

# A survey of smartphone-based Face Recognition systems for Security Purposes

Atrab A. Abd El-aziz<sup>1</sup>, Eman M. EL-daydamony<sup>2</sup>, Hassan.H.Soliman<sup>3</sup>

<sup>1</sup> Information Technology Department, Faculty of Computers and Information, Kafrelsheikh University, Kafrelsheikh, Egypt  
e-mail: [Atrab\\_Ahmed@fci.kfs.edu.eg](mailto:Atrab_Ahmed@fci.kfs.edu.eg)

<sup>2</sup> Information Technology Department, Faculty of Computers and Information, Mansoura University, Mansoura, Egypt  
e-mail: [eman.8.2000@gmail.com](mailto:eman.8.2000@gmail.com)

<sup>3</sup> Information Technology Department, Faculty of Computers and Information, Mansoura University, Mansoura, Egypt e-mail: [hsoliman@mans.edu.eg](mailto:hsoliman@mans.edu.eg)

**Abstract:** Smart devices, such as smartphones and tablets, are frequently used to store and send confidential and private information. The disadvantages of traditional methods of recognition have led researchers to explore biometrics to obtain accurate and convenient security of mobile devices, taking advantage of image detection technologies that capture environmental, positional and interactive information. The face is our main focus of concentration and represents an important role in the transmission of identity and emotions. In this paper, face recognition biometric researches to mobile device security are surveyed. The discussion of various feature extractions algorithms, along with the advantages and research challenges associated with face modality have reviewed.

**Keywords:** security, face recognition, smartphones, biometrics.

## 1. Introduction

In recent years, technology has revolutionized and smartphone technology is one of the most important technological innovations. The smartphone is an emerging technology that gets a dynamic improvement. Nowadays, smartphones are considered the most important electronic device due to their open operating systems, memories, highest computing capability, capacious and large screens that inspire the development of applications in all fields. Smartphones are used to allow the recognition of people at any time quickly and safely [1].

Large amount of sensitive information is stored in smartphones due to the large amount of internal or external storage. This significant amount of data on smartphones has elevated many concerns and challenges related to the security of smartphones. The security of smart devices can be achieved through the adoption of biometric identification technology, as it has received great attention and rapid development in recent years [2]. Consequently, biometrics is introduced to overcome the problems and challenges that typically face security problem [3].

Facial recognition using smartphones has attracted researchers in many fields, including pattern recognition, image processing machine learning, security and computer vision. Face recognition is one of the widely adopted biometric technologies since the approach of data acquisition is non-intrusive. The recognition of the face in the analysis process can be done with or without personal cooperation [4].

Face recognition using smartphones is still considered as a new frontier. Many researchers across the world are still working on better and optimized solutions for the face recognition challenges.

## 2. Definition

Face recognition is a process capable of uniquely verifying or identifying a person by analysing and comparing patterns based on the person's facial contours [5, 6].



Figure 1. Face Recognition used in OpenFace

Biometric face recognition has three primary tasks [7]:

- Verification (authentication) - Am I who I say I am? (One to one search). The system is asked to determine if the people are who they say they are.
- Identification (recognition) - Who am I? (one to many search). The system is demanded to decide, among a group of people whose facial features are collected in a database.
- Watch list - Are you looking for me? (one to few search). The watch list process is a generalization of the identification process which involves unknown persons.

The facial recognition system using smartphones usually consists of four steps [8] as shown in figure 2.

1. Face Detection (localization): First, the face must be located and detected from the captured image or video frames.
2. Face Pre-processing: this step includes face alignment, normalization, light correction and etc. The normalization of the coarse thread detection is the purpose of the preprocessing step so that reliable extraction of characteristics can be achieved.
3. Features Extraction: The purpose of this step is to extract a compact set of photometric and geometric features from the face of interpersonal discrimination.
4. Feature Matching: This is the actual recognition process. The feature vector gained from the extraction of features is matched to classes of facial images already stored in a database.

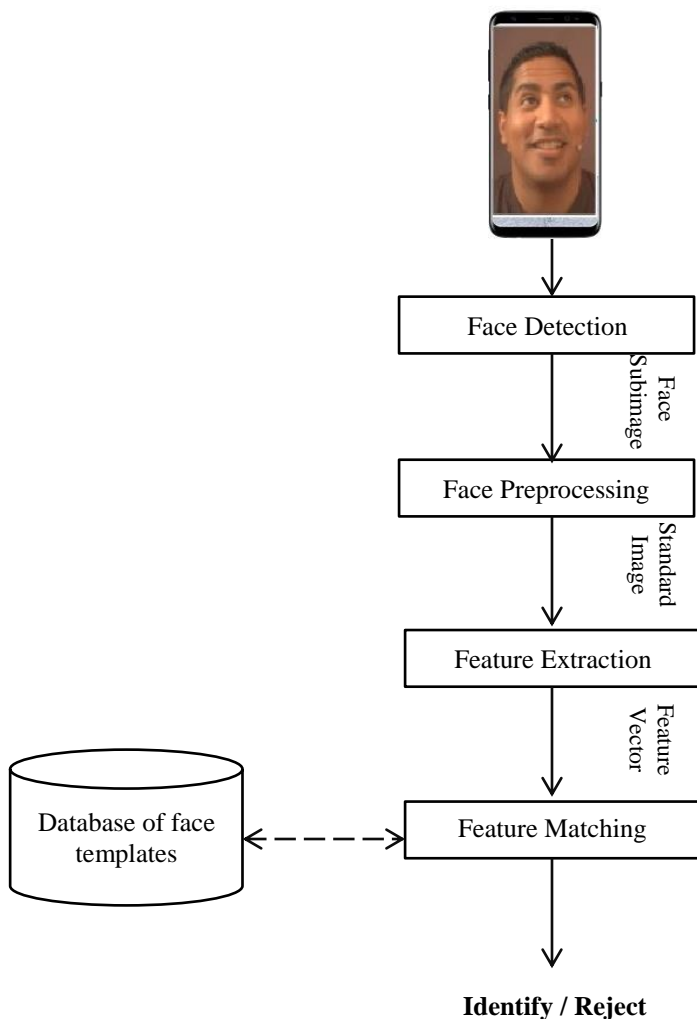


Figure 2. Flowchart of Face Recognition

These steps ensure the security of the recognition process, but some challenges and problems also arise when facial recognition is used on smartphones. As it is used to protect private data or to unlock the smartphone many times a day, more computing time is required due to the complex recognition algorithm.

### 3. Motivation

With the rapid pervasiveness of smartphones, much of the confidential sensitive information is stored on smartphones. This sits great security risks to users as the smartphone can be lost and stolen. Biometric face recognition has risen as an effective research field with various applications across the earlier decades. Face recognition applications range from controlled to dynamic settings. Consequently, face recognition is a biometric technology that has gained tremendous approval among users.

Smart devices often have built-in face detection systems, simply because they do not have enough computing power, uncomplicated detection algorithms are performed on them, which don't have as high a performance except can run on low power platforms. Accordingly, there is a trade-off relationship between high performance and hardware and power limitations.

### 4. Related work

Abeni et al. [9] showed that a support vector machine of a class for mobile devices depends on the facial recognition system. For evaluation, the recognition system was experimented by a Nokia 6680 cell-phone and with the Symbian operating system. The results indicated that an EER of 3.95% could be achieved. Then, Hadid et al. [10] have proposed Haar-like features with the AdaBoost approach for face detection and analysing scheme. They have demonstrated a local binary pattern (LBP)-based method on a Nokia N90 phone. The obtained results were very promising and achieved average recognition rates of 96%. Although it was a fast and accurate approach, it wasn't a robust method since it was designed for older phones. Modern phones have more powerful CPUs and GPUs.

Later, the authors in [11] demonstrated a facial authentication approach based on hierarchical correlation (HCFA) for mobile devices. Their scheme could investigate the association among each output peak of cross-correlation produced from elected sub-areas of a face. They also performed the experiment utilizing the Nokia S60 emulator using Java ME. The scheme supported the mobile computing environment with limited resources due to storage demand and low memory.

Then, Mayrhofer and Findling [12] introduced an open face-to-face mechanism using all the information that can be obtained from a 180-degree panning of the device near the person's head and sensor data from the built-in sensors of the person device. They evaluated several neural networks and support vector machines on Samsung Nexus S GT-I9023 device. They reported a 90 % accuracy rate which demonstrated the feasibility of their approach.

Another contribution in [13] proposed a facial authentication scheme based on an assisted sensor, which adopted light and movement sensors to defend against media and implicit camera crime. The experimental results reported that the approach could obtain a detection rate of 97% and a false alarm rate of 2% in real environments. The authors in [14] investigated an efficient method for fully automatic face recognition toward solving smartphones active authentication problems. They derived a benchmark dataset using videos recorded by the front camera. The recorded videos in real-world included challenges properties such as varying distances, blurring from holding the device, partial capturing, background and illumination variations. The benchmark dataset consists of 750 videos from 50 different users over three sessions. Another approach [15] has been introduced which is considered more reliable in the face recognition system. The authors described how to overcome the problems faced by existing face recognition systems such as variable light conditions. They investigated an image encoding technique called Local Binary Patterns (LBP) as a facial images texture descriptor captured in various lighting conditions. Their face detection method successfully detected at a rate of 91.30% control accuracy and 100% accuracy in other environments.

Another efficient approach [16] has been introduced which is considered more reliable in face recognition system. They proposed a deep feature-based face detector to detect user's faces in images containing extreme pose, illumination variations and partial faces using the front camera. Moreover, they developed libraries in OpenCL to implement deep convolutional neural network (DCNN) based algorithms on GPUs. The experiments have been run using two different data sets and have been classified using SVM classifier. Their face detection algorithm was detected successfully at a rate of 99.30%.

In [17], the main focus of the author is to use the face and periocular traits and apply recognition technique based on biometrics in smartphones. They also build a database from 46 subjects containing face and periocular images. They applied three feature extraction techniques includes Speeded Up Robust Features (SURF) [18], Scale Invariant Feature Transform (SIFT) [19] and Binarized Statistical Image Features (BSIF) [20]. After experiments, the performance of feature extraction technique is much better when fusing periocular trait with face trait. They reported 1.3% error rate and 96.5% Accuracy.

This work has been extended by them in [21] and a new multimodal biometric system is developed which uses iris, face and periocular traits for the recognition process of a person. The system was tested using two different devices - Samsung Galaxy Note 10.1 tablet and Samsung Galaxy S5 smartphone. An extensive set of experiments conducted using the proposed system shows the applicability for secure authentication scenarios. The proposed system was tested using a unimodal and multimodal approach. From the experiments, An Error rate reduced to 0.68% which was obtained from fusing multiple traits.

Authors in paper [22] demonstrated an implicit and unconstrained multimodal biometric system for smartphones using face, touch strokes, and phone-movement patterns. They also collected a mobile multimodal dataset from 95 subjects. The classification and regression tree analysis (CART) was used for Face localization [23] and then Binarized Statistical Image Features (BSIF) algorithm is applied for feature extraction process. Experimental results show high accuracy with an EER of 0.01 %.

The basic taxonomy of the work related to face recognition field has been shown below in figure 3.

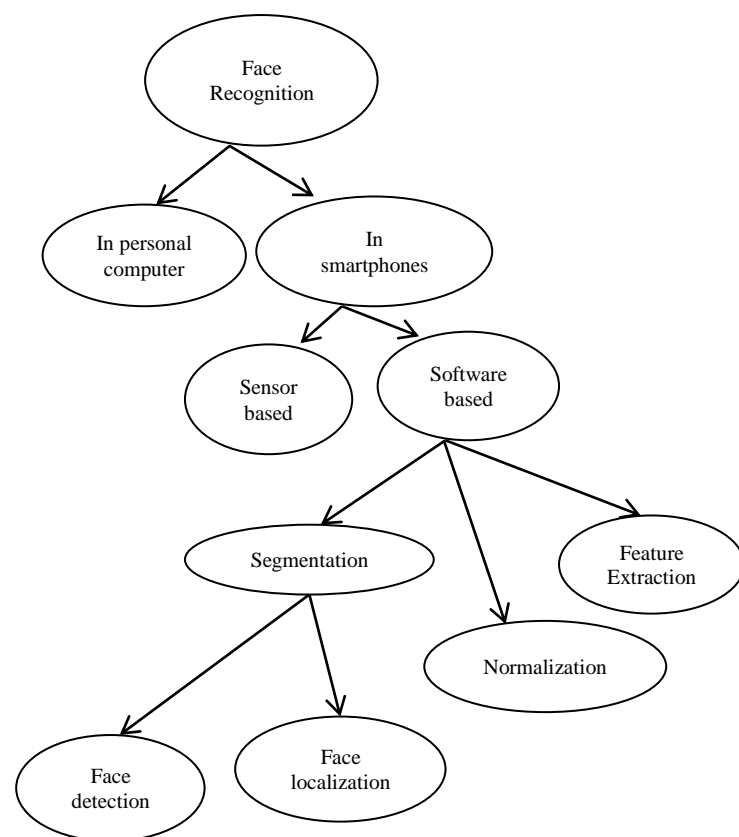


Figure 3. Face recognition related work taxonomy

Several techniques and algorithms used in all the above discussed papers are summarized in table 1 beside their objectives, deficiencies and results.

Table 1. Summarized Related Work of Face Recognition

| Reference  | Algorithm(s)  | Objective(s)   | Device                                       | Result                 | deficiency  |
|--|---|--|--|------------------------|---|
| Implementing biometrics based authentication for mobile devices[9]   | Support Vector Machine  | - Reduce error rate  | Nokia 6680                                   | EER 3.95%              | - Designed for old phones   |
| Face and eye detection for person authentication in mobile phones[10]  | local binary pattern  | - Achieve High precision and reduce time   | Nokia N90                                    | ACC 96%                | - Designed for old phones   |
| Mobile device access control: An improved correlation based face authentication scheme and its Java ME application[11] | hierarchical correlation based face authentication                                    | - Reduce error rate  | Nokia S60 emulator                           | EER of 3.58%           | - Required more memory  |
| Towards pan shot face unlock Using biometric face information from different perspectives to unlock mobile devices[12] | SVM and neural network  | - Provide reliable and harder to attack system   | Samsung Nexus S GT-I9023                     | ACC 90%                | - Depended on only one position for face  |
| Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones[13]                    | Motion-Vector Correlation   | - Defending against the virtual camera attacks<br>- propose a Motion-Vector Correlation algorithm                                  | Samsung Galaxy Nexus                         | EER 2%                 | - system can be compromised with Video imitator   |
| Face –based active authentication on mobile devices [14]   | principal component analysis  | - collecting facial dataset combined with features based on fiducially points can be used for active authentication in smartphones | IPhone 5s                                    | RR 95.5%               | - difficulty addressing the variations in illumination<br>- the dataset misses variations due to change in life style |
| Face Recognition with Environment Tolerance on a Mobile Device[15]   | Local Binary Patterns<br>Support Vector Machine                                       | - overcome the problems encountered by variable light conditions<br>- utilize LBP on modern mobile handset device hardware         | HTC  | RR 91.3%               | - image dataset was very small  |
| Deep Feature-based Face Detection on Mobile Devices[16]  | Support Vector Machine  | - Overcome the problems encountered by capturing such as light illumination and partial images.                                    | Samsung Galaxy S4 & Nexus 6                  | ACC 99.3%              | - doesn't suitable for real time monitoring due to their run times on mobile devices                                  |
| Fusion of Face and Periocular Information for Improved Authentication on Smartphones[17]                               | SURF<br>SIFT<br>BSIF  | - increase performance and accuracy  | Samsung Galaxy S5 & Samsung Galaxy Note 10.1 | ACC 96.5%<br>EER 1.3 % | - Small dataset   |
| Multi-modal Authentication System for Smartphones Using Face, Iris and Periocular[21]                                  | -SURF<br>-SIFT<br>-BSIF   | - reduce error rate  | Samsung Galaxy S5 & Samsung Galaxy Note 10.1 | EER 0.68%              | - More Computational time   |
| Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns[22]                      | -classification and regression tree analysis<br>-Binarized Statistical Image Features | - reduce error rate<br>- enhance accuracy and usability  | iPhone 6s                                    | EER 0.01%              | ignored security and system vulnerability   |

## 5. Challenges and Considerations

The accuracy of the face recognition system depends on different associated vectors. In this paper, some of these common considerations associated with facial recognition system are explained [24].

- i. Variation in facial appearance (intra-class): are variations of the appearance of the same face produced by facial expression, illumination, facial pose, and lens aperture time and lens aberrations of the camera.
- ii. Interclass similarity: The problem of having distinctive people have a substantially similar appearance, as family members, twins and strangers can look alike.
- iii. Non-linear manifolds: The difficulty of having only a small number of samples and a high-dimensional input space.
- iv. Image quality: Another consideration that affects the recognition rate is the quality of the image itself. The poor quality image isn't effective to provide the effective results since it can hide some of the adaptive facial features.
- v. Aging: the problem is the change of the person's face according to age. Because of this, the aging vector in the authentication system is required to be covered.

## 6. Algorithms

The most promising feature extraction algorithms used for face recognition are listed in table 2. Out of this Principal Component Analysis and Local Binary Pattern will be described in detail.

Table 2. Face Feature Extractions Algorithms

| Preserving       | Technique                           |
|------------------|-------------------------------------|
| Global Structure | Fisher Linear Discriminant Analysis |
|                  | Gabor filter                        |
|                  | Optimal Elastic Base Graph          |
|                  | Principal Component Analysis        |
|                  | Kernel Principal Component Analysis |
| Local Structure  | Kernel Principal Component Analysis |
|                  | Locality Preserving Projections     |
|                  | Laplacian Eigenmap                  |

## 6.1. Local Binary Pattern (LBP)

The methodology of the Local Binary Pattern (LBP) descriptor technique [25]:

The sample of the face is subdivided into small areas and then the histograms of the binary pattern are obtained with a central value as a threshold and obtaining the results as a binary number into account, the pixels are labelled. Then the histograms of the labels are used as an image descriptor in face recognition.

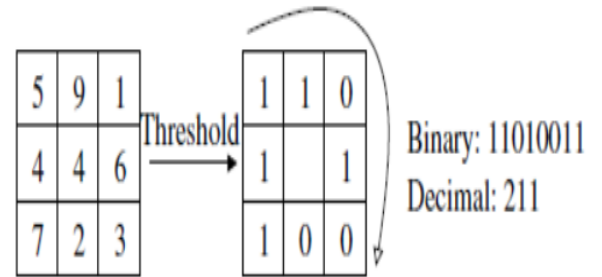


Figure 4. The LBP Operator

The histograms generated contain different information related to all regions of the face. Therefore, the histogram of the face template can be defined by Equation (1),

$$H_i = \sum_{x,y} I\{f(x,y) = i\} \quad i=0,\dots,n-1 \quad \text{Eq (1)}$$

Where  $f(x,y)$  is the face sample,  $n$  is the number of labels obtained by LBP and  $H_i$  is the face histogram. To obtain an adequate representation of the face, spatial information of the face is also collected, since the image of the face is divided into regions  $R_1, \dots, R_n$ , and the extended histogram is based on Equation (2)  $H_{i,j} = \sum_{x,y} I\{f(x,y) = i\} I\{(x,y) \in R_j\}$ ,  $i=0,\dots, n-1$  and  $j=0,\dots, m-1$  Eq (2)

The algorithm represents the representation of the face in three separate levels. The histogram labels include information about remarkable patterns at the pixel level, and then the labels are gathered in a tiny region to afford information on the regional level. Eventually, localized histograms are mixed to produce an optimal description of the face image. [26].

## 6.2. Principal Component Analysis

Principal component analysis (PCA) is a linear transformation that obtains the variance of the input data. In the PCA algorithm, the characteristics of the original image are projected in a new coordinate space. In the new coordinate space, each coordinate axis will represent a main component vector [27].

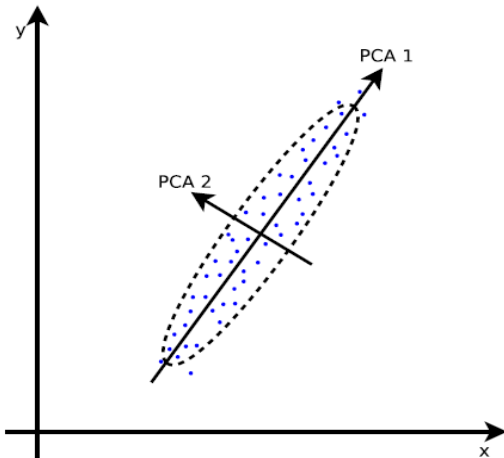


Figure 5. Example of PCA

Assume the input data is  $X = [x_1, x_2, \dots, x_n]$ ,  $n$  is the number of samples and  $x_i$  is the  $i_{th}$  data sample. Then, the  $i_{th}$  data sample can be reconstructed in the PCA space using equation(3) [28].

$$y_i = \Phi_X^{-1}(X_i - X^-) \quad | \quad = \Phi_X^T (X_i - X^-)$$

Eq (3).

Where  $\Phi_X$  is the matrix of eigenvectors. The principal objective of PCA is to decrease the large dimensionality of the detected variable to the smaller essential dimensionality of the independent variable without missing important information [29].

## 7. Conclusion

Smart devices offer many services that enable consumers to benefit from these high-tech devices. In addition, the increasing resources available in these devices have allowed a sufficient storage and use of several formats compared to the typical use of entertainment and tablet games, which leaves manufacturers and consumers increasingly concerned about the safety of mobile devices. Biometrics has been investigated to address the issues associated with traditional techniques. Facial recognition systems are widely used in security fields, especially with smartphones. In this paper, we survey the improvement of techniques for recognizing facial users in smartphones. In addition, the three tasks of face recognition have been addressed. By analysing a series of related efforts, we identified that facial traits can afford high identification precision. In addition, we identified that some problems and extensive challenges must be considered when implementing facial recognition systems and we perceive this with the development of smartphones. Smartphones will be more important and beneficial to design the facial recognition mechanisms expected in mobile phones.

We anticipate that this survey may stimulate further research to study the challenges and open difficulties that are known in this region. Finally, we reviewed the important feature extraction techniques of face recognition.

## References

- [1] Q. Zhang, H. Li, Z. Sun, Z. He, and T. Tan, "Exploring complementary features for iris recognition on mobile devices," 2016 Int. Conf. Biometrics, pp. 1–8, 2016.
- [2] Atrab A.Abd El-aziz, Eman M. EL-daydamony, Alaa. M. Raid, "Multi-modal Online User Authentication System based on Finger Knuckle Print and Keystroke Dynamics using Smartphones", JCIT, Vol. 12, No. 3, pp. 1 ~ 11, 2017.
- [3] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and iris recognition for mobile engagement," Image Vis. Comput., vol. 32, no. 12, pp. 1161–1172, 2014.
- [4] S. Y. Kung, M.-W. Mak, and S.-H. Lin, "Biometric authentication: a machine learning approach". Prentice Hall Professional Technical Reference, 2005.
- [5] Abul-Kashem, M., & Akhter, M. N., & Ahmed, S., & Alam, M. M., "Face Recognition System Based on Principal Component Analysis (PCA) with Back Propagation Neural Networks (BPNN)", Canadian Journal on Image Processing and Computer Vision.2(4), 36-45, 2011.
- [6] Baltrušaitis, Tadas, Peter Robinson, and Louis-Philippe Morency. "Openface: an open source facial behavior analysis toolkit." Applications of Computer Vision (WACV), 2016 IEEE Winter Conference on. IEEE, 2016.
- [7] R. Chellappa, P. Sinha, and P. J. Phillips, "Face recognition by computers and humans," Computer, vol. 43, no. 2, pp. 46–55, 2010.
- [8] Manuel Gunther et al. "Face Recognition in Challenging Environments: An Experimental and Reproducible Research Survey", pages 247-280. Springer International Publishing, Cham, 2016.

- [9] P. Abeni, M. Baltatu, and R. D'Alessandro, "Implementing biometricsbased authentication for mobile devices," In Proc. IEEE Global Telecommunications Conference (GlobeCom), pp. 1-5, 2006.
- [10] A. Hadid, J.Y. Heikkil, O. Silven, and M. Pietikinen, "Face and eye detection for person authentication in mobile phones," In Proc. ICDSC, pp. 101-108, 2007.
- [11] K. Xi, J. Hu, and F. Han, "Mobile device access control: An improved correlation based face authentication scheme and its Java ME application," *Concurrency Computation Practice and Experience*, vol. 24, no.10, pp. 1066-1085, 2012.
- [12] R.D. Findling and R. Mayrhofer, "Towards pan shot face unlock: Using biometric face information from different perspectives to unlock mobile devices," *International Journal of Pervasive Computing and Communications*, vol. 9, no. 3, pp. 190-208, 2013.
- [13] S. Chen, A. Pande, and P. Mohapatra, "Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones," In Proc. MobiSys, pp. 109-122, 2014.
- [14] M. E. Fathy et al. "Face-based active authentication on mobile devices". In Proc. Speech and Signal Processing (ICASSP) 2015 IEEE Int. Conf. Acoustics, pages 1687-1691, 2015.
- [15] P. J. Riesch et al. "Face recognition with environment tolerance on a mobile device". In Proc. IEEE 2nd Int Cyber Security and Cloud Computing (CSCloud) Conf, pages 342-348, 2015.
- [16] S. Sarkar et al. "Deep feature-based face detection on mobile devices". In 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), pages 1-8, February 2016.
- [17] K. B. Raja et al. "Fusion of face and periocular information for improved authentication on smartphones". In Proc. 18th Int Information Fusion (Fusion) Conf, pages 2115-2120, 2015.
- [18] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in *Computer Vision—ECCV 2006*. Springer, pp. 404–417, 2006.
- [19] D. G. Lowe, "Object recognition from local scale-invariant features," in *Computer vision, 1999. The proceedings of the seventh IEEE international conference on*, vol. 2. Ieee, pp. 1150–1157, 1999.
- [20] J. Kannala and E. Rahtu, "Bsf: Binarized statistical image features," in *Pattern Recognition (ICPR), 2012 21st International Conference on IEEE*, pp. 1363–1366, 2012.
- [21] K. B. Raja et al. "Multi-modal authentication system for smartphones using face, iris and periocular". In Proc. Int. Conf. Biometrics (ICB), pages 143-150, 2015.
- [22] Akhtar, Zahid, et al. "Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns." *Signal and Information Processing (GlobalSIP), 2017 IEEE Global Conference on*. IEEE, 2017.
- [23] R. Lienhart et al., "Empirical Analysis of Detection Cascades of Boosted Classifiers for Rapid Object Detection", *Symp. on Pattern Recognition*. pp. 297–304, 2003.
- [24] Madhan, Madhu, and Pooja Ahlawat. "A Study on Different Challenges in Facial Recognition Methods." ,2015.
- [25] Rouhi, Rahimeh, Mehran Amiri, and Behzad Irannejad. "A review on feature extraction techniques in face recognition." *Signal & Image Processing 3.6* , 2012.
- [26] Ojala, T. Pietikainen and M. Harwood, "A comparative study of texture measures with classification based on feature distributions", *Pattern Recognition*, 1996.
- [27] Abiyev, Rahib H. "Facial feature extraction techniques for face recognition." *Journal of Computer Science* 10.12, 2014.
- [28] M. Turk and A. Pentland. "Eigenfaces for recognition *Journal of Cognitive Neuroscience*", 3(1):7186, 1991.
- [29] V. Le, J. Brandt, Z. Lin, L. Bourdev, and T. S. Huang. "Inter- active facial feature localization". In *ECCV* , 2012.