Intelligent Automation And Soft Computing, 2020

Vol.26,no.1,133–139
https://doi.org/10.31209/2019.100000134

Distinction Between Real Faces and Photos by Analysis of Face Data

Byong Kwon Lee[1], Yang Sun Lee[2]

[1]Dept. of Multimedia Engineering, College of Engineering, Dongguk University, Seoul, 04620, South Korea
[2]Div. of Convergence Computer & Media, Mokwon University, Daejeon, 35349, South Korea

ABSTRACT

Biometric user authentication using the face has been applied mainly to access control systems. However, access is allowed even when a photo is presented instead of an actual face. This can facilitate illegal access including attending as a substitute or substitute authentication. An alternative approach has been implemented to solve this problem. The approach determines between a real face and a photo of a face using a UV sensor but this requires substantial cost and installation process because additional hardware (the UV sensor) is necessary. This paper proposes a three-step approach to identify between a real image and a photo. Step 1 determines authenticity using the background data and eliminating the face data. Step 2 determines authenticity using eyelid blinking on the face and facial gestures. Step 3 authorizes the user by extracting the feature points on the face.

KEY WORDS: Virtual Reality, Mobile HMD, Multi-Kinect

1 INTRODUCTION

ACCESS control systems using user face recognition authorize the user by analyzing the feature points on a face using biometrics (Chowdhury, M. et. al., 2017). Most access controls to date use the ID-PASSWD approach. This approach has serious risk for exposure. Users may forget their ID or a password in some cases. When a password changes, login fails. It is increasingly necessary to find new authentication means with less risk of forgetting, loss, theft or reproduction. The approach drawing the most attention is 'biometrics', using a part of the human body. The 'biometrics' approach is characterized by the fact that a part of an individual's body is the unique property of that person and can be never lost.

Biometrics enable the creation of the strongest 'personal authentication means' (Marqués, I. and Graña, M., 2012). For example, biometrics using fingerprints or the iris is used for Apple iPhones and Samsung Galaxy Note 7 as the locking or unlocking means.

However, the existing authentication system implements face recognition on the condition that this data are read in real time. The accuracy of face identification is 99.96% for Google 'Face Net' (Florian Schroff et. al., 2015) and 97.25% for Facebook 'DeepFace' (Yaniv Taigman et. al., 2014).

This paper investigated a method for identifying between the actual face and a facial photo with the input image and face recognition.

Section 2 examines the relevant research while Section 3 explains the methodology proposed in this paper. Section 4 executes the test using the method proposed in this paper and Section 5 explains the conclusion.

2 RELATED WORK

2.1 Histogram Tone Range

THE color space of the image used for the histogram "Tone Range" is basically composed of red, green and blue (Standard Color Space). In addition, each of the RGB color spaces has a brightness level of 0 to 255, and the storage unit is basically represented by 1byte (8 bits). RGB histogram extraction converts the color space into a brightness value, expressed in RAW data format, and expressed as a digital value ranging from 0 to 255. Figure1 shows the brightness from 0 to 255 in RGB Color Space. It is classified as "Shadows", "Midtones" and "Highlights". (Limei Fu, 2018).

CONTACT Yang Sun Lee yslee48@gmail.com

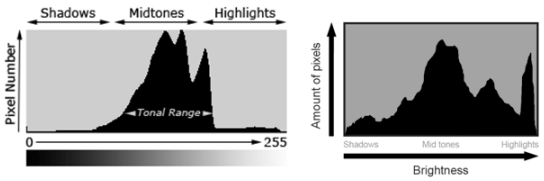

Figure 1. **Histogram Tone Range**

The "Tonal Range" is expressed differently for each image and it is important to express meaningful values for the image. In this paper, we used "Tonal Range" as a basis for judging the authenticity. However, the histogram expression mentioned above does not have an ideal histogram in which any image is 100% matched to the real world, only to find a similar value (approximate).

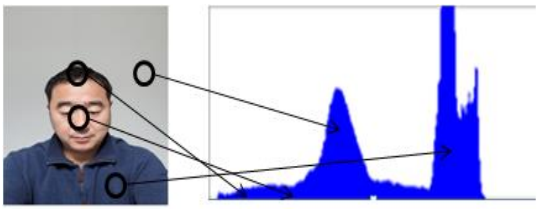

Figure 2. **Histogram Tone Range of Face Image**

Figure 2 shows the matching of the "Tonal Range" in the histogram for the real face image. The data is expressed in RAW form of the RGB color space for the brightness level of the face image. In this paper, a histogram of 0 to 255 levels for red, green, and blue is shown in the RGB color space. We analyzed the "Tonal Range" of the face image and judged the authenticity of the actual face image and the photographic image.

2.2 Image-Based Face Recognition Algorithms

PCA finds the principal component in the distributed data (Arash Saboori and Javad Birjandtalab, 2016). More specifically, when data on 'n' points (x1,y1), (x2,y2), ..., (xn,yn) forms an oval shape on 2D coordinates as shown in the figure below, what is the method for explaining the data distribution features using two vectors most clearly? As shown in Figure 3, the best method to explain this is to explain data distribution using two vectors, e1 and e2. When the direction and size of e1 and e2 are identified, the shape of data distribution can be identified most easily and effectively. PCA is used not to analyze each element of data but to analyze the principal component of the distribution when multiple data form one distribution together. The principal component means the direction vector with the biggest data distribution in that direction. In Figure 3, data distribution (scope of dispersion) is the largest along the direction of e1. The direction with the second largest distribution is e2, which is perpendicular to e1.

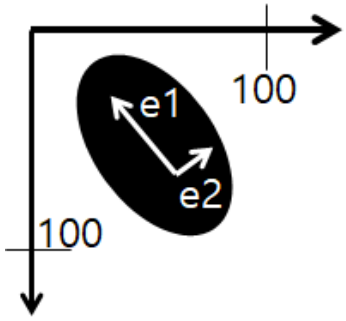

Figure 3. **PCA Example in 2D**

ICA (independent Component Analysis) is similar to PCA analysis in the aspect that it selects only those features that have significant impact on the classification of features for solving difficult problems because of an overly large dimension of features. However, ICA adopts the approach to identify new features from the given features since it is difficult to classify the specific zones on the whole face only with given features. ICA can make up for the disadvantages of PCA analysis by identifying the new features including statistically significant independent elements from the features which are not classified (M.S. Bartlett, 2002).

LDA (Linear Discriminant Analysis) reduces the dimension of a specific vector related to data using the approach of maximizing the ratio of between-class scatter to within-class scatter) (Muhammad Ali Akbar, 2016). Figure 4(a) is easier to read than Figure 4(b) because data in the same class are clustered around the center and the distance between the centers of each class is far away. As explained above, LDA reduces the dimension by mapping around the axis that maximizes the class separation (maximal separability) as the main axis in a specific space for maintaining the differentiation data between classes as much as possible.

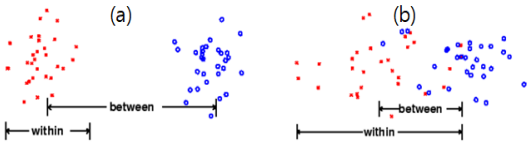

Figure 4. **(a) Data Distribution Easy to Read (b) Data Distribution Difficult to Read**

The Hidden Markov model (HMM) (Josh Hanna et. al, 2012) is one of the statistics models for determining the hidden parameter from the parameters measured on the basis of the assumption that the modeling system is the Markov process with unknown parameters. The parameters of the identified model can be used for better analysis. One example is pattern recognition. In the Regular Markov model, an operator can directly see the status. Then, these state transition

probabilities are the only parameters. However, the Hidden Markov model adds outputs: Each state has probability distribution for available output tokens. Accordingly, the sequence of states cannot be directly identified by observing the sequence of tokens generated by HMM. In other words, it is called the Hidden Markov model because it is applied when the sequence of states is not observed and only outputs are observed. The HMM is applied in Real Time Speech Recognition Application, Optical Character Recognition(OCR), Real world Natural Language Processing and basically Bioinformatics.

2.3 *Eye-blink detection system*

Haar is handled by convolving images of different sizes and orientations (Figure 5). Haar is a prototype cluster of edge, line and center surround masks. The shape for the prediction can be calculated as two or three rectangles.

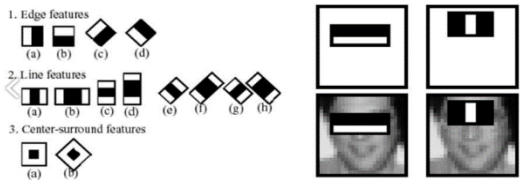

Figure 5. **Haar-like features**

The Haar feature basically uses the difference of brightness between zones in the images (Shigang Chen et. al, 2011). As shown in the figure on the bottom left, there are elementary features in various shapes. The features of the objects are extracted by combining (in various locations and sizes) multiple elementary features (hundreds and thousands). The feature value of each elementary feature is estimated by deducting the brightness of the dark zone from the total brightness of the image pixels corresponding to the white zone in the feature. Identification of an object using the feature judges whether the calculated brightness difference of the zone is larger or smaller than the threshold assigned to that feature. This approach does not use only one feature but combines and applies multiple features. For example, when the feature is f1, f2, ..., and fn, and f1<t1, f2<t2, f3>t3, ... and fn<tn are satisfied, it is the target object. When those conditions are not satisfied, the image is determined as background. Since even the same kinds of features are considered to be different depending on the location and size (scale) in an object, features can be infinitely combined. It is important to select significant features among them. The significant features mean those features generating similar values for the objects to be identified and random values for the objects that are not targeted.

The active approach to eye-blinking detection provides very accurate results, and the method is robust (Borna Noureddin et. al, 2012).

The benefits of IR-based eye-control human-computer interfaces are balanced by high end-user costs due to special hardware. In addition, the recognition of the IR form is not effective in the outdoor environment due to the influence of direct sunlight on the IR illumination. Prolonged exposure of the eye to IR can cause eye damage, which can cause health problems with the use of the system (Bin Li and Jian Wang, 2013).

3 PHOTO AND REAL TIME IMAGE

FOR a verification system using a real-time face image, some may try to get access to the system using a fake photo for illegal access or attending as a substitute. To prevent this type of illegal access, a verification system with mounted a IR sensor is introduced (Dongshi Xia and Zongcai Ruan, 2007). Figure 6 presents access using both a photo and a real-time. Figure 6(a) is a verification attempt using a photo, not a real-time face image. Figure 6(b) is a verification attempt using a real face.

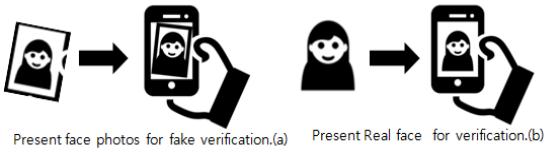

Figure 6. **Photo and Real face for Access Control**

This paper proposed an approach to identify the real face and the face photo to minimize the risk of access using a copied photo as shown in Figure 6(a). The proposed approach checks the amount of change by separating the face and the background, displaying the histogram using RGB (Red, Green, Blue) and comparing the histogram value that is actually entered and the value that has been saved in advance. Figure 7 determines forgery using the change data by producing a histogram in Red, Green and Blue using the face and background data captured for verification. The Histogram Tone Range proposed in the relevant research is compared and analyzed. The proposed algorithm extracts the RGB values obtained from the image within the range of 0 ~ 255 and selects it as the sample data to judge whether or not the image is falsified.

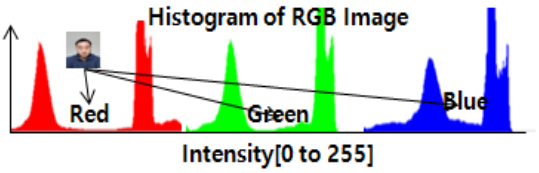

Figure 7. **A Histogram of face RGB Image**

Figure 8 displays the diagram of the whole process classifying the presented photo and the face image. 1 Pass_Filter classifies the photo and the real face. 2

Pass_Filter recognizes the face on the basis of the image data collected by 1 Pass_Filter.

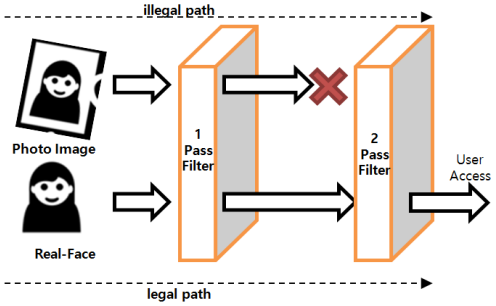

Figure 8. A Process Illegal and legal path

Fig 8, illegal paths that present photographic images pass only 1 Pass_Filter and 2 Pass_Filter rejects. The legal path is that the real face is presented and passes through the filter. 2 Pass_Filter recognizes a face by analyzing the facial feature points. Finally, the authentication is completed by comparing the registered user facial feature data.

3.1 *Collection of face feature data for verification*

The collection of face feature data for verification is the process of collecting user information for using the system at first. It is the process of separating the background and the face and extracting the background information and feature points of the face. Figure 9 presents the process of collecting the basic data required for verification. The data on the face feature points and background collected from a camera are separated and saved in the database. The face feature data saved are used as the feature point data for verifying the face in 2 Pass-Filter as shown in Figure 8.

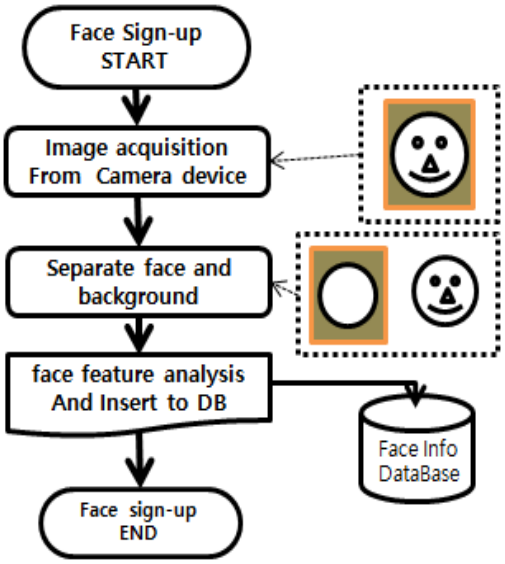

Figure 9. The authentication data collection procedure

3.2 *Classification of a photo and real face*

There is an active approach for classifying a face photo and a real face. This approach checks the change by comparing the background information of the face taken by the camera and that of the face saved in the database. However, the approach uses the camera installed on the access door and is used when the background is fixed. Figure 10 illustrates the face photo on the left and the comparison of RGB change by extracting the histogram with the image collected from the camera.

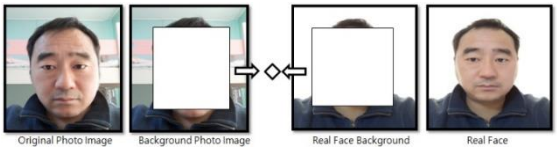

Figure 10. Background Information Comparison of Face

The other approach is to check the histogram change by issuing a motion command to the user through manual authentication and then analyzing the motion of the user's face. Another approach checks the eye blinks. Figure 11 shows the diagrams of the active approach and the passive approach.

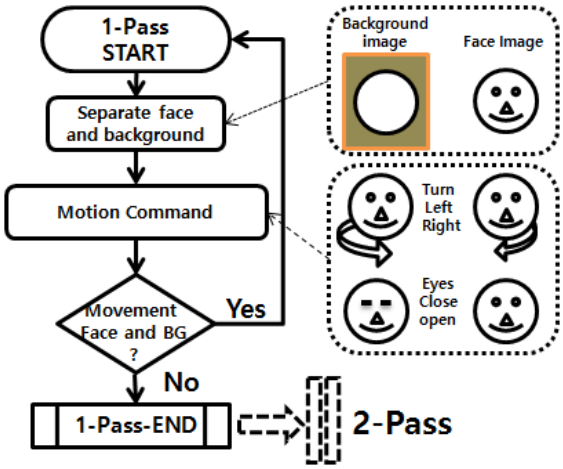

Figure 11. Procedures for Active and Manual Authentication Approaches

The approach for checking the eye blink in the proposed approaches provides a reference point with the requirements as shown in Figure 12. In accordance with the test, the value between 0.0 and 0.79 is determined as 'eyes closed' and the value between 0.8 and 1.0 as 'eyes open', which accomplished the best effect. For verification, LandMark was extracted from the user's face image in the screen zone and whether the left and right eyes were opened or closed was analyzed by eye tracking. Eye tracking was configured to return '-1' (eye reading failed), '0.0' (eye completely closed) and '1.0' (eye opened) depending on the user's eye status in real time. The face photo

and the real face were classified because the face photo had no eye blink.

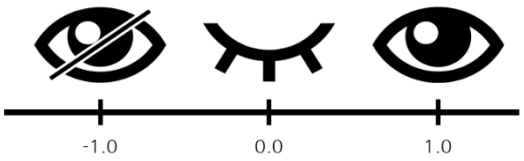

Figure 12. invalid, close and open of eyes

3.3 Face Recognition and Authentication

Recognition of feature points on the face executes the authentication process using the feature points collected through 1 Pass_Filter. 2 Pass_Filter, the face recognition process (Fig 13), is illustrated in the diagram after the 1 Pass_Filter recognizes the photo. The 2 Pass_filter recognizes the face using the information on the facial feature points extracted in the 1 Pass_Filter. If no data on the feature points are found through search, repeat database update. Data from the final search are applied to the access control system.

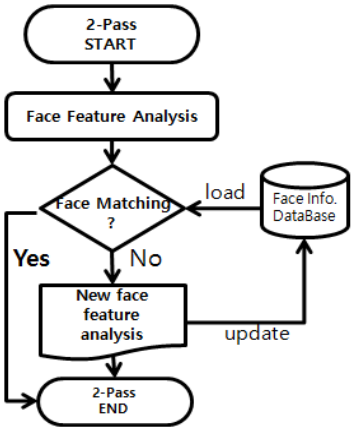

Figure 13. Face Recognition Process

4 EXPERIMENT

THIS paper proposed the active(automatic) authentication approach and the passive authentication approach on the face photo and the real face. The active approach separates the background and face shape on the basis of the presented face image and compares background histogram. The passive approach determines whether it is the real face or the face photo using the motion commands (turning a face, blinking eyes).

Figure 14 shows the process by which 1 Pass_Filter actively (automatically) determines whether it is a photo of a face or a real face by comparing the histogram RGB. For the test, commands were randomly given to the user including 'turning head (to the left or to the right)'. When the change of the histogram is over the threshold, 'Pass' is activated. If not, 'noPass' is activated.

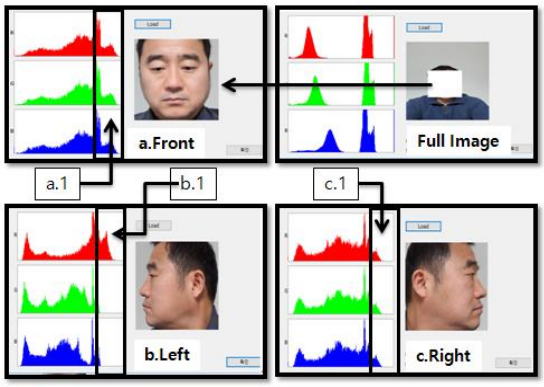

Figure 14. Tone Range of Highlighted Area of Real Face

Figure 14 compares the highlighted areas, shadow, mid-tone and highlighted areas, the three kinds of tone areas in the histogram. Since the number of pixels such as a.1>b.1, or a.1>c.1 is smaller, the photo of a face and the real face are classified. Figure 15 presents the opposite case to that of Figure 14. In Figure 15, the number of pixels on the highlighted area was increasing. In conclusion, the number of RGB pixels was rapidly increasing when the real face was recognized. It was determined as the criteria for determining truth and fiction.

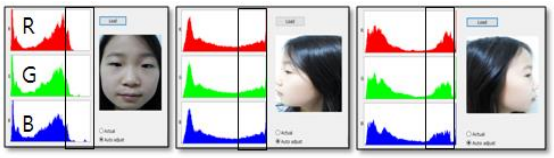

Figure 15. Tone Range of Highlighted area of Real Face

Figure 15 presents the results from the test determining true and false by checking eye blink as a passive approach. To determine test objectivity, one adult and one child were selected for test. The optimum range demonstrating the highest recognition rate in the test was 0.8~1.0 when eyes were opened and 0.0~0.79 when eyes were closed. Figure 16 shows the result of an adult eye blink and Figure 17 shows the result of a child eye blink. Figure 18 displays the change of recognition when the left and right eyes were repeatedly blinked. In conclusion, the optimum range of 'eyes opened' was over 0.8. Using this range, the truth or falsehood of the face presented for authentication was determined.

Table 1 Face Size of a Child and an Adult

State (Range)	Left Eye	Right Eye
Open (0.80~1.00)	0.99 (a,f)	0.98 (a,f)
	0.96 (d,i)	0.86 (c,h)
Close (0.00~0.79)	0.56 (c,h)	0.24 (d,i)
	0.20 (b,g)	0.31 (b,g)
Invalid (-1.00)	-	-1.0(e,j)

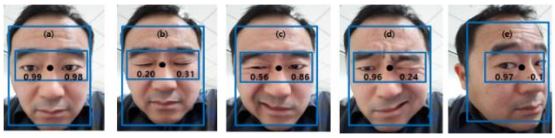

Figure 16. Eye Motions on an Adult Face

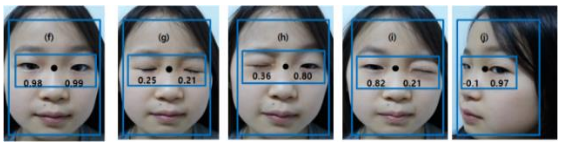

Figure 17. Eye Motions on a Child Face

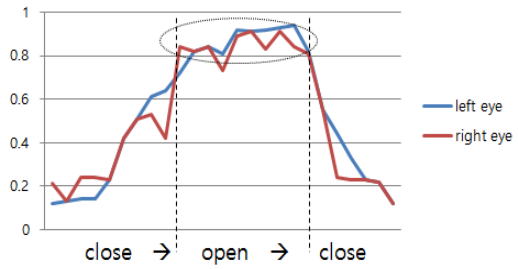

Figure 18. Eye Blink Change

The final step is 2 Pass_Filter, the face recognition and authentication process. The authentication process is executed by comparing the feature points of a face entered in real time and those saved in the database.

(a) Figure 19 is the original face image collected from the image collection device and (b) recognizes the face zone using OpenCV. (c) extracts the crop and feature points by extracting the face zone. (d) compares the feature points of the real face and those in the database. (e) is the database with feature points of the user's face. Finally, (d) determines the face. This process was implemented using the existing Face OpenCV Library.

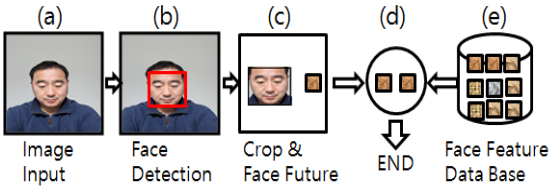

Figure 19. Real Time Face Detection

5 CONCLUSIONS

WHILE existing authentication research using face recognition has been focusing on the face in most cases, illegal authentication can be issued when the photograph of a face is presented. While the signals from a body were analyzed using an IR sensor for solving this problem, this process requires substantial cost and is difficult to maintain and repair.

This paper proposed an active approach and a passive approach for identifying between a photo of a face and a real face. The active approach recognized the real face by separating the background and the face and comparing the change of background. Furthermore, motions requested by motion commands were analyzed in the passive approach. Truth or falsification was determined by classifying 'open' or 'close' depending to the range of eye blink. This approach solved the issue caused by face photos in the existing face recognition system. The application field of this paper can be applied to access control field which requires high recognition rate at low cost.

In addition, it can be provided as an optimal solution for attendance management and student management at school.

Further study must investigate an intelligent access control system that can accurately recognize face and background using Deep Learning technology. Also, it is considered that a solution to the personal information (face data, facial contour data) stored in the face recognition database.

6 DISCLOSURE STATEMENT

NO potential conflict of interest was reported by the authors.

7 REFERENCES

Chowdhury, M., Gao, J., Islam, R. (2017). Biometric authentication using facial recognition. *SecureComm 2016. LNICST*, 198, 287–295. https://doi.org/10.1007/978-3-319-59608-2_16

Marqués, I., Graña, M. (2012). Image security and biometrics: a review. *HAIS 2012. LNCS (LNAI)*, 7209, 436–447. https://doi.org/10.1007/978-3-642-28931-6_42

Florian Schroff, Dmitry Kalenichenko and James Philbin (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering, *in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2015*. pp. 815–823.

Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato and Lior Wolf (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification, *2014 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1701–1708.

Limei Fu (2018). Particle Filter Pedestrian Tracking Algorithm Based on Selected Region RGB

Histogram, *2018 International Conference on Robots & Intelligent System (ICRIS)*, pp.287-290.

Arash Saboori, Javad Birjandtalab (2016). Remote sensing image data fusion using spatial PCA and average block-DCT, *Signal Processing and Communication Systems (ICSPCS) 2016 10th International Conference on*, pp. 1-7.

M.S. Bartlett, J.R. Movellan and T.J. Sejnowski (2002). Face Recognition by Independent Component Analysis, *2002 IEEE Trans. on Neural Networks*, 13(6), pp. 1450-1464.

Muhammad Ali Akbar, Amine Ait Si Ali, Abbes Amira (2016). An Empirical Study for PCA- and LDA-Based Feature Reduction for Gas Identification, *IEEE SENSORS JOURNAL*, 16(14), pp. 5734-5745.

Josh Hanna, Fatma Patlar, Akhan Akbulut, Engin Mendi, Coskun Bayrak (2012). HMM based classification of sports videos using color feature, *6th IEEE International Conference Intelligent Systems*, pp. 388–390.

Shigang Chen,Xiaohu Ma, Shukui Zhang (2011). AdaBoost Face Detection Based on Haar-Like Intensity Features and Multi-threshold Features, *2011 International Conference on Multimedia and Signal Processing*, 1, pp.251-255.

Borna Noureddin, Peter D. Lawrence, Gary E. Birch (2012). Online Removal of Eye Movement and Blink EEG Artifacts Using a High-Speed Eye Tracker, *2012 IEEE Transactions on Biomedical Engineering*, 59, pp.2103-2110.

Bin Li, Jian Wang (2013). Human eye characteristics in IR-based eye detection, *2013 IEEE International Conference on Consumer Electronics – China*, pp.1255-1260.

Dongshi Xia, Zongcai Ruan (2007). IR Image Based Eye Gaze Estimation, *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, 1, pp.220-224.

8 NOTES ON CONTRIBUTORS

Byong Kwon Lee received the B.S. degree in computer engineering from Hanbat University, Daejon, Korea in 2000, and the M.S. degree in computer engineering from Hannam University, Korea in 2002, also Ph.D. degree in Dept. of IT engineering from Chungbuk National University, Korea in 2007. He has worked as an Assistant Professor in Dept. of Multimedia Engineering, College of Engineering Dongguk University, in Korea. His current research interests in fuzzy-neuro computing, image processing, multimedia computing and Embedded System.

Yang Sun Lee received the B.S. and M.S. degrees in Electrical & Electronic Engineering from Dongshin University and Ph. D. degrees in Dept. of IT Engineering from Mokwon University in 2001, 2003 and 2007, respectively. He also received 2nd Ph. D. degrees in Graduate School of Engineering from Fukuoka Institute Technology (FIT) of Japan in 2012. He was a Senior Engineer at R&D Center, Fumate Co., Ltd. from 2007 to 2009. And he was a Research Professor at Dept. of Information Communication Engineering, Chosun University from 2009 to 2011. Since 2012, he has worked as an Assistant Professor in Division of Convergence Computer & Media at Mokwon University, Korea. He is also serving as a guest editor, and editorial staff and review committee of Journal of Supercomputing – Springer, Journal of System Architecture - Elsevier, Security and Communication Networks - Wiley InterScience, Wireless Personal Communications – Springer, International Journal of Communication Systems – Wiley InterScience, IET Signal Processing – IET Journal, IET Communications – IET Journal and other journals. His current research interests include IoT, Wireless Multimedia Communication, V2X Communication, Software Engineering, Network Transmission Scheme, M2M and Ubiquitous Sensor Networks. He is a member of the IEEE, DCS, KIIT, KONI.