Multi-biometric Template Protection on Smartphones: An Approach Based on Binarized Statistical Features and Bloom Filters

Martin Stokkenes[1(✉)], Raghavendra Ramachandra[1], Kiran B. Raja[1], Morten Sigaard[2], Marta Gomez-Barrero[3], and Christoph Busch[1]

[1] Norwegian University of Science and Technology, Trondheim, Norway
{martin.stokkenes2,raghavendra.ramachandra,kiran.raja,
christoph.busch}@ntnu.no
[2] Denmark Technical University, Kongens Lyngby, Denmark
Mortenkrsi@hotmail.com
[3] Hochschule Darmstadt, Darmstadt, Germany
marta.gomez-barrero@h-da.de

Abstract. Widespread use of biometric systems on smartphones raises the need to evaluate the feasibility of protecting biometric templates stored on such devices to preserve privacy. To this extent, we propose a method for securing multiple biometric templates on smartphones, applying the concepts of Bloom filters along with binarized statistical image features descriptor. The proposed multi-biometric template system is first evaluated on a dataset of 94 subjects captured with Samsung S5 and then tested in a real-life access control scenario. The recognition performance of the protected system based on the facial characteristic and the two periocular regions is observed equally good as the baseline performance of unprotected biometric system. The observed Genuine-Match-Rate (GMR) of 91.61% at a False-Match-Rate (FMR) of 0.01% indicates the robustness and applicability of the proposed system in everyday authentication scenario. The reliability of the system is further tested by engaging disjoint subset of users, who were tasked to use the proposed system in their daily activities for a number of days. Obtained results indicate the robustness of the proposed system to preserve user privacy while not compromising the inherent authentication accuracy without protected templates.

1 Introduction

Biometric recognition involves verifying a claimed identity based on physiological (e.g. face, fingerprint, veins, etc.) and behavioural characteristics (keystroke, mouse dynamics, gait, etc.). Biometrics has become a part of everyone's daily life. The reliability and the accuracy of biometrics based systems, especially in constrained conditions have shown the benefit for applications such as border control, access control, forensics, etc. In spite of broad deployment of biometric

C. Beltrán-Castañón et al. (Eds.): CIARP 2016, LNCS 10125, pp. 385–392, 2017.
DOI: 10.1007/978-3-319-52277-7_47

systems, the accuracy of such systems has remained challenging in unconstrained conditions. Further, the vulnerability of biometric systems being attacked at various levels (sensor, comparison etc.) and the privacy concerns regarding stored biometric templates create a psychological barrier in accepting biometrics in the general sphere of life.

However, access control systems have started to employ smartphone based biometric authentication using face [5], iris [9] and periocular [7] to authenticate the user. Such systems further gained mainstream attention as major smartphone vendors like Apple, Samsung, HTC, etc. provided fingerprint-based authentication that can be used to unlock the smartphone and convenient access control. However, as the ease of presentation attacks on such sensors is known [2], fingerprint recognition should be used in applications including banking and finance transactions only if the transaction volume is limited. For higher transaction volumes face and periocular recognition are a better choice.

As the number of applications using smartphone access control continues to increase, the need to protect the biometric templates when stored on the device has become a task of utmost importance to preserve the privacy of the smartphone user. Even though device manufacturers have claimed to protect the biometric data by keeping the biometric templates in the secured hardware separated from the rest of the device, one cannot rule out the possibility of indirect attacks to retrieve stored biometric templates - for instance fingerprint templates stored in the smartphone [14]. The recent work reported in [14] has exposed the security loop-hole in HTC One Max smartphone where the fingerprint template was accessed from smartphone. Similar attacks carried out on Samsung Galaxy S5 smartphone to avail the fingerprint template further exemplifies the lapse of hardware based security [14]. These incidents illustrate the demand for an efficient biometric template protection scheme to ensure the user's privacy and to avoid misuse of the stolen biometric templates on smartphones.

Recently significant progress has been made in smartphone based biometrics. The majority of the work is devoted to exploring the embedded sensors and designing efficient feature extraction and comparison algorithms of low complexity that are suitable for smartphones [1,3]. However to the best of our knowledge, there is no reported work addressing biometric template protection on smartphones. In general, biometric template protection, which is one of the widely explored areas in biometrics, has resulted in a significant number of algorithms [10]. A very promising template protection approach using Bloom filters was proposed recently [11] and studied for different biometric characteristics such as iris [11] and face [12]. These studies have shown that it is possible to obtain privacy preserving protection which is not degrading the verification performance. Motivated by the lapse of hardware based smartphone security and leveraging the secure nature of Bloom filters for biometric templates, we introduce this template protection scheme for a smartphone based multi-biometric system. Our intention is to create the right balance between the accuracy and privacy, both of which are essential blocks for the success of smartphone based secure access control applications employing biometrics.

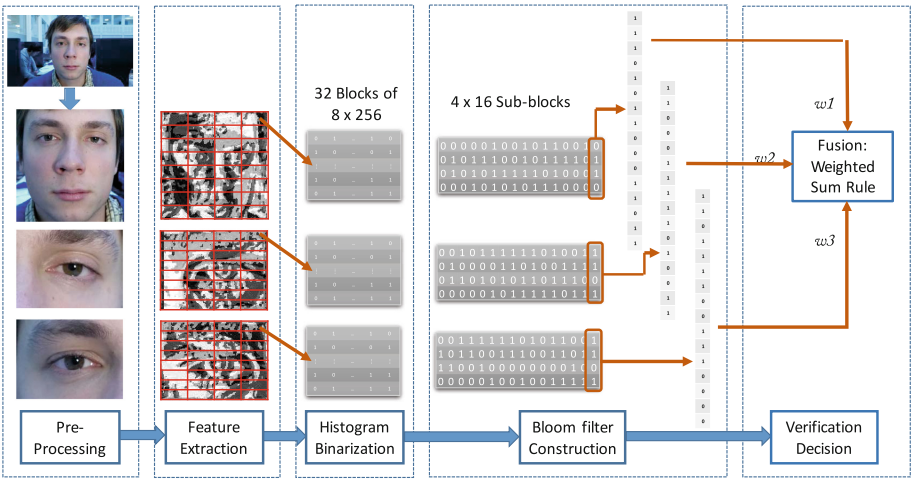


Fig. 1. Block diagram of the proposed multi-biometric template protection scheme for smartphones

Template protection schemes can only be considered secure if they adhere to the principles of Irreversibility and Unlinkability, which are requirements according to the ISO/IEC 24745 standard[1].

Irreversibility - It should not be possible to reconstruct from a protected biometric template the original template or a biometric sample.

Unlinkability - It should be infeasible to link a subject's protected biometric template from one application to another.

The rest of the paper is organized in the following manner: Sect. 2 introduces the proposed approach for multi-biometric template protected system on smartphone. Section 3 provides the details on the experimental set-up, evaluation protocols and the obtained results. Section 4 provides the concluding remarks of the current work and identifies the possible future work.

2 Proposed Multi-biometric Approach

This section provides the details of the proposed approach to enable a multi-biometric template protection system on smartphone. The proposed system includes the extraction of statistical image features from the captured face and periocular images and binarization of the extracted feature vectors followed by the transformation to protected templates using Bloom filters. The choice of Bloom filters is motivated by the non-degraded biometric performance while securing the biometric template as reported in [4].

[1] International Organization for Standardization, ISO/IEC 24745:2011, 'Information technology – Security techniques – Biometric information protection', 2011.

Figure 1 shows the block diagram of the proposed biometric template protection scheme. The proposed system consists of three principal steps: (1) Segmentation of face and periocular region (left and right) from the captured image. (2) Generalized feature extraction and binarization scheme to extract the discriminant binary features from all segmented image regions. (3) Template protection using Bloom filters.

2.1 Face and Periocular Segmentation

In this work, we have carried out the face and periocular segmentation based on the Haar cascade classifier [13]. We have implemented two different classifiers as proposed in [8] to segment the face and periocular region (left and right) in real-time. Figure 1 shows an example and the results for the segmented face and periocular regions. The segmented face images are resized to 64×80 pixels and the periocular image to a size of 120×88 pixels that will be used for feature extraction. The parameters used for the resize step are selected based on the testing database (see Sect. 3) by considering both accuracy and the need for low complexity computations on the smartphone.

2.2 Generalized Feature Extraction and Binarization

The selection of a suitable feature extraction technique plays an important role to achieve both biometric template protection and also the expected verification performance on the smartphone. The Bloom filter, as many other template protection approaches, requires binary feature vectors as input. The main challenge is to use a low computation based binary feature extraction scheme that can provide good verification accuracy on both face and periocular biometrics. In this work we explore the binarized statistical image features (BSIF) [6] that can provide binary features by performing convolution with a number of filters that are learned on natural images. These statistically independent filters are optimized by exploring natural image statistics via unsupervised learning using Independent Component Analysis (ICA). Depending upon the various patch sizes and the number of ICA basis functions, one can learn a number of BSIF filters with various sizes (adjusted to the patch size) and bits (number of basis selected from ICA). In this work, we propose a feature extraction scheme based on eight different filter sizes such as: 3×3, 5×5, 7×7, 9×9, 11×11, 13×13, 15×15 and 17×17 and each filter is of 8 bit in length. The choices of the BSIF filter size and length is based on empirical trials on a testing dataset yielding higher verification accuracy (see Sect. 3).

Given a face (or periocular) image captured using the smartphone, we first divide the entire image into 32 different blocks such that each block size is of 8×20 pixels in the case of the face image and 15×22 pixels in the case of a periocular image. Then, for each block, we extract the BSIF features by convolving eight different BSIF filters each of 8-bit length. Finally the response of each filter with 8-bit size is encoded to a histogram of dimension 1×256. Since we have eight different filters, the feature size for each block is 8×256. We repeat this process

for each block and concatenate the result to a final BSIF feature vector set of dimension 65536. The extracted histogram features h is binarized as follows:

$$h(i,j) = \begin{cases} 1 & \text{if } h(i,j) > 0 \\ 0 & \text{if } h(i,j) = 0 \end{cases} \tag{1}$$

We finally reorganize the binarized features to have a matrix of dimension 4×8 rows and 8×256 columns that can be used to generate a protected template using Bloom filter [4][2].

2.3 Biometric Template Protection: Bloom Filters

In this work we have employed the Bloom filter by considering its irreversibility property in generating protected biometric templates [4]. The Bloom filter parameters are defined as follows: $nBits$ denotes the number of bits used to address a location in a Bloom filter. $nWords$ denotes the number of inputs to each Bloom filter. The length of each Bloom filter is defined by 2^{nBits}. Based on recommendations in [4] we use $nBits = 4$, which makes the length of each Bloom filter 16-bits. The number of inputs to one Bloom filter is restricted to $nWords \leq 2^{nBits}$. In our case we set $nWords = 16$.

Input to each Bloom filter is derived in the following manner: As described in the previous section, each template consists of 32 blocks of 8×256 binary elements, $x_{ij} \in 0, 1$. To address a location in a Bloom filter of length 16, we further divide each of the 32 blocks into 4×16 sub-blocks where each column (containing 4 binary values) is used as a codeword denoting an index in a Bloom filter. The value in the location indicated by the index is then set to 1. This approach will generate 1024 Bloom filters of length 2^{nBits}, achieving a final template of 2 kB.

To compare two templates we obtain a dissimilarity score using the distance metric as shown in Eq. 2 where $|b|$ is the hamming weight or number of bits set to one in a Bloom filter, and $HD(b_i, b_j)$ is the Hamming Distance between two Bloom filters or number of disagreeing pairs of bits [4].

$$DS(b_i, b_j) = \frac{HD(b_i, b_j)}{|b_i| + |b_j|} \tag{2}$$

The unprotected and protected templates for face and periocular (left and right) regions are processed independently to obtain three separate dissimilarity scores. The final decision result is obtained by taking the majority vote on the decisions from each of the three scores.

3 Experimental Setup and Results

In this section we present the results of the proposed biometric template protection scheme for face and periocular biometrics on a smartphone. First, we evaluate the proposed system on a newly collected multi-biometric database using

[2] The reorganization of the features will ease the implementation of the Bloom filter protection technique.

Table 1. Quantitative results of proposed scheme on testing database

Verification performance				
Characteristic	Without Bloom filter		With Bloom filter	
	GMR@FMR = 0.01%	EER%	GMR@FMR = 0.01%	EER%
Face	90.05	1.67	82.63	2.90
Left periocular	83.32	3.20	72.22	5.39
Right periocular	83.78	4.53	68.03	5.48
Fused	95.95	1.12	91.61	1.80

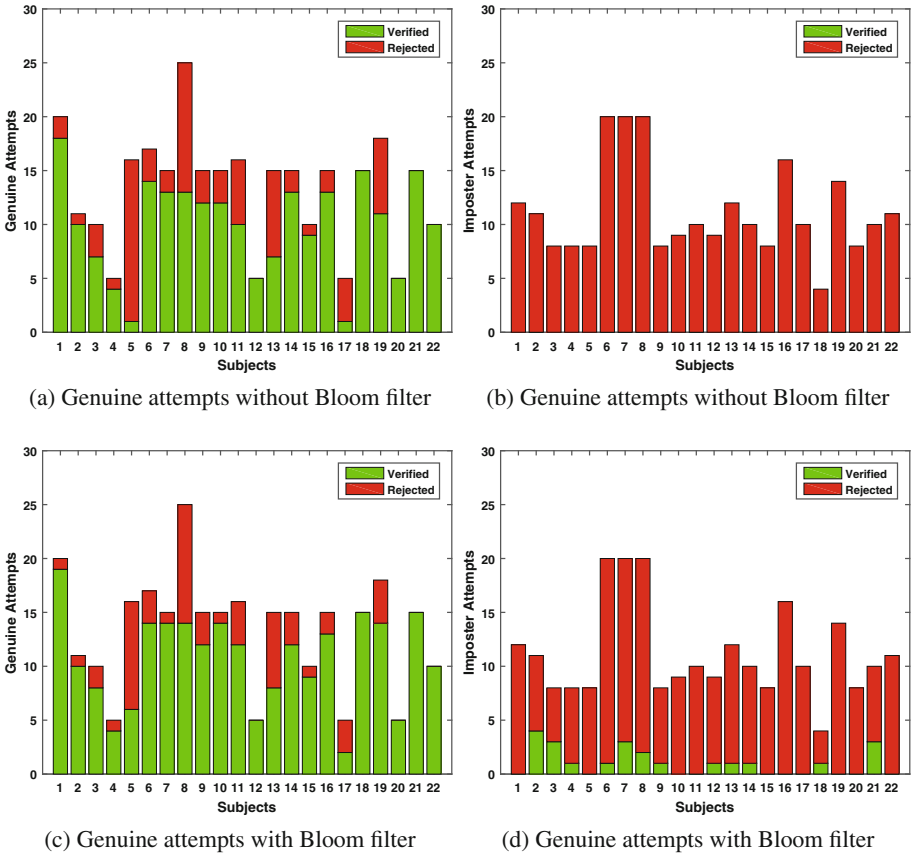
the Samsung Galaxy S5 smartphone constituting of 94 subjects. Table 1 shows the results from evaluation on the testing database in terms of Genuine Match Rate (GMR) for a fixed value of False Match Rate (FMR) and Equal Error Rate (EER). We observe that there is some performance degradation after Bloom filter is applied. However, with fusion of the different biometric characteristics we obtain a GMR of 91.61% when FMR = 0.01%, indicating robustness and applicability of the proposed template protection scheme on smartphones for multi-biometrics. Then, a real-time evaluation, described in the next section, is carried out by providing the template protected biometric system for access control to 22 subjects on a Samsung Galaxy S5.

3.1 Real-Time Evaluation of the Proposed System

In this experiment the smartphone application was distributed on a Samsung S5 phone to 22 unique subjects along with the instruction to use the proposed system in order gain access to a secure application using multi-biometric (face and periocular) recognition. The threshold for genuine accept rate was set on the basis of threshold obtained on testing set at an FAR of 0.1%. The subjects were instructed to enrol into the system with 10 images and they were further instructed to test the application independently in various lighting conditions for a number of times.

On average 10 genuine attempts were recorded for the entire subset of users. The users were also asked to attempt to login as impostors to some other subjects than themselves to gauge the robustness of the system against zero-effort impostor attempts. These subjects repeatedly tried to gain impostor access for a period of 4 days. Experiments were carefully designed and the users were asked to attack target subjects that had the same ethnical background, for instance, an American subject was asked to pose as another compatriot to account for the robust impostor attacks.

Figure 2a shows the number of successful attempts when the system was not operating with protected templates and Fig. 2b shows the impostor attempts. The section indicated in the green color signifies the successful genuine attempts while the sections in red color indicate the rejection of the attempts for both genuine subjects and impostors. It can be observed from Fig. 2c and 2d that the



(a) Genuine attempts without Bloom filter

(b) Genuine attempts without Bloom filter

(c) Genuine attempts with Bloom filter

(d) Genuine attempts with Bloom filter

Fig. 2. Genuine and impostor attempts in real-time application of proposed system. Green color indicated number of successful attempts and red color indicates the number of failed attempts to login to the system. (Color figure online)

system with the proposed template protection scheme works under operational conditions as good as the system without template protection. Very equivalent performance in both cases indicates the robust nature of the proposed template protection scheme while not compromising the verification accuracy significantly.

Based on the extensive analysis conducted from the above experiments, it can be observed that the proposed template protection system for multi-biometric based smartphone application is promising with an acceptable degradation of verification accuracy.

4 Conclusion

Preserving privacy of the smartphone user's biometric templates is of utmost importance as the biometric characteristics cannot be renewed in case of

compromise arising out of attacks on the biometric references. Wide spread use of smartphones for biometrics based authentication further justifies the need for protecting the templates on smartphones. In this work we have proposed a novel system using the strengths of Bloom filter and generalizability of BSIF on both face and periocular characteristics to devise a template protected biometric system for smartphones. Extensive experiments conducted on the database of 94 subjects indicate high verification accuracy even with protected templates. The GMR of 91.61% justifies the applicability of the proposed system for a real-life authentication scenario. Further, evaluation using disjoint set of subjects to test the reliability of system indicates the robust nature of proposed system against zero impostor attempts even with same ethnical origin.

References

1. Barra, S., Casanova, A., Narducci, F., Ricciardi, S.: Ubiquitous iris recognition by means of mobile devices. Pattern Recogn. Lett. **57**, 66–73 (2015)
2. Cao, K., Jain, A.: Hacking mobile phones using 2D printed fingerprints. Michigan State University, MSU, Technical report (2016)
3. De Marsico, M., Galdi, C., Nappi, M., Riccio, D.: Firme: face and iris recognition for mobile engagement. Image Vis. Comput. **32**(12), 1161–1172 (2014)
4. Gomez-Barrero, M., Rathgeb, C., Galbally, J., Busch, C., Fierrez, J.: Unlinkable and irreversible biometric template protection based on bloom filters. Inf. Sci. **370**, 18–32 (2016). http://www.sciencedirect.com/science/article/pii/S0020025516304753
5. Ijiri, Y., Sakuragi, M., Lao, S.: Security management for mobile devices by face recognition. In: 7th International Conference on Mobile Data Management, MDM 2006, p. 49, May 2006
6. Kannala, J., Rahtu, E.: BSIF: Binarized statistical image features. In: 21st International Conference on Pattern Recognition (ICPR), pp. 1363–1366 (2012)
7. Raja, K.B., Raghavendra, R., Stokkenes, M., Busch, C.: Smartphone authentication system using periocular biometrics. In: 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–8, September 2014
8. Raja, K.B., Raghavendra, R., Stokkenes, M., Busch, C.: Multi-modal authentication system for smartphones using face, iris and periocular. In: Proceedings of 2015 International Conference on Biometrics, ICB 2015, pp. 143–150 (2015)
9. Marsico, M.D., Galdi, C., Nappi, M., Riccio, D.: Firme: face and iris recognition for mobile engagement. Image Vis. Comput. **32**(12), 1161–1172 (2014)
10. Nandakumar, K., Jain, A.K.: Biometric template protection: bridging the performance gap between theory and practice. IEEE Sig. Process. Mag. **32**(5), 88–100 (2015)
11. Rathgeb, C., Breitinger, F., Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In: Proceedings - 2013 International Conference on Biometrics, ICB 2013 (2013)
12. Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J., Fierrez, J.: Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In: 2015 International Workshop on Biometrics and Forensics (IWBF), pp. 1–6, March 2015
13. Viola, P., Jones, M.: Robust real-time face detection. Int. J. Comput. Vis. **57**(2), 137–154 (2004)
14. Zhang, Y., Chen, Z., Xue, H., Wei, T.: Fingerprints on mobile devices: abusing and eaking. In: Black Hat Conference (2015)