fake faces than the L-L test. The performance of Engine D is the highest in the F-L test. Although each engine exhibited different recognition performance depending on the properties of the engine, there is no significant difference in the face recognition performance when using fake face videos instead of live faces.

Figures 7, 8 9 and 10 show the performance changes according to the lighting direction for each engine. The recognition rate (RR) and detection rate (DR) are plotted along the *y* axis, and the lighting direction is plotted along the *x* axis, with poorer lighting conditions towards the left. For Engine A, the recognition performance of both live and fake face videos drastically declined under left/right-side 60° lighting. The performance of Engine B was generally good except for left/right-side 90° lighting. The performance of Engine C was similar to that of Engine A. For Engine D, it is impossible to recognize faces under left/right-side 60° or 90° lighting. Generally, the face recognition performance deteriorates under poor lighting conditions. However, the coverage range for the lighting direction is different. If the lighting coverage range of the engine is wide, it is regarded as a good recognizer.

The face recognition performance results are similar under good lighting conditions. However, the performance gaps between live and fake faces under poor lighting conditions increased irrespective of whether the engine is good or not. In other words, secure face recognition systems without a costly camera installed (e.g., stereo, infrared camera, etc.) will not be able to differentiate live faces from not live faces under good lighting conditions.

6 Discussion

We know that the performance gaps between live and fake faces under poor lighting conditions increase from the experiment. Thus, we focus on why the gaps in the recognition rates increase under local lighting conditions. Generally, there are no features for face detection or recognition in highlighted and shadowed regions. Figure 11 shows a comparison of the average histograms of live and fake face images under 90° left-side lighting conditions. The histogram shows the num-

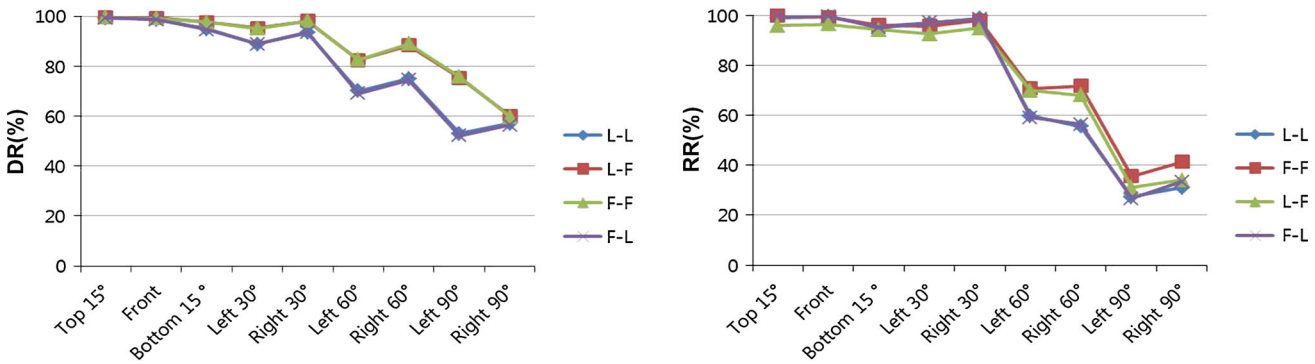

Fig. 7 Change in the performance of Engine A

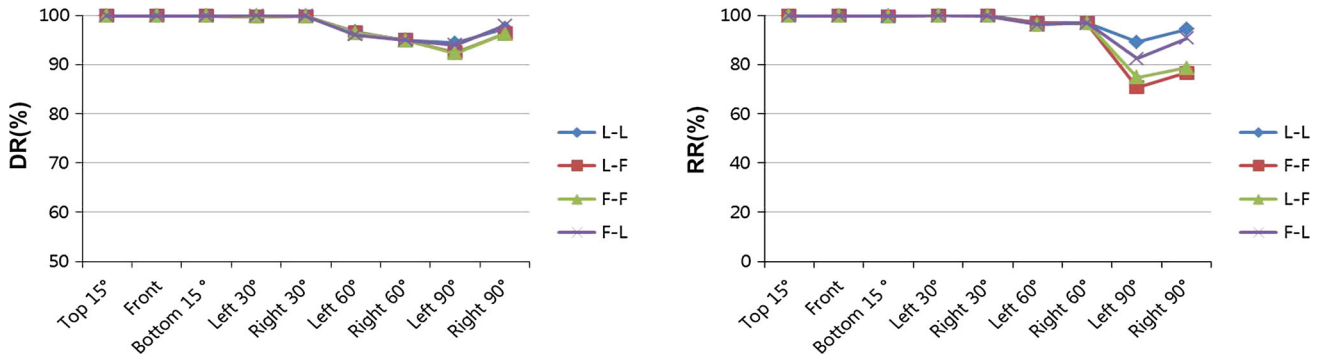

Fig. 8 Change in the performance of Engine B

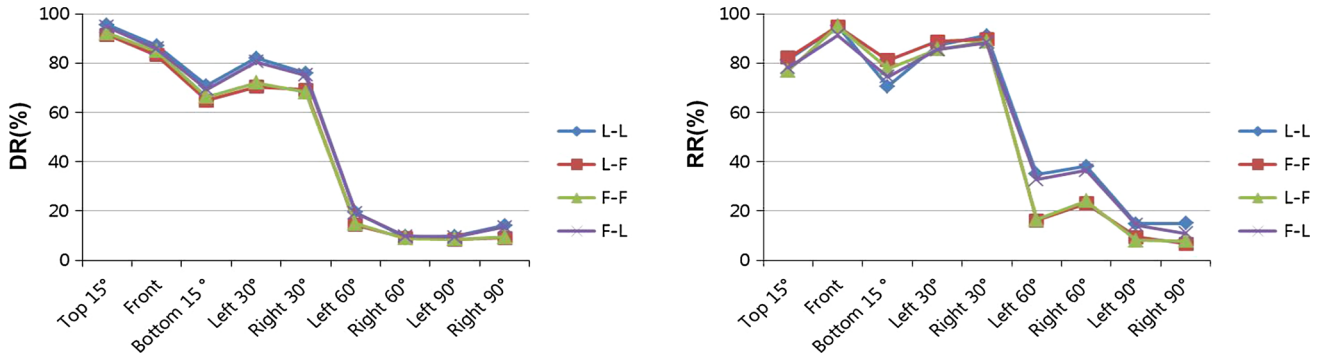

Fig. 9 Change in the performance of Engine C

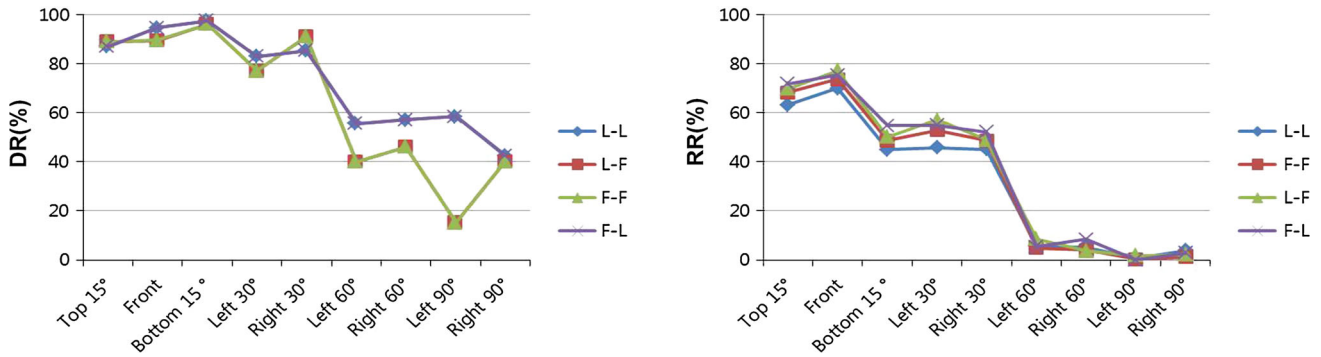

Fig. 10 Change in the performance of Engine D

ber of pixels in an image at each different intensity value found in that image, and the pixel intensity is plotted along the x axis, with darker color towards the right. From this, we can see that fake face images have more shadowed regions than live face images.

We can consider the gamma to solve this problem. Gamma defines the relationship between a pixel's numerical value and its actual luminance. Originally, gamma correction was used for human vision under common illumination conditions, with a greater sensitivity to the relative differences between darker tones than between lighter ones (Wiskott and Fellous 1997). In most computer display systems, images are encoded with a gamma of approximately 0.45 and decoded

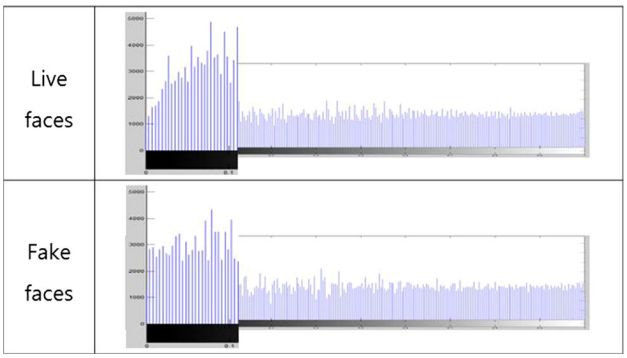

Fig. 11 Average histogram of face images under 90° left-side lighting conditions

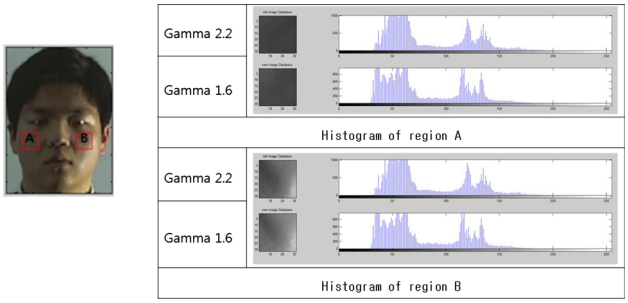

Fig. 12 Histograms of the highlighted and shadowed regions

with a gamma of 2.2. However, this is not optimized for cameras but for human vision. Figure 12 shows a comparison the histograms of highlighted and shadowed regions according to the gamma. The face image after adjusting the gamma value of the display has greatly improved the shadow or highlight details. If the facial images have been enhanced by adjusting the features of a display such as the gamma or lighting, it will be another issue for fake face recognition.

7 Conclusion

With the development of UHD displays and capturing devices, spoofing attacks using high-definition face video will become more common. In this paper, we compared the recognition performance using live faces and high-definition fake face videos from display devices. As a result, there are no performance gaps between live and fake faces under good lighting conditions irrespective of whether the engine is good or not. In addition, we analyzed the histograms of images under local lighting conditions and guided future research directions regarding fake faces. In our future work, we will conduct further research on the low-level aspects of fake face recognition such as the color difference, rather than on the performance aspects.

Acknowledgments This work is supported partly by the R&D program of the Korea Ministry of Trade, Industry and Energy(MOTIE) and the Korea Evaluation Institute of Industrial Technology (KEIT). (Project: Technology Development of service robots performance and standardization for movement/manipulation/HRI/Networking, 10041 834).

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Bao W, Li H, Li N, Jiang W (2009) A liveness detection method for face recognition based on optical flow field. In: Proceedings of the 2009 International Conference on Image Analysis and Signal Processing, Taizhou, China, pp 233–236

"CASIA Face Anti-Spoofing Database" (2012). http://www.cbsr.ia.ac.cn/english/FaceAntiSpoofDatabases.asp

Chakraborty S, Das D (2014) An overview of face liveness detection. Int J Inf Theory 3(2):11–25

Chingovska I, Anjos A, Marcel S (2012) On the effectiveness of local binary patterns in face anti-spoofing, Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the, IEEE

Cho M, Jeong Y (2014) Face recognition performance comparison of fake faces with real faces in relation to lighting. J Internet Services Inf Secur (JISIS) 4(4):82–90

Datacolor, "Spyder4ELITE". http://spyder.datacolor.com

Duc NM, Minh BQ (2009) Your face is not your password face authentication bypassing lenovoasustoshiba, Black Hat Briefings

Idiap Research Institute, "The Replay-Attack Database" (2012). https://www.idiap.ch/dataset/replayattack

IEC 61966-2-1:1999 (1999) Multimedia systems and equipment Colour measurement and management Part 2-1: colour management

ISO 15076-1:2010 (2010) Image technology colour management—architecture, profile format and data structure—Part 1: Based on ICC.1:2010

Jee HK, Jung SU, Yoo JH (2006) Liveness detection for embedded face recognition system. Int J Biol Med Sci 1(4):235–238

Kim G, Eum S, Suhr JK, Kim DI, Park KR, Kim J (2012) Face liveness detection based on texture and frequency analyses, 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, pp 67–72

Kim S, Yu S, Kim K, Ban Y, Lee S (2013) Face liveness detection using variable focusing, Biometrics (ICB), 2013 International Conference on, pp 1–6

Kollreider K, Fronthaler H, Faraj MI, Bigun J (2007) Real-time face detection and motion analysis with application in liveness assessment. IEEE Trans Inf Forensics Secur 2(3):548–558

Kollreider K, Fronthaler H, Bigun J (2005) Evaluating liveness by face images and the structure tensor. In: Proceedings of 4th IEEE Workshop on Automatic Identification Advanced Technologies, Washington DC, USA, pp 75–80

Lagorio A, Tistarelli M, Cadoni M (2013) Liveness detection based on 3D face shape analysis, Biometrics and Forensics (IWBF), 2013 International Workshop on, pp 1–4

Li SZ, Jain AK (2011) Handbook of face recognition, Chapter 1. Springer, New York

Mtt J, Hadid A, Pietikainen M (2011) Face spoofing detection from single images using micro-texture analysis, Biometrics (IJCB), 2011 international joint conference on, IEEE

Neurotechnology, "VeriLook". http://www.neurotechnology.com/verilook.html

"NUAA Photograph Imposter Database"(2010). http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html

Pan G, Wu Z, Sun L (2008) Liveness detection for face recognition, recent advances in face recognition. INTECH Open Access Publisher, pp 109–124

Penev P, Atick J (1996) Local feature analysis: a general statistical theory for object representation, Netw Comput Neural Syst: 477–500

Rowley H, Baluja S, Kanade T (1998) Neural network-based face detection. Pattern Anal Mach Intell IEEE Trans 20(1):23–38

Sato A, Imaoka H, Suzuki T, Hosoi T (2005) Advances in face and recognition technologies. NEC J Adv Technol 2(1):28–34

Sung KK, Poggio T (1998) Example-based learning for view-based human face detection. Pattern Anal Mach Intell IEEE Trans 20(1):39–51

Sun L, Pan G, Wu Z, Lao S (2007) Blinking-based live face detection using conditional random fields, ICB 2007. International Conference, Seoul, Korea, 27–29 Aug 2007, pp 252–260

Tan X, Li Y, Liu J, Jiang L (2010) Face liveness detection from a single image with sparse low rank bilinear discriminative model, Computer Vision ECCV 2010. Springer, Berlin Heidelberg

Turk M, Pentland A (1991) Eigenfaces for recognition. J Cogn Neurosci 3(1):71–86

Wiskott L, Fellous JM et al (1997) Face recognition by elastic bunch graph matching. Pattern Anal Mach Intell IEEE Trans 19(7):775–779

Yang J, Lei Z, Liao S, Li SZ (2013) Face liveness detection with component dependent descriptor, Biometrics (ICB), 2013 International Conference on, pp 1–6