Facial bihashing based user-device physical unclonable function for bring your own device security

Zheng, Yue; Cao, Yuan; Chang, Chip Hong

2018

Zheng, Y., Cao, Y., & Chang, C. H. (2018). Facial bihashing based user-device physical unclonable function for bring your own device security. 2018 IEEE International Conference on Consumer Electronics (ICCE). doi:10.1109/ICCE.2018.8326074

<https://hdl.handle.net/10356/80438>

<https://doi.org/10.1109/ICCE.2018.8326074>

© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/ICCE.2018.8326074>].

Downloaded on 26 Apr 2023 16:46:02 SGT

Facial Biohashing Based User-Device Physical Unclonable Function for Bring Your Own Device Security

(Invited Paper)

Yue Zheng, Yuan Cao, and Chip-Hong Chang

School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

Email: yzheng015@e.ntu.edu.sg, ycao3@e.ntu.edu.sg, echchang@ntu.edu.sg

Abstract—Bring your own device (BYOD) is gaining popularity. Using multifarious personal devices in the workplace to perform work-related tasks brings new challenges to trust and privacy management. Existing authentication schemes usually target at user or device separately, while the BYOD system needs to ensure that only the authorized user with the trusted devices can be given access. This paper presents a novel biohashing based user-device physical unclonable function (UD PUF) to provide a bipartite authentication of both user and device for the BYOD system. Biometric features are extracted as user identity while PUF endows the device with an inseparable and unclonable “fingerprint”. Biohashing acts as an intermediary between these two incoherent macroscopic biometric and microscopic silicon entropy sources for security enhancement. The concept is demonstrated using a 64×64 image sensor PUF simulated in 180nm 3.3V CMOS technology, and the ORL and yale databases of faces. Our preliminary experimental results showed that a genuine (user, device, challenge) combination exhibits a very low equal error rate of 0.032, and tampering of any elements of the tuple will cause the hamming distance between the “live” and enrolled templates to have nearly random distribution.

I. INTRODUCTION

With the rapid development of technology, it has become a commonplace that the personal laptops, tablets, and smart phones owned by company employees are more advanced and newer than the IT equipment deployed by their companies. This inevitable IT self-sufficiency drives the bring your own device (BYOD) policy, which allows employees to bring personally owned devices to access privileged company information and applications. There are good incentives, such as increased productivity, employee satisfaction and cost savings, for organizations to embrace BYOD. The dark side of BYOD is that companies have little or no control over those personal devices, which may be lost, stolen or compromised to threaten IT security and put company sensitive information systems at risk. Therefore, measures to ensure that only the authorized person with trusted devices can access the corporate networks are of paramount importance for enterprise to contrive BYOD.

Instead of the traditional way of claiming identity by password, biometric features are increasingly utilized for user identification due to their appealing attributes such as easy to install and use, non-repudiable accountability, time and cost saving, etc. Owing to the strong and permanent link between human and their biometrics, one major concern for biometric identification is the security and privacy of biometric templates. Existing countermeasures [1] include storing bio-

metric templates in secure hardware like A8 chip on Apple iPhone6, encrypting them using standard encryption algorithms like AES and RSA, and adopting feature transformation approaches such as biohashing. As only the user but not the device is identified, when the device is lost or stolen, the registered biometric templates are vulnerable to invasive or semi-invasive attacks and confidential information may be accessed with proxy device by forging the user biometric.

In much the same way as biometrics can be used to identify different users, each device can also be identified by its device-unique “fingerprint”. Such a unique fingerprint can be generated by a physical unclonable function (PUF). A PUF is an emerging security primitive that exploits random unpredictable manufacturing process variations of identically designed circuits to generate a unique response upon challenged by a query. PUF is generally considered to be more secure than using conventional hardcoded electronic tagging, digital signature or cryptographic hash for device authentication as it does not rely on the secure storage of secret key. Consequently, PUF holds strong promise to protect biometric templates for bipartite authentication, i.e., to identify the user based on his personal device and to identify the device based on its associated owner.

In this paper, a new biohashing based user-device (UD) PUF for BYOD system is proposed. UD PUF provides an interesting means to bind the biometric feature with the device “fingerprint” to increase the vigilance for access control. UD PUF is a nascent concept. There are only a handful of proposals [2], [3], but their implementations did not adapt to the silicon variability. Failing to consider the uncorrelated sensitivities and noise characteristics between human biometrics and physical sensors leads to the high error rate in differentiating (same user, same challenge, different device) combinations. This issue is uniquely mitigated in our proposed UD PUF by using biohashing as a bridge to user biometric templates (face image) and device (CMOS image sensor) PUF challenge-response pairs without compromising the sensitivity of biometric data acquisition. After the biometric template is extracted, it will be re-projected onto a device-unique “PUF space”, which is specified by the random output of a silicon PUF embedded in the device, and used directly for matching in the quantized transformed domain. The process is transparent to the user and the system. It is more secure since the verification template is a function of both human biometric

and device response to an unknown challenge randomly issued by the server upon receiving the access request.

The rest of the paper is organized as follows. The concept of biohashing is introduced in Section II. The proposed biohashing based UD PUF, its operating principle and authentication scheme are elaborated in Section III. Section IV presents the experimental results and Section V concludes the paper.

II. AN OVERVIEW OF BIOHASHING

Biohashing was initially proposed as a biometric template protection technique. The key idea of biohashing is to transform the raw biometric feature onto a new random space, and store the transformed templates for later processing. Both the transformed templates and transformation parameters have to be stored. The transformation function has to be non-invertible, and the transformed results should preserve the original intra-class distance. Fig. 1 shows the general idea of a biohashing scheme. Its basic steps are simplified and described as follows [4], [5]:

- Apply feature extraction to the raw biometric data to obtain an m -bit feature vector y .
- Generate a pseudo-random matrix of size $m \times n$ using a user-specific token: $\{r_i \in \mathbb{R}^m | i = 1, 2, \dots, n\}$, where n is the length of the final biohash value.
- Apply Gram-Schmidt algorithm to transform the random matrix r into an orthonormal matrix $\{R_i \in \mathbb{R}^m | i = 1, 2, \dots, n\}$.
- Make a random projection of y with R via the inner product:

$$v = \langle y \cdot R \rangle = R^T y \quad (1)$$

- Digitize the projection result $\{v_i | i = 1, 2, \dots, n\}$ to obtain an n -bit biohash value $\{b_i | i = 1, 2, \dots, n\}$ by comparing v_i with a pre-defined threshold τ .

$$b_i = \begin{cases} 0 & \text{if } v_i \leq \tau \\ 1 & \text{if } v_i > \tau \end{cases} \quad (2)$$

Fig. 1. Concept of biohashing.

III. PROPOSED BIOHASHING BASED UD PUF

Existing biohashing schemes have their security drawbacks. The user-specific transformation matrix R has to be stored or deterministically hardcoded in order to project the raw biometric feature onto the same random space each time. However, the stored transformation matrix could be stolen or compromised. The transformed templates will be totally invertible once the attackers obtain the information of the stored secrets. Furthermore, existing biohashing schemes can only identify the user, but reveal nothing about the device identity. These two problems are addressed here by incorporating PUF into the existing biohashing schemes. PUF can be viewed as a unique “device feature” since it is derived from the inherent unpredictable and unclonable device mismatches due to process variations. More importantly, its response can only be evaluated upon stimulated by a challenge.

Among the biometric features (e.g., iris, fingerprint, face, voice, etc.), facial features are more practical and convenient for BYOD system since vision sensors have become increasingly ubiquitous and pervasive in modern IT devices. Face recognition has been intensively researched and its recognition rate has been improved tremendously in recent years. On the other hand, most IT devices have an integrated CMOS image sensor, which can be turned into a PUF for response generation upon queried, making it extremely difficult to replace or tamper a personal device without being detected. A biohash can thus be generated and validated by seamlessly integrating the user biometrics with the device signature.

A. Device Key Generation

The device key is generated using the CMOS image sensor based PUF we proposed in [6], where the random oracle is inherited from the fixed pattern noise (FPN) of CMOS image sensor. FPN is the random variations of output pixel voltage values of an image sensor, under uniform illumination or even in complete darkness. It is induced by the device and interconnect mismatches among the active pixel sensors as a consequence of imperfect manufacturing process variations [7]. A detailed description of CMOS image sensor based PUF is beyond the scope of this paper and the readers are referred to [6] for more information.

Fig. 2. Device key generation by CMOS image sensor PUF.

Fig. 2 shows the block diagram of device key generation scheme based on the CMOS image sensor PUF. When an verification request is sent, the device will receive a challenge from the system. The challenge is applied to initialize the linear feedback shift register (LFSR), and XORed with the user and device IDs to generate the true challenge C . Another “shadow challenge” C' is also generated by mixing the true challenge C with the LFSR output. The two internal challenges C and C' are decoded into pixel addresses to locate two pixels in the CMOS image sensor array. Two reset voltages, P_C and $P_{C'}$, are read and compared to retrieve a binary bit as the final response. In order to obtain a k -bit device key, the LFSR is clocked multiple times to generate k “shadow challenge” C' .

B. Facial Feature Extraction Algorithms

The main facial feature extraction approaches can be classified into two groups, namely Local Feature Description (LBD) and Holistic Subspace Analysis (HSA) [8]. Both groups have their pros and cons, and can achieve good performance under respective controlled conditions. LBD approaches enable the local features to be extracted from a single image, but usually have a large feature size; HSA is effective in dimensionality reduction but a large training set for subspace learning is usually required. Gabor filter and Local Binary Patterns (LBPs) are two representative LBD approaches, while Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) are well-known representatives of HSA. LDA has better performance in image classification, but it has small sample size problem, which is usually encountered in face recognition. Fortunately, PCA can perform better than LDA when the training set is small [9]. To achieve better recognition rate with limited sample size, we introduce a combined mechanism aggregating Gabor filter from LBD as well as PCA and LDA from HSA [10]–[12].

1) *Gabor filter*: Gabor filter is a powerful tool for local facial feature extraction, which is robust to illumination variations [13]. It looks for specific frequency content in specific directions around the point or region of analysis of an image. In the spatial domain, a 2D Gabor filter $\varphi_{\mu,\nu}(x,y)$ is a Gaussian kernel function modulated by a sinusoidal plane wave whose center frequency and orientation are given by f_μ and θ_ν , respectively [10], i.e.,

$$\varphi_{\mu,\nu}(x,y) = \frac{f_\mu^2}{\pi k \eta} e^{-((f_\mu^2/k^2)x'^2 + (f_\mu^2/\eta^2)y'^2)} e^{j2\pi f_\mu x'} \quad (3)$$

where $x' = x \cos \theta_\nu + y \sin \theta_\nu$, $y' = -x \sin \theta_\nu + y \cos \theta_\nu$, $f_\mu = f_{max}/2^{(\mu/2)}$, and $\theta_\nu = \nu\pi/8$.

To obtain the Gabor features, a set of gabor filters $\varphi_{\mu,\nu}(x,y)$ have to be constructed first, which typically have a size of five scales ($\mu = 0, 1, \dots, 4$) and eight orientations ($\nu = 0, 1, \dots, 7$) [10]. For a given face image $I(x,y)$, its Gabor feature corresponding to the parameter set (μ,ν) can be calculated by

$$G_{\mu,\nu}(x,y) = I(x,y) * \varphi_{\mu,\nu}(x,y) \quad (4)$$

where $G_{\mu,\nu}(x,y)$ is the complex filtering output, whose magnitude is used for face representation. However, the augmented Gabor (magnitude) features are usually very large. For example, a simple image of size 128×128 will result in a

$128 \times 128 \times 40 = 655360$ -bit feature vector after filtering with 40 Gabor filters. Therefore, it is combined with HSA to further reduce the feature dimensionality for effective data processing and storage.

2) *PCA*: PCA is one of the most common forms of dimensionality reduction methods widely used for feature extraction in face recognition. The basic idea of PCA is to find a new set of linearly uncorrelated variables, called the principal components, to account for as much variability in the original data as possible. By applying Karhunen-Loeve (KL) transform, the original set of possibly correlated data can be converted into those linearly independent principal components, which are arranged in a descending order. The dimensionality is reduced by keeping only the first few principal components of the transformed data.

PCA can be done using eigenvector decomposition of a data covariance matrix or single value decomposition (SVD) of a data matrix. Given a large dimension sample $X = x_1, x_2, \dots, x_n$ ($x_i \in \mathbb{R}^m$). The j -th principal component is the eigenvector μ_j , i.e., $\mu_j^T \mu_j = 1$, and the projection of the observation x_i on this dimension is $(x_i^T \mu_j) \mu_j$. Therefore, the cost function for removing this dimension is given by:

$$\begin{aligned} J_j &= \frac{1}{m} \sum_{i=1}^m (x_i^T \mu_j)^2 \\ &= \frac{1}{m} (x^T \mu_j)^2 \\ &= \frac{1}{m} (\mu_j^T x x^T \mu_j) \\ &= \mu_j^T S \mu_j \end{aligned} \quad (5)$$

where $S = \frac{1}{m} x x^T$.

To reduce t dimensions, we need to minimize the cost function

$$\begin{aligned} J &= \sum_{j=n-t}^n \mu_j^T S \mu_j \\ s.t. & \mu_j^T \mu_j = 1 \end{aligned} \quad (6)$$

which can be achieved by using Lagrangian multiplier. The PCA problem can then be transformed into the problem of solving the eigenvalues of S .

3) *LDA*: LDA is a supervised learning method. The main idea is to find a subspace of orthogonal features that best separates two or more classes of data. LDA is able to map a C -class sample data into an m -dimensional space ($m = C - 1$), where the between-class variation measured in scatter matrices S_b is maximized while the within-class variation measured in S_w is minimized to increase the recognition rate.

$$S_b = \sum_{c=1}^C N_c (\mu_c - \mu)(\mu_c - \mu)^T \quad (7)$$

$$S_w = \sum_{c=1}^C \sum_{i=1}^{N_c} (y_{ci} - \mu_c)(y_{ci} - \mu_c)^T \quad (8)$$

where μ and μ_c are the mean vectors of the overall sample data and class c , respectively, and y_{ci} is the i -th observation from N_c observations of class c .

LDA aims at finding a linear projection weight W to project the high-dimensional sample data y into a low-dimensional variable y' :

$$y' = W^T y \quad (9)$$

The optimum W can be found by maximizing the Fisher criterion function $J(w)$ as follows:

$$\begin{aligned} W &= \arg \max_W J(W) \\ &= \arg \max_W \frac{|W^T S_b W|}{|W^T S_w W|} \end{aligned} \quad (10)$$

C. UD PUF System Overview

Fig. 3 illustrates the use of the proposed biohashing-based UD PUF to verify a user request to access the system using his/her personal device. The device is equipped with a CMOS camera with a built-in CMOS image sensor PUF. The enrolment and verification protocol is described as follows:

Enrolment phase:

- An authorized user is allowed to register several devices for access to the server. For each (user, device) combination, a request ID will be created accordingly.
- Once the request ID is accepted by the system, a challenge will be issued. As illustrated in Fig. 2, the challenge will be applied to the device PUF to generate the corresponding device key, which will be transmitted to the server. For a particular (user, device) combination, multiple challenges can be generated during the enrolment phase.
- At the same time, The user is required to take several facial images using his/her device camera. The images are pre-processed to the pre-defined size and sent back to the system for feature extraction.
- Feature extraction algorithms (Gabor filter, PCA and LDA) are applied after collecting the face images of all the authorized users. The mean face, feature dimensionality and the transformation matrix W (the eigenfaces) are stored as the face model.
- The user-specific LDA feature vector and the unique device key are integrated using the biohashing technique. The LDA feature and the device key are deleted once the templates are obtained. The generated templates are stored in the system database in the form of (user, device, challenge, template) quadruple.

Verification phase:

- A user presents his/her request ID to seek access permission to the system using his/her device.
- If the request ID does not exist in the system, permission will be denied immediately. Otherwise, a challenge from the enrolled pool of this (user, device) combination will be sent to the device.
- A device key will be generated upon receiving the challenge, and sent back to the server along with the pre-processed face image.
- The received face image is used to extract the face feature according to the face model, and a new template can be obtained by applying the face feature and the device key to the biohash module.

- The enrolled template of this claimed identity will be retrieved from the template database, and will be compared with the obtained “live template”. Authentication is successful if the hamming distance between the two templates is within a pre-defined threshold.
- The above verification process can be conducted multiple times by sending different challenges to the device to reduce the false negatives caused by imperfect regeneration of face images or potential burst errors due to PUF response reliability and transmission problem.

IV. RESULTS AND DISCUSSIONS

A. Dataset and Experimental Setting

Although the user face images in practice are taken from their corresponding CMOS image sensors, for efficiency and impartiality, the experiments were conducted using two face databases widely used for benchmarking face recognition methods with multiple instances of the CMOS image sensor based PUF. Since the face images and the PUF responses are independently sent to the server for our proposed idea, the results of the simulation will not be biased by using of standard face databases. The ORL database [14] is used as the face images of authorized users, while the yale database [15] acts as the face images of imposters. The ORL database contains 400 male and female face images, with 10 (6 for training in the enrolment phase and 4 for testing in the verification phase) different posing individually for 40 distinct subjects. These grey scale images of size of 112×92 were taken in different times with variations in lighting, facial expression and facial details. The imposter's face images are extracted from the yale face database, which contains 15 subjects with 11 grayscale face images each. One image in the centerlight case of each subject was taken to form a group of 15 imposters. As for the device key extractor, 40 CMOS image sensor based PUF instances of size 64×64 are simulated to represent the authorized devices for each user. For 40 authorized users, the maximum number of LDA basis vectors are set to 39. In order to generate the 39-bit digitalized templates, the device key has to be 1521-bit (39×39). To be able to access every pixels in this sensor array, the challenge bit length is set to 12. Another 15 such PUF instances with the same setting are treated as the non-registered devices.

B. Biohash threshold definition

In the biohash scheme, the projected value v is binarized via a pre-defined threshold τ , which should be selected as the mean of the v distribution to have an equal probability of ‘1’ and ‘0’ bits. The PUF response has been demonstrated to have a near-ideal normal distribution [6]. Its orthonormal matrix is also normally distributed, which leads to an approximately normal distribution of the projected v . Therefore, the threshold τ is set to be zero in the proposed work. Fig. 4(a) shows the distribution of the PUF-oriented orthonormal projection matrix and Fig. 4(b) shows that the feature vector after biohashing has an approximately normal distribution with zero mean. Therefore, it is reasonable to set the biohash threshold to ‘0’.

Fig. 3. Verification scheme using the proposed biohashing based UD PUF.

Fig. 4. (a) Distribution of values of the orthonormal matrix R , (b) Distribution of values of the feature vector after BioHashing.

Fig. 5. (a) Inter-class and intra-class hamming distance distribution after biohashing. (b) The ROC curve of the proposed classifier.

C. Verification performance

The verification performance is tested using the authorized user (The ORL database) and device (The 40 genuine CMOS image sensor based PUF) group. The templates reproduced by the same (user, device) identity should be highly similar to the enrolled one, while the templates of different combinations from the registered pool should have large distinguishable variations from each other. Four “live templates” of each user can be obtained in the verification phase. Both the intra-class and inter-class hamming distance between the “live templates” and the “enrolled templates” are tested. Fig. 5 shows that the normalized inter-class hamming distances are clustered around 0.5 while the intra-class hamming distances tend to have smaller variations.

During the verification phase, the newly obtained templates will be compared with the claimed registered templates. A verification threshold is set to distinguish the authorized requests from malicious attempts. If the hamming distance between these two templates is smaller than the threshold, the verification is successful. Otherwise, it will be rejected. Verification performance is measured in equal error rate (EER), which is defined as the rate at which both acceptance and rejection errors are equal. EER values can be easily obtained from the receiver operating characteristic (ROC) curves. Fig. 5(b) shows the ROC curve of the proposed method. The curve is obtained by plotting the true accept rate (TAR) against the false accept rate (FAR) at verification threshold ranges from 0 to 1 at a step

of 0.05. The bigger the region covered by the ROC curve, the better the performance of the classifier. Fig. 5(b) shows the proposed method has a low EER of 0.032. It also suggests that the optimal threshold for verification should be set to be around 0.35, which coincides with the optimal threshold indicated in Fig. 5(a) that lies between 0.3 and 0.4.

D. UD-PUF discriminability

The discriminability of a UD-PUF describes its capability to detect changes made to any of the three entries of a particular (user, device, challenge) tuple. A good UD PUF should be sensitive to variability in silicon, user and challenge. For different (user, device, challenge) combinations, the UD-PUF should generate vastly different responses, which correspond to different templates in the proposed work. The following three cases are considered for testing the UD-PUF discriminability by changing one of the three entries, and keeping the other two unchanged.

1 (different user, same device, same challenge)

It is possible that an unauthorized person has stolen the registered device, and pretends to be the authorized user. The imposter’s images are extracted from the yale face database. The imposter database contains 15 face images of different subjects, which are pre-processed into the same format as the ORL database. In this case, each imposter is respectively paired with the device and

challenge of all the 40 enrolled users. Hence 600 test samples can be obtained in total.

2 (same user, different device, same challenge)

In this case, an authorized user attempts to gain access into the system with a non-registered device, whose device keys are simulated from another 15 CMOS image sensor PUF instances by applying the same challenge. These 15 untrusted device keys are used to replace the corresponding genuine device of each combination in the scheme. Hence 600 imposter templates can be obtained in the final stage.

3 (same user, same device, different challenge)

The template of each combination can also be influenced by the challenges, which provides an easy opportunity to erase the biometric feature and reconfigure the system. By replacing the challenge with a new one, the corresponding device key will be changed. Therefore, the biometric feature will be projected into a different random space, which leads to the refreshment of the stored templates. Similarly, 15 new challenges are iteratively applied as above in order to observe the statistical results of changes in challenge.

Fig. 6. Discriminability against: (a) Case 1: (Different user, same device, same challenge); (b) Case 2: (Same user, different device, different challenge); (c) Case 3: (Same user, same device, different challenge).

A common method to evaluate the discriminability is to compute the hamming distance between the obtained fake templates with the enrolled templates. For maximum discriminability, the ideal normalized hamming distance for each comparison should be 0.5. Fig. 6 shows the experimental results of the three abovementioned scenarios of tampering. Their hamming distances all float around the ideal value. By applying the threshold of 0.35 as analysed in Sec. IV-C, the false accept rate of a fake combination is only approximately 0.0183, 0.0217 and 0.030 for Case 1, Case 2 and Case 3 respectively with 600 test samples each. These results imply that the proposed work has good discriminability.

V. CONCLUSION

This paper presents a novel UD PUF scheme. The proposed UD PUF can authenticate both the user and the device by combining human biometrics (face image) and physical device PUF (CMOS image sensor) using bihashing technique. This is achieved by projecting the extracted biometric features onto a random device-specific PUF space. The proposed work provides higher security for BYOD regime since neither the raw biometric features nor the random projection space parameters have to be stored on device. Excellent template's reproducibility for genuine user-device pairs and discriminability against tampered user-device pairs can be achieved with the proposed method. A clear distinction between actual and manipulated (user, device, challenge) tuples is observed with a normalized hamming distance of around 0.5 for changes in any elements of the (user, device, challenge) tuple.

ACKNOWLEDGMENT

This research is supported by Singapore Ministry of Education AcRF Tier 1 Grant No. MOE 2014-T1-002-141 (RG186/14).

REFERENCES

- [1] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Magazine*, vol. 32, no. 5, pp. 88–100, Aug. 2015.
- [2] R. A. Scheel and A. Tyagi, "Characterizing composite user-device touchscreen physical unclonable functions (PUFs) for mobile device authentication," in *Proc. 5th Int. Workshop on Trustworthy Embedded Devices*, Denver, Colorado, USA, Oct. 2015, pp. 3–13.
- [3] Y. Guo and A. Tyagi, "Voice-based User-Device Physical Unclonable Functions for Mobile Device Authentication," *J. Hardware and Systems Security*, vol. 1, no. 1, pp. 18–37, May 2017.
- [4] Y. Liu and D. Hatzinakos, "Biohashing for human acoustic signature based on random projection," *Canadian J. Electrical and Computer Eng.*, vol. 38, no. 3, pp. 266–273, Summer 2015.
- [5] A. B. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, Jun. 2008.
- [6] Y. Cao, L. Zhang, S. S. Zalivaka, C. H. Chang, and S. Chen, "CMOS image sensor based physical unclonable function for coherent sensor-level authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 11, pp. 2629–2640, Nov. 2015.
- [7] H. Tian, B. Fowler, and A. E. Gamal, "Analysis of temporal noise in CMOS photodiode active pixel sensor," *IEEE J. Solid State Circuits*, vol. 36, no. 1, pp. 92–101, Jan. 2001.
- [8] Z. Chai, Z. Sun, H. Mendez-Vazquez, R. He, and T. Tan, "Gabor ordinal measures for face recognition," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 1, pp. 14–26, Jan. 2014.
- [9] A. M. Martínez and A. C. Kak, "PCA versus LDA," *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 23, no. 2, pp. 228–233, Feb. 2001.
- [10] V. Štruc and N. Pavešić, "The complete gabor-fisher classifier for robust face recognition," *EURASIP J. Advances in Signal Process.*, vol. 2010, p. 31, May 2010.
- [11] Vitomir Štruc and N. Pavešić, "Gabor-based kernel partial-least-squares discrimination features for face recognition," *Informatica (Vilnius)*, vol. 20, no. 1, p. 115138, Jan. 2009.
- [12] G. L. Marcialis and F. Roli, "Fusion of LDA and PCA for face verification," in *Proc. Int. Workshop on Biometric Authentication*, Copenhagen, Denmark, Jun. 2002, pp. 30–37.
- [13] S. Liao, A. K. Jain, and S. Z. Li, "Partial face recognition: Alignment-free approach," *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 35, no. 5, pp. 1193–1205, May 2013.
- [14] F. S. Samaria and A. C. Harter, "Parameterisation of a stochastic model for human face identification," in *Proc. 2nd IEEE Workshop on Appl. Computer Vision*, Sarasota, Florida, USA, Dec. 1994, pp. 138–142.
- [15] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection," *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 19, no. 7, pp. 711–720, Jul 1997.