Smartphone Authentication System Using Periocular Biometrics

Kiran B. Raja[*†], R. Raghavendra[*], Martin Stokkenes[*], Christoph Busch[*†]
{kiran.raja; raghavendra.ramachandra; martin.stokkenes; christoph.busch} @hig.no
[*]Norwegian Biometrics Laboratory, Gjøvik University College, 2802 Gjøvik, Norway
[†]Hochschule Darmstadt - CASED, Haardtring 100, 64295 Darmstadt, Germany

Abstract: The increasing usage of smartphones has raised security concerns regarding these devices due to presence of high amount of personal and sensitive data. The risk is higher without a proper mechanism to handle the authentication to access the smartphone device. In this work, we present a standalone modular biometric system based on periocular information to authenticate towards device. The proposed system has been implemented on the Android operating system. We field tested and evaluated the proposed system using a new database acquired capturing samples with three different devices. We apply the three well known feature extraction techniques, SIFT, SURF and BSIF independently in the proposed peroicular based authentication system. The best performance achieved with $GMR = 89.38\%$ at $FMR = 0.01\%$ indicates the applicability of the proposed periocular based mobile authentication system in a real-life scenario.

1 Introduction

Smartphones being a widely used personal device, are also used to store personal and sensitive data. Misuse of a smartphone due to low security to control the access to the device can lead to loss of personal data, which can be used to hack the accounts related to the owner of the device. Traditional methods have employed numeric, alphabetic or alpha-numeric PIN codes to secure the device, which are limited to fixed length. In consequence, the security of such access control methods is very limited, when expressed as entropy of the PIN code. For the most common case of arabic numerals (0-9), the symbol count is 10 and thus the entropy per digit H=3.322 bits. For a common 4-digit password the entropy is approximately 13 bits. Extending the password in length targeting at higher entropy reduces the usability of the method by creating hassle in managing multiple passwords of longer length [YBAG04]. Alongside the other problems, a simple brute force approach can be successful in cracking a short password. A plausible solution is to base the systems on biometric characteristics for authentication, which have higher entropy than passwords [RCB01, Dau06].

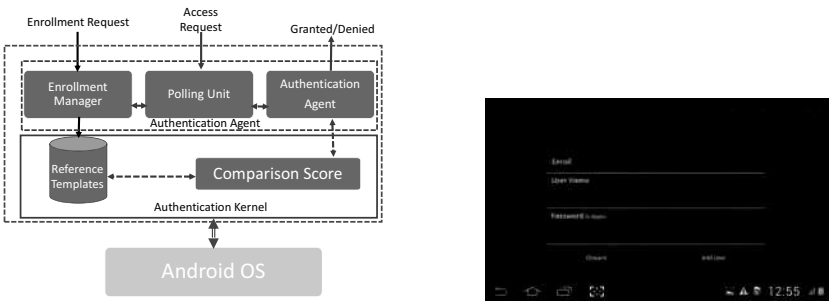
Commercial phones such as Apple iPhone 5S and Samsung S5 have provided an integrated fingerprint sensor for authentication on the device that was well perceived by a large number of customers. At the same time, academic research has been carried out to use different modalities for smartphone based authentication. Gait characteristics were explored, while smartphones were used as wearable sensors for authentication [NDBB11, DB13]. An advanced approach is to use the regular smartphone as a biometric sensor by exploiting

the capabilities of the built-in camera. Robust approaches have been proposed to use the camera as contactless fingerprint sensor for authentication [RBY13, SBB13, WN10]. Motivated by works on fingerprint recognition [RBY13, SBB13], in this work, we explore the periocular information for contactless authentication on smartphones. We present a complete standalone system to authenticate the device using the pericoular information. Further, in this work we have employed well known feature extraction methods such as SIFT and SURF based on their success in biometric applications for periocular recognition [BLGT06, PJRJ11]. Additionally, based on the recent success of Binarized Statistical Image Features (BSIF) [KR12] for periocular biometrics [KRB14], we explore this approach for periocular based smartphone authentication on Android operating system. Based on the popularity, market share and open source framework of smartphones, we focus our work on Android operating system devices. The complete system is developed and tested on the Android OS (v4.4.2) platform.

In the rest of the paper, we first present the architecture of the proposed system, which is detailed in Section 2 along with description of various components of the system. Next Section 3 provides the details of the hardware being used and implementation details of the proposed system along with the details of the evaluation. Section 4 describes the set of experiments conducted to validate the significance of the proposed system. Section 5 provides the important conclusions and identifies possible future work in this direction.

2 Architecture of Proposed System

The architecture of the proposed authentication system for any Android device is shown in the Figure 1a. The proposed system consists of two major components : Authentication Kernel and Authentication Agent. The Authentication agent consists of the Enrollment Manager, Polling Unit and Verification Agent. The Enrollment manager provides the interface for any user to enroll into the database and also controls the interface to authenticate the user to access the device. Any user preferring to enroll into the system is requested to enter the username and 6 digit password through the enrollment manager as shown in Figure 1b. The password entered is used as the fallback authentication factor in the authentication protocol: (i) if the capture subject's probe sample fails to be captured within the time-out period; (ii) if three successive attempts for biometric authentication have failed.



(a) Architecture of the proposed system (b) Illustration of enrollment user interface

Figure 1: Architecture and user interface of proposed system

Once the user enters the password during enrollment, the system prompts the user to present enrollment samples for periocular images. The enrolled images are used to obtain the reference features through the techniques mentioned in Section 2.3, which are stored into the reference templates database indicated in Figure 1a residing inside the authentication kernel. In order to protect the device at all times, the authentication agent contains a 'Polling Unit', which keeps polling for requests to access the device. Once an access request is obtained by the 'Polling Unit' then the 'Authentication Agent' is activated. That agent in turn requests the user to capture the probe periocular images. Once a probe image is acquired, the features are extracted. The extracted features are compared against all reference templates in the database, to obtain a comparison score using the techniques described in Section 2.5. The obtained score is communicated to the 'Authentication Agent' to decide upon the access to the device.

2.1 Enrollment Data Acquisition

The proposed system supports the enrollment mode through self acquisition with possibly both the frontal camera and the rear camera. The capture subjects are expected to look at the camera of the device while holding the device still and approximately at a perpendicular position in front of the face. When the face and eyes are detected in the frame, the region corresponding to the face is marked with a colored layout indicating the correct or incorrect position. The colored layout along with text is displayed to improve the user interaction with the device and to improve the quality of the captured sample image. However in order to avoid multiple face detections due to presence of other subjects in the view angle of the camera background such as in the case of a crowded scenario (e.g, Figure 2c), we propose the strategy of computing the ratio between the height of the detected face region (F_h) and the height of the screen (S_h), which is computed according to following equation:

$$capture\_proceed = \begin{cases} yes & \text{if } \frac{F_h}{S_h} \geq 0.8 \\ no & \text{otherwise} \end{cases} \tag{1}$$

(a) Red layout on frame indicating incorrect ratio computed according to equation 1

(b) Green layout on frame indicating correct ratio computed according to equation 1

(c) Effectiveness of computed ratio to address multiple face in single frame

Figure 2: Illustration of the image acqusition using the proposed system

If the layout is indicated in red color, the acquisition does not proceed. At the correct position and computed ratio calculated according to Equation 1, the layout turns green, which is used to capture images automatically. Figure 2a shows the screen shot depicting incorrect distance from the imaging device while Figure 2b presents the correct ratio

and distance from the imaging device. The images are captured when the layout is indicated by green color and the successful acquisition is indicated by an audio signal (a beep tone). The audio signal is particularly useful when the subject uses the rear camera to acquire the images by himself and in this way user interaction is optimized to achieve user convenience.

Figure 3a and Figure 3b show the images captured in a self-acquisition mode. The user is also presented an option to manually inspect the quality of images to decide on retaining the images or discarding them as shown in Figure 3c. The selected images are used for feature extraction in the proposed system.

(a) Self acquisition using front camera (b) Self acquisition using rear camera (c) Option to retain/discard image in the proposed system

Figure 3: Illustration of the image acqusition using the proposed system

2.2 Detection of Periocular Region in Proposed System

Although one can argue about using the complete face for the authentication, it has to be noted that the performance of face recognition is influenced by many factors such as pose of the head, non-uniform illumination on the face, which are predominately observed in real life scenarios where a user tries to interact with the device. The earlier studies on the effect of perspective (or pose) variation, occlusions for face recognition have justified the use of periocular region as an alternative biometric characteristic to minimize the impact of above mentioned factors [PJRJ11]. The periocular information is observed to be reliable and easy to capture. Inspired by these studies, we have used periocular information as a biometric characteristic in our proposed system, which allows the user-friendly and less constrained capture. In order to localize the periocular region, we first detect the eye by employing the Haar cascade based eye detector [VJ01] implemented in the OpenCV framework [BK08, Hos]. Presence of multiple faces in the imaging frame is handled by determining the ratio of the image in the view angle as expressed in the Equation 1. The face corresponding to the largest area on the frame is considered for detection of eyes. The periocular region is segmented by extending the boundaries of the detected eye region along the horizontal and vertical direction.

2.3 Feature Extraction Methods in Proposed System

The features from the periocular region are extracted using three different feature extraction schemes. Popular techniques to extract the features from image are Scale Invariant

Feature Transforms (SIFT) and Speeded Up Robust Features (SURF) to obtain the key points based on success reported from earlier works [PJRJ11, XCH+10]. The obtained key points are stored as templates in the database. Equivalent key points are obtained from the probe image and the obtained sets are compared with regard to their similarity. Based on the obtained score of compared set of key points, a particular subject is authenticated or rejected. Further in this work, we have implemented the Android version of Binarized Statistical Image Features (BSIF) [KR12] for extracting the features from the periocular region based on the success for periocular recognition as reported earlier [KRB14]. We have adapted the BSIF filters with dimension of 9×9 with 8 layers.

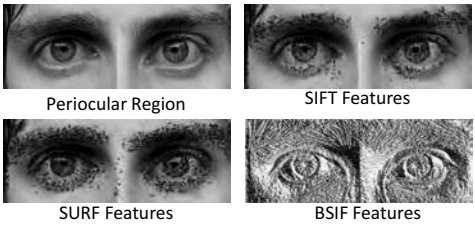


Figure 4: Illustration of features extracted

Figure 4 illustrates the features obtained for a sample periocular image for SIFT, SURF and BSIF feature extraction techniques.

2.4 Probe Data Acquisition

The probe data is acquired by the user in a self acquisition mode. The successful capture of the probe image is indicated by an audio beep. The captured probe images are used to generate the features using the techniques mentioned in Section 2.3. The generated features from probe data are compared against the reference data using the comparison methods described in Section 2.5.

2.5 Feature Comparison

The obtained features from reference images using SIFT, SURF and BSIF are compared to the probe images using various methods. The key points obtained from both SIFT and SURF are compared using Fast Library for Approximate Nearest Neighbors (FLANN) [ML09, BK08] with a brute force comparison method while the features from BSIF technique are compared using the Bhattacharya distance. The features based on the BSIF technique are encoded the form of gray images to obtain efficiently the histogram of source and probe images in order to achieve faster comparison [CS02]. Let the histogram for the reference be represented by H_r and the histogram for the probe be represented by H_p, then the distance between the histograms is given by :

$$d(H_r, H_p) = \sqrt{1 - \frac{1}{\sqrt{\overline{H_r} * \overline{H_p} * N^2}} \sum_i \sqrt{H_r * H_p}} \tag{2}$$

where N is the number of bins and $\overline{H_r}$, $\overline{H_p}$ present the mean values of the histogram of reference and probe image. If the computed distance if lower than the threshold, the user is accepted. For any probe image and an associated distance measure exceeding this threshold the decision is a reject.

3 Evaluation of Proposed System

3.1 Hardware Employed

In order to study the usability of the system on various kind of portable devices based on the Android operating system, we have used Samsung Galaxy S5, ASUS Nexus 7 (2013) and Samsung Galaxy Note 10.1 tablet in our experiments. The detailed specifications of each of the device is provided in the Table 1. Samsung Galaxy S5 provides the full HD image from the front camera with a resolution of 2 mega-pixels whereas others do not. All of the devices were operated in the natural illumination with day light with no external flash light.

Table 1: Specifications of hardware used in this work

Device	Operating System	Screen Size	Rear Camera	Front Camera
Samsung Galaxy S5	Android v4.4.2	1080 x 1920 pixels 5.1 inches	16 MP, 5312 x 2988 pixels	2 MP
Samsung Galaxy Note 10.1	Android v4.4.2	800 x 1280 pixels, 10.1 inches	5 MP, 2592 x 1944 pixels	1.9 MP
ASUS Nexus 7	Android v4.4.2	1200 x 1920 pixels, 7.0 inches	5 MP, 1280 x 760 pixels	1.2 MP

3.2 Implementation Details

The proposed system for periocular based authentication is developed on the Android operating system. The system is compatible with any other device having at least a dual-core processor. The system employs the open source framework OpenCV [BK08] for the Android operating systems to perform the graphical and image processing operations, which include user interaction, image capture and feature extraction. Optimizations have been done in necessary cases to improve the processing speed in various pipelines such as feature extraction or feature comparison.

3.3 Evaluation Details

The proposed authentication system based on periocular information for smartphones was evaluated by enrolling one user at a time by capturing 5 reference images on the three different portable devices as mentioned in Table 1. The enrolled user was then asked to authenticate on a device by providing a probe image in 10 different sessions over a period of 10 days. In total, 32 users were asked to test the proposed system which included 29 male and 3 female subjects.

For each enrolled user, the data was captured using the frontal and rear camera from all

three devices. A set of 5 reference images were obtained for both eyes from all three different devices in natural illumination, equivalently, the three devices correspond to 6 different cameras. Similarly, a set of 10 images were obtained for both eyes as probe samples for each subject from three different devices. Probe images corresponding to periocular images were obtained at different session (days). The total number of images for each subject amounts to 15 images for each acquisition corresponding to a single camera. Thus, the complete test dataset consists of 480 images corresponding to frontal camera, 480 images corresponding to rear camera and 480 images corresponding to assisted acquisition from rear camera considering both eyes. The database consists of a total of 2880 periocular images corresponding to a single device. As the complete database is collected using three different devices, a total of 8640 biometric templates are obtained using 17280 periocular images. According to the protocol employed in this system, each subject has one identity provided by both eyes.

3.4 Verification Protocol

Each of the enrolled subjects has 5 reference images from both eyes and probed using 10 different images obtained at different sessions from both eyes in the complete database collected over the period of one month. The features obtained using both eyes are treated as one single identity for the subject. Each of the probe image is compared against the reference image on the respective device to obtain the genuine and imposter score. The total number of genuine scores obtained for each user is 50 ($5\ reference \times 10\ probe$) while the number of imposter scores is 1550 ($31\ subjects \times 50\ images$). Comparison of one particular user with the rest of the enrolled users results in 49600 ($32\ subjects \times 31\ imposter \times 50\ images$) imposter scores for one particular camera and one particular feature. For instance for the frontal camera of the Samsung Galaxy Note combined with BSIF feature extraction method results in 1600 genuine scores and 49600 imposter scores.

4 Experimental Results

The experimental results obtained on all different smartphones are reported in terms of Genuine Match Rate (GMR) (%) at a given False Match Rate (FMR) (%) [ISO07]. The Genuine Match Rate (GMR) is defined using the False Non Match Rate (FNMR) (%) as:

$$GMR = 1 - FNMR \tag{3}$$

4.1 Experiment 1

This set of experiments were carried out to gauge the performance of the system as a standalone authentication application where the subjects have captured enrollment and probe images in a self acquisition mode. The obtained results of the experiments are outlined in Table 2. Of the three feature extraction techniques, it can be observed that BSIF features obtained with a filter dimension of 9×9 with 8 layers provides the best performance on all the cameras corresponding to different devices. The best scores for GMR values at lower FMR rates such as 0.01% is obtained with BSIF features. The best performance is reported for the rear camera of Samsung Galaxy Note 10.1 with a score of 89.38% while the lowest score is obtained for images from the rear camera of Asus Nexus

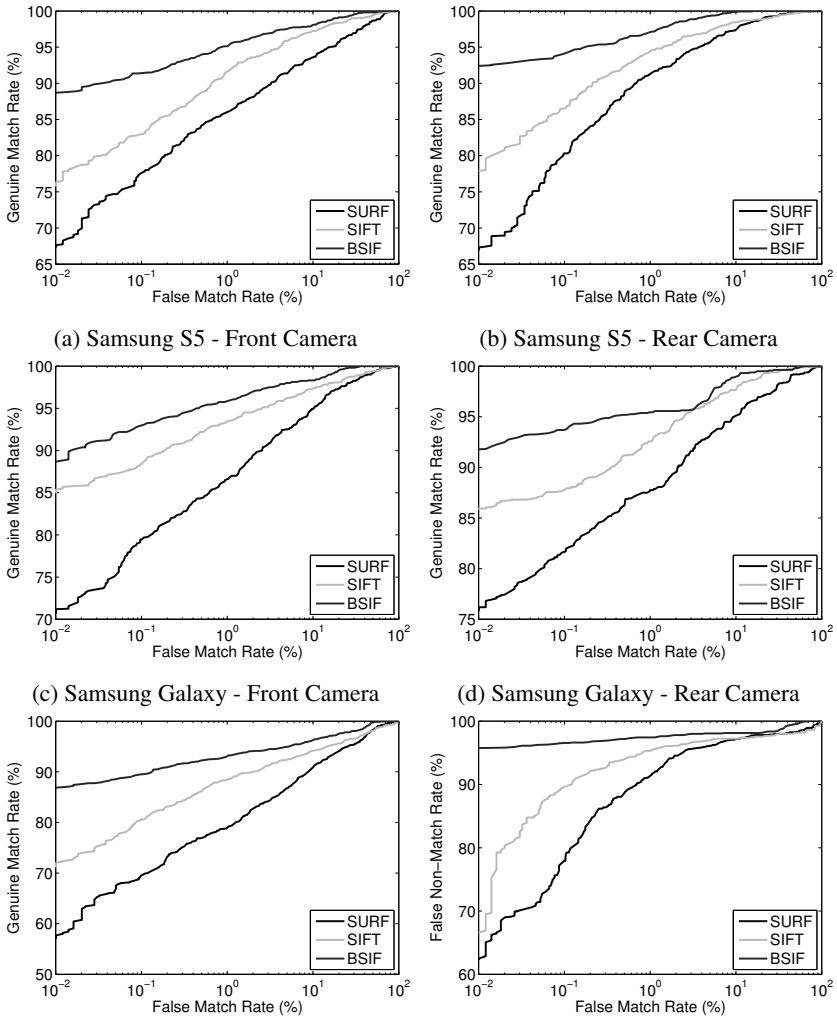
7 at FMR of 0.01%. Key observations from this set of experiments can be outlined as :

1. The performance obtained from the images captured using rear camera is higher than the performance obtained using images captured from the frontal camera in each device. This can be attributed to the superior images obtained in terms of resolution under the same imaging conditions.
2. Another important aspect to note is the performance of the system with respect to the placement of camera on the device. It can be observed from the Table 2 that Samsung Galaxy Note 10.1 has the best performance for the images corresponding to both front and rear camera. Unlike the other two devices, the camera on this device is centred exactly on the side corresponding to the longer dimension. The alignment of the camera in such a position allows the user to interact with the device in a convenient way such that they can look into the screen while capturing the image. The placement of the camera in a corner causes the user to look at it and thus causing the head pose change, which further leads to poor periocular images.

Phone	Camera Position	Feature	FMR @ 0.01%	FMR @ 0.1%	FMR @ 1%
Samsung Tab	Front	SIFT	84.94	88.44	93.56
		SURF	70.75	79.50	86.63
		BSIF	**85.69**	**89.44**	**93.63**
	Rear	SIFT	85.88	87.94	92.56
		SURF	75.88	81.69	87.75
		BSIF	**89.38**	**91.13**	**94.94**
Samsung S5	Front	SIFT	75.75	83.00	91.63
		SURF	67.38	77.69	86.19
		BSIF	**80.19**	**83.88**	**90.06**
	Rear	SIFT	78.00	86.56	94.50
		SURF	67.00	80.31	91.69
		BSIF	**83.19**	**86.69**	**92.44**
Asus Tab	Front	SIFT	71.13	80.63	88.63
		SURF	57.13	69.94	79.00
		BSIF	**82.38**	**86.94**	**90.94**
	Rear	SIFT	66.88	**89.69**	**95.31**
		SURF	62.38	77.94	91.56
		BSIF	**80.00**	88.06	93.00

Table 2: Verification results in terms of GMR at specific values of FMR

Figure 5 presents the plots of the obtained Genuine Match Rate (i.e. $1 - FNMR$) corresponding to various FMR values. The performance of the different feature extraction schemes follows consistently the trend that BSIF features provide the highest performance while SURF features provide the lowest performance.



(a) Samsung S5 - Front Camera

(b) Samsung S5 - Rear Camera

(c) Samsung Galaxy - Front Camera

(d) Samsung Galaxy - Rear Camera

(e) Asus Nexus - Front Camera

(f) Asus Nexus - Rear Camera

Figure 5: Verification performance in terms of GMR at different values of FMR

4.2 Experiment 2

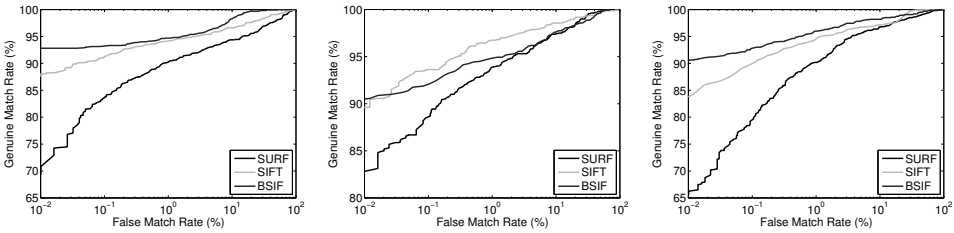
In order to evaluate the impact on performance when the subjects themselves acquired the images, another set of images for each user was captured using the rear camera through assisted mode by a trained expert. All the subjects in the experiment were also enrolled and verified through the images acquired using the assisted mode. A similar protocol of capturing 5 reference images and 10 probe images was followed for this set of experiments. It can be observed from the Table 3 that the performance of the system is slightly higher as

compared to the performance of images stemming from the rear camera in the self acquisition mode. The superior performance in this case is due to uniform pose of the subject under no restriction to adjust the position in accordance to the camera. The acquisition time for this set of experiments were shorter due to assisted acquisition. Nevertheless, the improvement in performance was not drastically high as compared to the self acquisition mode validating the suitability and user-friendliness of the proposed system while being robust in terms of performance for everyday authentication applications.

Phone	Feature	FMR @ 0.01%	FMR @ 0.1%	FMR @ 1%
Samsung Tab	SIFT	87.56	91.19	94.19
	SURF	69.38	83.75	90.44
	BSIF	**91.81**	**93.50**	**94.50**
Samsung S5	SIFT	89.56	**93.63**	**96.75**
	SURF	83.13	88.69	93.88
	BSIF	**90.56**	92.13	94.94
Asus Tab	SIFT	83.81	90.19	94.88
	SURF	65.56	79.68	90.18
	BSIF	**89.56**	**93.63**	**96.75**

Table 3: Verification results obtained with assisted acquisition in terms of GMR at specific values of FMR

Figure 6 presents the obtained GMR values for different FMR values for the images acquired in assisted mode using the proposed system. As observed in the earlier set of experiments, it can be seen that the best performance is obtained for BSIF features at lower FMR values.



(a) Samsung Tab - Rear Camera (b) Samsung S5 - Rear Camera (c) Asus Nexus - Rear Camera

Figure 6: Verification performance with assisted acquisition in terms of GMR at various levels of FMR

5 Conclusion

This work has proposed a new and unique biometric authentication system based on the periocular information for smartphones. The proposed system has been implemented and extensively evaluated on three different Android devices having different imaging sensors.

Each device is evaluated for performance from images in frontal and rear camera to study the impact of resolution of the camera and the factor of usability. The proposed system has been tested with three well known feature extraction techniques. The best result of 89.38% for GMR is obtained at a $FMR = 0.01\%$ for the Samsung Galaxy Note 10.1 validating the robustness of the proposed system. At the same time, all the different systems have consistently performed well with a GMR score of more than 80%. With the obtained results, it can be clearly seen that the proposed system is robust to be employed in regular authentication scenarios on smartphones.

Of all the three feature extraction techniques employed, BSIF has consistently preformed well in all the conditions. A possible future work on score-level fusion can be carried out to make the system more robust. Another aspect of the improved performance under assisted acquisition suggests the necessity for the pose normalization of the face images before the extraction of periocular image to have non-uniform shadows. Incorporation of normalization of face pose to mitigate the factors affecting the performance can be studied in future works.

The other important factor to consider in the future work is to incorporate presentation attack detection (a.k.a spoofing) in the proposed system to make it more robust, reliable and trust worthy while maintaining the user-friendliness.

6 Acknowledgements

The authors wish to express thanks to Morpho (Safran Group) for supporting this work, and in particular to Morpho Research & Technology team for the fruitful technical and scientific exchanges related to this particular work.

References

[BK08] Dr. Gary Rost Bradski and Adrian Kaehler. *Learning Opencv, 1st Edition*. O'Reilly Media, Inc., first edition, 2008.

[BLGT06] Manuele Bicego, Andrea Lagorio, Enrico Grosso, and Massimo Tistarelli. On the use of SIFT features for face authentication. In *Conference on Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06.*, pages 35–35. IEEE, 2006.

[CS02] Sung-Hyuk Cha and Sargur N Srihari. On measuring the distance between histograms. *Pattern Recognition*, 35(6):1355–1370, 2002.

[Dau06] John Daugman. Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons. *Proceedings of the IEEE*, 94(11):1927–1935, 2006.

[DB13] Mohammad Derawi and Patrick Bours. Gait and activity recognition using commercial phones. *Computers & Security*, 39:137–144, 2013.

[Hos] Roman Hosek. Android eye detection updated for OpenCV 2.4.6. "`http://romanhosek.cz/android-eye-detection-updated-for-opencv-2-4-6/`". Date of access : 01-May-2014.

[ISO07] ISO/IEC JTC1 SC37 Biometrics. International Standards ISO/IEC TR 24722, Multimodal and Other Multibiometric Fusion. Technical report, International Organization for Standardisation, 2007.

[KR12] Juho Kannala and Esa Rahtu. BSIF: Binarized statistical image features. In *21st International Conference on Pattern Recognition (ICPR), 2012*, pages 1363–1366. IEEE, 2012.

[KRB14] Kiran B. Raja, R Raghavendra, and Christoph Busch. Binarized Statistical Features For Improved Iris and Periocular Recognition in Visible Spectrum. In *2nd International Workshop on Biometrics and Forensics, Malta*. IEEE, 2014.

[ML09] Marius Muja and David G Lowe. Fast Approximate Nearest Neighbors with Automatic Algorithm Configuration. In *VISAPP (1)*, pages 331–340, 2009.

[NDBB11] Claudia Nickel, Mohammad O Derawi, Patrick Bours, and Christoph Busch. Scenario test of accelerometer-based biometric gait recognition. In *Security and Communication Networks (IWSCN). 3rd International Workshop, Gjøvik, Norway*, 2011.

[PJRJ11] Unsang Park, Ross Jillela, Arun Ross, and Anil K Jain. Periocular biometrics in the visible spectrum. *IEEE Transactions on Information Forensics and Security*, 6(1):96–106, 2011.

[RBY13] R Raghavendra, Christoph Busch, and Bian Yang. Scaling-robust fingerprint verification with smartphone camera in real-life scenarios. In *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013*, pages 1–8. IEEE, 2013.

[RCB01] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. An Analysis of Minutiae Matching Strength. In Josef Bigun and Fabrizio Smeraldi, editors, *Audio- and Video-Based Biometric Person Authentication*, volume 2091 of *Lecture Notes in Computer Science*, pages 223–228. Springer Berlin Heidelberg, 2001.

[SBB13] Chris Stein, Vincent Bouatou, and Christoph Busch. Video-based fingerphoto recognition with anti-spoofing techniques with smartphone cameras. In *International Conference of the Biometrics Special Interest Group (BIOSIG), 2013*, pages 1–12. IEEE, 2013.

[VJ01] Paul Viola and Michael Jones. Rapid object detection using a boosted cascade of simple features. In *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001. CVPR 2001.*, volume 1, pages I–511. IEEE, 2001.

[WN10] Heiko Witte and Claudia Nickel. Modular Biometric Authentication Service System (MBASSy). In *BIOSIG*, pages 115–120. Citeseer, 2010.

[XCH+10] Juefei Xu, Miriam Cha, Joseph L Heyman, Shreyas Venugopalan, Ramzi Abiantun, and Marios Savvides. Robust local binary pattern feature sets for periocular biometric identification. In *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), 2010*, pages 1–8. IEEE, 2010.

[YBAG04] Jeff Jianxin Yan, Alan F Blackwell, Ross J Anderson, and Alasdair Grant. Password Memorability and Security: Empirical Results. *IEEE Security & privacy*, 2(5):25–31, 2004.