International Journal of Control and Automation
Vol.9, No.1 (2016), pp.435-444
http://dx.doi.org/10.14257/ijca.2016.9.1.37

Two-Factor Authentication Methodology using Hybrid Face Recognition

Junghun Park[1], Bowon Jung[2], Okkyung Choi[3,*]

[1]*Dept. of Information Security Consulting, CYBERONE CO., Ltd, Seoul, 06300, Korea*
[2]*Dept. of Computer Engineering, Sejong University, Seoul, 05006, Korea*[3]*Bangmok College of General Education, Myongji University, Yongin, 17058, Korea*
[1]*pjh112@nate.com,* [2]*bowon_i@naver.com,* [3]*okchoi@mju.ac.kr*
**Corresponding author: Okkyung Choi*

Abstract

With the rapid development of mobile devices and IT technologies, protecting personal information is becoming an important issue, and safety must be seriously considered. However, while smartphones in use today continue to have security vulnerabilities in the authentication stage, so far no complimentary security technology has been firmly prepared to address it. Authentication is the process of confirming the truth of an attribute of an entity. As intelligent mobile devices are getting popular, the role of authentication has become more critical as a mean to control access to one's banking account or personal information. In this paper, user authentication is made more secure by using two-factor authentication with the hybrid recognition method. The core elements of the authentication technology are using the hybrid face recognition method employing dual-stage holistic and local feature-based recognition algorithms. This enhanced the recognition rate and recognition time by adapting weighted sub-region and diverse Garbor scale in the two-factor authentication system. To demonstrate the practical efficiency and validity of the proposed method, the experiments are conducted and the experimental results are compared with the existing methods.

Keywords*: Face Recognition, Garbor, MLBP, Smartphone, User Authentication*

1. Introduction

With the rapid development of mobile devices and communication technologies, protecting personal information is becoming an important issue and safety must be considered seriously. Authentication is a critical step, considering the devastating financial damage it could bring upon when it failed. Not only that, but also unrecoverable collateral damage like personal information leak or reputation loss that may occur. There are various ways in protecting the personal information of a user. Traditionally, mobile devices are secured by password system [21]. The password system of smartphones and tablets use a pattern password or PIN consisting of 4 digits or characters; however, it has the demerits that other person can easily find out the password by observing the movement of finger or the user can forget the password.

Therefore, the method, in which a user sets up the password for its smartphone, is very vulnerable to hacking if the user would not change it after a certain period of time or the user can't remember the password. To overcome this issue, biometrics technology is commonly used in protecting personal information. Biometrics technology is a recognition technology using the body state information of a person. Since it uses specific attribute information of an individual, there is no concern of loss or theft. Representative

Corresponding author

ISSN: 2005-4297 IJCA
Copyright ⓒ 2016 SERSC

biometrics technologies use voice, iris, fingerprint or face. By using biometrics, a person could be identified based on "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows"(password, PIN) [1,17]. Biometrics methods definitely complement PIN or key methods currently being used. At present, the commercialized and extensively used biometrics methods are finger vein recognition at an entry/exit door, face recognition of Google Android phones, fingerprint recognition of Apple iPhone and voice recognition. Finger vein recognition [19,20]is one of the most well-known biometrics refers to a recent biometric technique which exploits the vein patterns in the human finger to identify individuals and it has been proved to be an effective biometric for personal identification in recent years. This method is getting popular because it is not necessary to carry a plastic card such as IDcard and there is very little chance of being a victim of theft. But its drawback is that it requires specialized equipment and technical skills[18].

Each recognition method has its merits and demerits. The recognition rate of voice recognition gets heavy influence from language, word or pronunciation. Iris recognition is known as having the highest recognition rate; however, it is costly to build recognition environment and a user can have a sense of resistance because the iris part should be in contact. Fingerprint recognition has high recognition rate; however, it is easy to copy a fingerprint and the recognition is disabled if a fingerprint has been erased. Face recognition gets heavy influence from various variables such as lighting, posture, occlusion, cosmetics surgery or makeup. However, since it is possible to build the recognition environment for face recognition with a camera, face recognition has high accessibility and a user does not have a sense of resistance since it does not involve any physical contact. Since most recent mobile devices and embedded systems has a camera, so face recognition can be utilized anytime and anywhere.

In this study, we suggest a hybrid face recognition method as a way of authenticating ownerships of mobile device users. It was possible to resolve existing issues and improve recognition rate and recognition speed compared to existing methods. The core elements of the authentication technology are Two-Factor authentication, strong user authentication method using advanced face recognition method, and non-repudiation feature. An actual security module was designed and tested in order to prove its efficiency and validity.

The rest of this paper is organized as following: Several related works are described in the next section. In section 3, design of suggested method is described, along with the principles of its modules. In section 4, the results of user study and experiments are provided to verify efficiencies of our paper. Conclusions are provided in the final section.

2. Related Work

2.1. Face Recognition

Personal identification is a significant function in the real world and facial images are the most common biometric characteristic used by humans to make a personal recognition, hence the idea to use this biometric in technology. This is a nonintrusive method and is suitable for covert recognition applications[1]. As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention and many methods of face recognition have been proposed[2].

The face recognition methods have the following categorization according to the type of features used:

- Holistic methods: These methods represent the whole face region as the raw input to a recognition system.
- Local methods: These methods extract local features such as eyes, nose, mouth and cheeks, and their locations and local statistics are fed into a structural classifier[2].

 Copyright ⓒ 2016 SERSC

- Hybrid methods: Both local features and the whole faces are used to recognize a face. Zhao et al.[2]claimed that "One can argue that these methods could potentially offer the best of the two type of methods."

The most well-known holistic methods are Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Independent Component Analysis (ICA) and Probabilistic Decision-Based Neural Network (PDBNN). PCA[3], called Eigenface, uses most discriminative eigen-vectors to express the faces and it replaces the high dimensional vector images to the low dimensional vector images to recognize the face easily.
Local methods have been surveyed and theses methods extracted local features from face regions. Ahonen et al. [4] applied a texture descriptor, called a Local Binary Pattern (LBP), for face recognition. An LBP operator is applied to the face image, and then output is partitioned into sub regions. Histograms of sub regions are utilized for face recognition.

2.2. MLBP

MLBP is measured by transforming a pixel of an image using the relationship between its neighboring pixels and it is mainly used for various fields, including face detection and face recognition[5-8].The first step of the transformation sequence is the generation of 3x3 windows based on pixel. The average of all pixels in the windows is obtained. If a pixel is bigger than the average value, it is transformed to 1 and if a pixel is smaller than the average value, it is transformed to 0. Next, the binary numerals obtained by arranging the pixels in certain direction (vertical, horizontal, counter clockwise, clockwise) are transformed into decimal numerals and they are used as the central pixel values. In this study, the binarized pixels are arranged in clockwise direction based on the pixels at upper left. Since MLBP takes the relation with surrounding pixels relatively, it is known as a robust method against illumination variation. Equations (1) and (2) are the MLBP formulas

$$S(P) = \begin{cases} 1, if P \geq \bar{P} \\ 0, if P \leq \bar{P} \end{cases} \quad (1)$$

In Equations (1), S(P) is a comparison function; while P means all the pixels in 3x3 windows. $\bar{P}$is the average of all pixels. If the pixel value is bigger than $\bar{P}$, it is converted to 1. If it is smaller than $\bar{P}$, it is converted to 0.

$$MLBP(x, y) = \frac{(\sum_{i=0}^{8} S(P)2^i)}{2} (2)$$

As in above Equations (2), the transformed pixel values are arranged in the desired direction and they are used after being transformed into decimal numerals. Arranged nine binary codes need to be expressed in a eight bits depth pixel, so it needs to be quantized by dividing it by 2. The MLBP is completed by applying this process to all the pixels. Figure 1 is the transformation process of MLBP. For example, as shown in Figure 1, MLBP operator assigns a label to every pixel of an image by thresholding the 3x3 neighborhood of each pixel with the center pixel value and considering the result as a binary number. For example, "011000011" is the designed pattern of the central pixel. By applying MLBP operator to one facial image, one pattern map can be computed. Then, the pattern map is divided into many blocks and the histogram computed in each block is concatenated together to form the description of the input facial image.

Copyright ⓒ 2016 SERSC

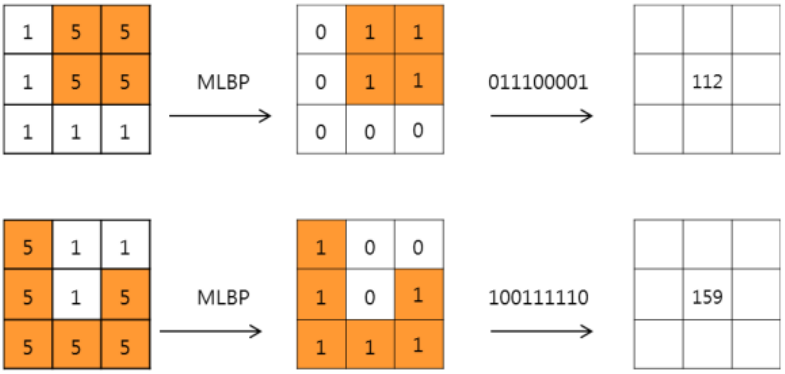

Figure 1.Example of MLBP

3. Proposed Method

3.1. Overall Proposed Method

Each smartphone device has IMEI number. IMEI number is a unique number bound to each mobile phone and it has been managed and assigned by its manufacturer so it is almost impossible for them to have an identical IMEI number. IMSI is bound to a mobile device subscribed to GSM service and it consists of mobile country code, mobile network code, identity number of mobile subscriber and identity number of country mobile subscriber. In case of user authentication during logging in, IMEI, IMSI and password show the user's device information, which tells 'What you have' factor and 'What you know'. When a user registers for the service, ID checkbox uses IMSI to make his/her mobile subscriber identity number as its default, and the system registers the user to the Authentication Server after email verification. Authentication Server sends a verification code, a number created by random number generating algorithm to the user's email address. The user enters the random number and signs in by entering password and taking a picture. The picture contains GPS information of the location and the image file also contains the current date and time, latitude and longitude, so a simple Google map could locate the user's whereabouts. It works as non-repudiation feature. Fig. 2shows the overall process of the proposed method.

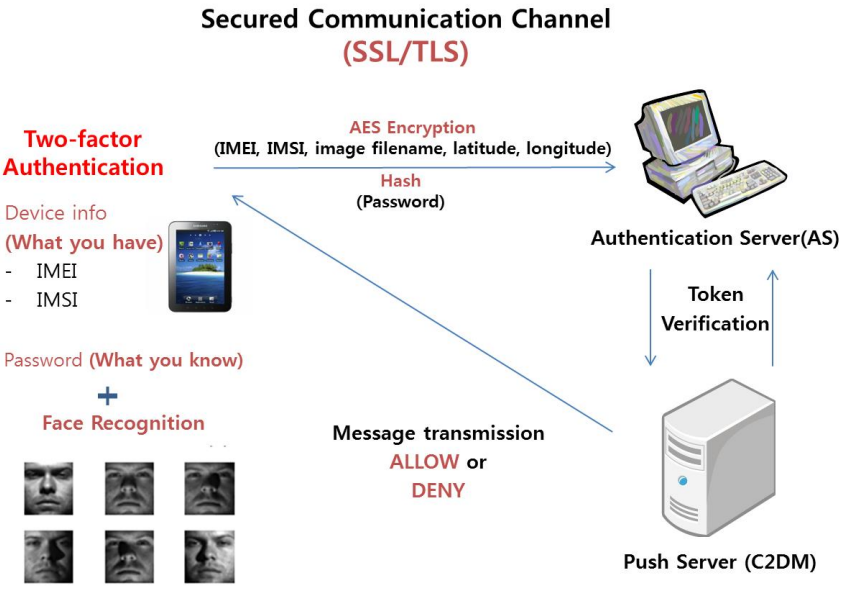

Figure 2.Overall Proposed Method

Copyright ⓒ 2016 SERSC

3.2 Hybrid Face Recognition Method

We propose a hybrid classifier for face recognition utilizing the advantages of Garbor Wavelet and MLBP.

Fig. 3 shows the flowchart of the proposed method. It utilizes a Garbor Wavelet in the first step and a MLBP in the second step. At first, histogram equalization is performed. The recognition rate is maintained comparing with existing methods by applying the Histogram Equalization as for preprocessing because it reduced the impact from the illumination change. After Histogram Equalization is performed, it utilizes a Garbor Wavelet and a MLBP to obtain higher recognition rates. At the end, the classifier reduces the number of candidate training images by selecting only the upper *n* training images after sorting them in ascending order according to their distance values between a test image and training images [12]. The main advantage of this coarse-to-fine step is reducing of the recognition time and a flexible two-step recognition structure. In the experimental evaluation, the proposed method showed higher recognition rates and lower computation time under illumination changes than the existingmethods.

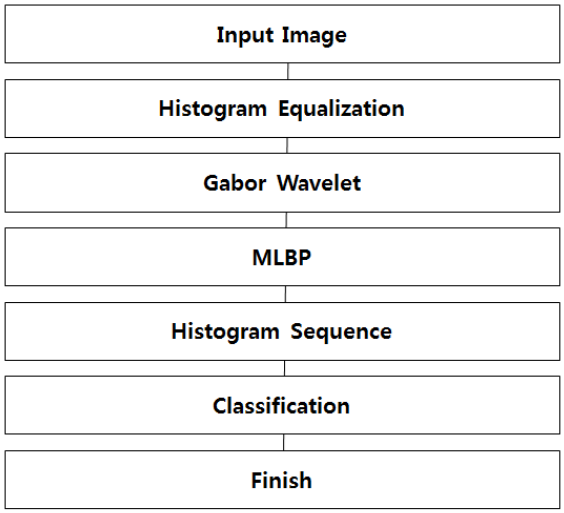

Figure 3.Flowchart of the Proposed Algorithm

4. Performance Evaluation

4.1 User Study

This study was realized in the android based platform. Usability means how conveniently a certain product is used for a specific purpose. The experiment was conducted on 50 graduate students who are attending at university for several weeks and had enough knowledge about how to use the system. For the ideal evaluation on the usability, various elements should be evaluated [9]. Each user has different ability in identifying the texts on a display device, the criterion for visibility was established using a Likert scale. A Likert scale is a psychometric scale commonly involved in research that employs questionnaires. The questionnaire[15] used for Likert scale had 5 step scale and used the score between 1 point (very negative) and 5 point (very positive) as measures. The results are showed in Table 1 and Fig. 4.

Copyright ⓒ 2016 SERSC

Table 1.Evaluation Result on the User Study

(Avg: Average, SD :Standard Deviation)

Evaluation item		Smart Pad		Smart Phone	
		Avg	SD	Avg	SD
Portability	1. Is it easy to carry portable devices anytime and anywhere?	4.7	0.48	4.85	0.37
	2. Is it convenient to access the authentication process while moving?	4.6	0.52	4.7	0.47
Convenience	3. Is the proposed method easy to use?	4.1	0.74	4.15	0.75
	4. Is it useful when many people have used at the same time?	3.8	0.63	3.95	0.6
	5. Is it efficient to use the interface of proposed method?	3.9	0.74	4.05	0.69
	6. Are you willing to use the proposed method in the future?	4.1	0.57	4.2	0.62
Issuance	7. Is it convenient to issue, register and replace the authentication process?	4	0.67	4.1	0.64
Security	8. Is it safe to prevent the information leakage?	3.3	0.48	3.25	0.44
Education	9. Is it easy to learn the proposed method?	4.4	0.52	4.7	0.47

First, portability is about judging the availability of the corresponding authentication medium when there is a need for a separate authentication medium to utilize electronic finance authentication technology. Now that the proposed method mainly deals with feature-based image GPS information along with the use of unique smartphone identifiers IMEI, IMSI plus the knowledge-based password, convenience of portability is very high as seen in the results of Question 1 and 2.

Second, convenience involves determining whether a way a user should perform or an input procedure when authenticating electronic finance is sophisticated or not. The proposed method brings inconvenience because it makes use of the camera modules in smartphones to photograph user authentication images. As seen in the results of Questions 3, 4, 5 and 6, however, convenience of use is high since respondents said they would be willing to use it in future electronic financial transactions due to its easy use, convenience even when used by multiple users as well as an intuitive interface.

Third, issuance involves judging if it can be performed with ease when authentication technology is needed to be installed, issued, registered and replaced. The proposed method allows the use of Android Market to download it to the smartphone easily in the form of app. As it brings convenience in deleting and updating a new version, it has high convenience in issuance as shown in Question 7.

Fourth, security involves judging if a prompt response is possible when main information of authentication technology or authentication media has been stolen or disclosed by others. Regarding the proposed method, it is stored in the server when entering unique smartphone identifiers IMEI, IMSI in membership entry process, so when others intend to misuse it, its use can be rejected or the GPS value where the authentication was attempted can be retrieved. As the GPS value itself may show a poor reception under and inside a building, however, convenience of management is on average as shown in Question 8. Future study is expected to be able to get the user's position known by using network-based service.

Fifth, education involves judging if the probability of security incidents rises when separate security education has not been carried out for users who use authentication technology. As the proposed method can be used without the separate security education, convenience of education remains high as seen in the results of Question 9. With the experiment conducted on computer engineering students, it is expected to also become

 Copyright ⓒ 2016 SERSC

public easily in use as it adopts a method of shooting authentication images by using the existing login type plus camera modules, as seen in the results of convenience of use.

Fig. 4 shows the results of a User Study. The overall usability items such as Portability, Convenience, Issuance, Safety, and Education showed a similar result in both devices. As a result, it is proved that there's no difference between the smart pad and smartphone as they are different only in LCD size, CPU and RAM.

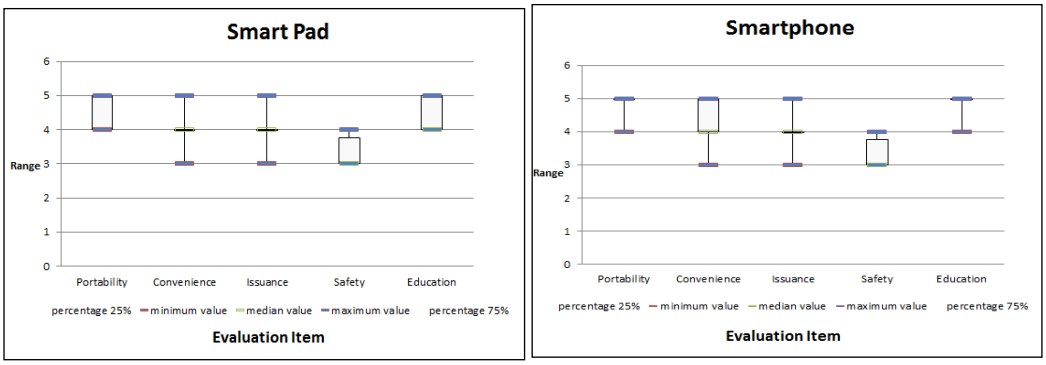

Figure 4.User Study (Smart Pad vs Smartphone)

4.2 Experiments of hybrid recognition method

All experiments were carried out on the database with 2,414 images of 38 individuals from Extended Yale Database B[10-12]. There are 64 images for each individual. All the images used in this experiment have no change in the expression or pose because this database was manufactured to experiment the illumination changes. The database is divided into 5 subsets named Subsets 1 to 5, according to the ranges of angles between light source direction and the camera axis. The subsets of the database are shown in Fig. 4. The numbers of images of each subset are given in Table 2[12].

Subset 1 is used as a training set as it is the set where illumination variation effects are negligible. Subsets 2 to 4 are used for the performance evaluation under different illumination conditions. Subset5 is excluded in experiment because illumination variable is severe[12]. In this paper, experiment on Subset 5 is not important because some figures are difficult to distinguish as shown in Fig. 5.

All images in Subsets 1 to 4 are manually aligned, cropped, and then resized to 105 by 120. We preprocessed images with a Local Binary Pattern (LBP) to compensate the illumination variations[12].

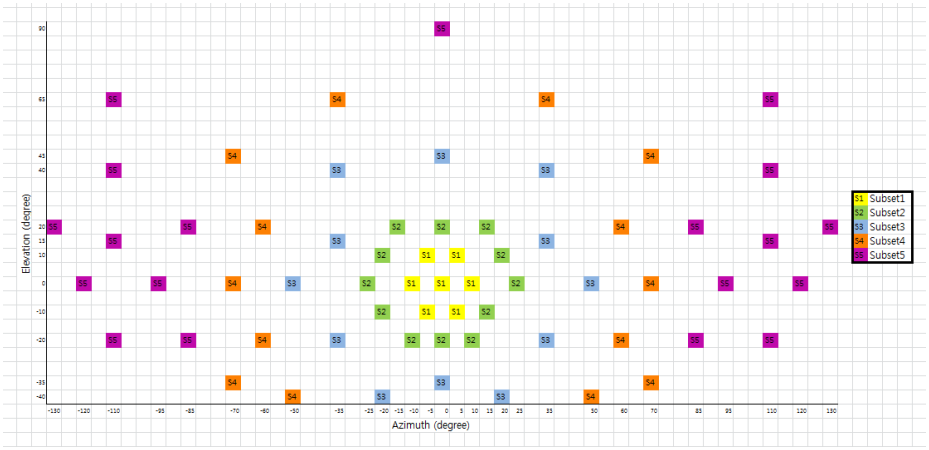

Figure 5.Extended Yale B Subset

Copyright ⓒ 2016 SERSC

Table 2.Number of Images in Each Subset

Subset 1	Subset 2	Subset 3	Subset 4	Subset 5	Total
263	456	455	526	714	2,414

We proposed the improved face recognition using MLBP(Modified Local Binary Pattern) and the Gabor Wavelet. The results of recognition rate between the proposed method(scale 3, scale 5) and the existing method are shown in Table 3. We performed recognition rate test based on Subsets 4 and 5 because illumination variation is relatively less in Subsets 2 and 3. Table 3 and Table 4 show the results of recognition rate and recognition time. In the case of the recognition time, it is calculated on the basis of the average of all test images.

Table 3.Recognition Rate at Rank One

	SubSet4	SubSet5
Existing method	487/526	303/714
Scale 3	482/526	371/714
Scale 5	495/526	479/714

Table 4.Recognition Time

	Recognition Time(s)
Existing method	8.6
Scale 3	5.6
Scale 5	8.8

5. Conclusions

Advances in technology have made life easier and mobile devices have been widely used not only as a communication tool, but also a digital assistance to our daily life, which imposes high security concern on mobile devices [21]. Thus, mobile device holds greater performance with higher levels of knowledge like that of PC, but it is also true that there is a riskier security associated to it. Hence smartphone based mobile financing requires a more powerful security measure for financial transactions than the existing devices. But smartphones in use today have security vulnerabilities in the authentication stage, so far no complimentary security technology has been firmly prepared for such matter. Today's human authentication factors have been placed inthree categories, namely What you know, such as password, secret, personal identification number (PIN); What you have, such as token, smart card etc. and What you are, such as biometrics[17]. Biometrics technology is a rapidly evolving which is being widely used in security system[16] to reduce those problems but it still has a security problem such as leakage of personal information.

In this paper, we propose an efficient Two-Factor Authentication method with the improved face recognition system using MLBP(Modified Local Binary Pattern) which is strong in the illumination change and the Gabor Wavelet which is strong in environmental change such as location, size, and indicator. By applying various Gabor scales to the face recognition system, the recognition rate and recognition time were improved. Finally, by performing the performance test using the Extended Yale B Database which was constructed for the various illumination change environments, the real time face recognition became available and it proved that the proposed face recognition was exact and efficient. The future work is to collect and analyze a variety of evaluation data and defines the exact and efficient recognition rates to promote the proposed method widely[13,14].

 Copyright ⓒ 2016 SERSC

References

[1] K. Delacand and M. Grgic, “A survey of biometric recognition methods”, Proceedings of the46th International Symposium Electronics in Marine, **(2004)**; Zadar, Croatia.
[2] W. Zhhao, R.Chellappa, P. J. Phillips and A. Rosenfeld, “Face recognition: a literature survey”, ACM Computing Survey, vol. 35, no. 4, **(2003)**, pp. 399-458.
[3] V. P. Kshirsagar, M. R. Baviskar and M. E. Gaikwad, "Face recognition using Eigenfaces", Proceedings of 3rd International Conference on Computer Research and Development (ICCRD), **(2011)**; MA, USA.
[4] T. Ahonen, A. Hadid and M. Pietikainen, “Face description with local binary patterns: Application to face recognition”, IEEE Transactions onPattern Analysis and Machine Intelligence, vol. 28, no. 12, **(2011)**, pp. 2037-2041.
[5] D. Huang, C. Shan, M. Ardabilian, Y. Wang and L. Chen, “Local binary patterns and its application to facial image analysis: a survey”, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 41, no. 6, **(2011)**, pp. 765-781.
[6] B. Froba and A. Ernst, “Face detection with the modified census transform”, Proceedings of Sixth IEEE International Conference on Automatic Face and Gesture Recognition, **(2004)**; Erlangen, Germany.
[7] T. Ahonen, A. Hadid and M. Pietikainen, “Face recognition with local binary patterns”, Lecture Notes in Computer Science, vol. 3021, **(2004)**, pp. 469-481.
[8] W. Zhang, S. Shan, X. Chen and W. Gao, “Local gabor binary patterns based on mutual information for face recognition”, International Journal of Image and Graphics, vol. 7, no. 4, **(2007)**, pp. 777-793.
[9] R. May and N. Haber, “How we remember what we see”, Scientific American., vol. 222, no. 5, **(2007)**, pp. 104-112.
[10] A. S.Georghiades, P. N.Belhumeur and D. J. Kriegman, “From few to many: Illumination cone models for face recognition under variable lighting and pose”, IEEE Trans. of Pattern Analysis and Machine Intelligence, vol. 23, no. 6, **(2001)**, pp. 643-660.
[11] K. C.Lee, J. Ho and D. J. Kriegman, “Acquiring linear subspaces for face recognition under variable lighting”, IEEE Trans of Pattern Analysis and Machine Intelligence., vol. 27, no. 5, **(2005)**, pp. 684-698.
[12] H. Cho, R. Roberts, B. Jung, O. Choi and S. Moon, "An Efficient Hybrid Face Recognition Algorithm Using PCA and GABOR Wavelets", International Journal of Advanced Robotic Systems, vol. 11, **(2014)**, pp. 1-8.
[13] J. S. Cho, S. S. Yeo and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value", Computer Communications., vol. 34, no. 3, **(2011)**, pp. 391-397.
[14] S. M. Hwang and S. S. Yeo, "Software process certification system based on K-model for high-performance software engineering", Concurrency and Computation: Practice and Experience, vol. 24, no. 4, **(2011)**, pp. 396-406.
[15] O. Choi, W. Jung, B. G. Lee and S. Moon, “A Study on Distributed Processing of Big Data and User Authentication for Human-friendly Robot Service on Smartphone”, Journal of Internet Computing and Services, vol. 15, no. 1, **(2014)**, pp. 55-61.
[16] M. N. Uddin, S.Sharmin, A. H. S. Ahmed, E. Hasan, S. Hossain and Muniruzzaman, "A Survey of Biometrics Security System", International Journal of Computer Science and Network Security, vol. 11, no. 10, **(2011)**, pp. 16-23.
[17] A. T. B.Jin, D. N. C. Ling and A.Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number", Pattern recognition, vol. 37, no. 11, **(2014)**, pp. 2245-2255.
[18] E. Lee, H. Yeh, H. S. Yang, S. Moon and O. Choi, “A Secure NFC-Based Mobile Printing Service Using Recognition Robot”, International Journal of Distributed Sensor Networks., Article ID 564506, **(2015)**, pp. 1-7.
[19] L. L.Fan, H. Ma, K. J.Wang, Y. L. Shen, Y. Shi, M. Tang and S. L. Sun, “Near Infrared Finger Vein Recognition Method Based on Subspace Projection Technology”, Advanced Materials Research, vol. 1030, **(2014)**, pp. 2382-2385.
[20] Y. Lu, S. Yoon, S. J. Xie, J. Yang, Z. Wang and D. S. Park, “Finger Vein Recognition Using Histogram of Competitive Gabor Responses”, Proceedings of 22nd International Conference on Pattern Recognition, **(2014)**; Stockholm, Sweden.
[21] R. Jianfeng, X. Jiang and J. Yuan, "A complete and fully automated face verification system on mobile devices", Pattern Recognition, vol. 46, no. 1, **(2013)**, pp. 45-56.

Copyright ⓒ 2016 SERSC

Authors

Junghwon Park, He received his M.S. degree in Engineering from Ajou University, Suwon, Korea. His major is Knowledge Information Security. Now he is working at the department of Information Security Consulting, CYBERONE CO., Ltd, Seoul, Korea. His main research interests include Ubiquitous Computing and mobile security.

.

Bowon Jung, He received hisM.S. degree in Computer Science & Engineering from Sejong University, Seoul, Korea. He is currently a researcher in RobotsandDesign. His research focuses on the Service Robot, Face Recognition, Computer Vision and Robotics.

Okkyung Choi, She received her M.S. and Ph.D. degrees in Computer Science & Engineering from Chung-Ang University, Seoul, Korea. She is currently an assistant professor of Bangmok College of General Education at Myongji University. Her research focuses on the design and implementation of Semantic Web Services System, Cloud Computing, Big Data Processing, Mobile Security, Standardization of Service Robot and Programming Languages. In these fields she has published more than 100 papers in journals and conference proceedings.

Copyright ⓒ 2016 SERSC