Continuous biometric authentication using Possibilistic C-Means

Matheus Magalhães Batista dos Santos, Maurício Pamplona Segundo
Department of Computer Science, Federal University of Bahia
Salvador, Bahia, Brazil

***Abstract*—We propose a continuous biometric authentication framework that uses the Possibilistic C-Means (PCM) algorithm to guarantee that only authorized users can access a protected system. PCM is employed to cluster a history of biometric samples in two classes: genuine and impostor. The degree of membership of the current biometric sample to those classes is then used as a score, which is fused over time to reach a decision regarding the safety of the system. The main advantage of our approach is that it is training-free, and thus is applicable to any biometric feature that can be captured continuously without modification. We evaluated our system using 2D, 3D and NIR videos of faces and achieved results comparable to a training-based state-of-art work.**

***Index Terms*—Possibilistic C-Means, Fuzzy clustering, Biometrics, Continuous authentication**

I. Introduction

Traditional authentication methods like passwords and id cards are too risky in high security environments [1]–[3]. Many biometrics have been proposed to tackle this problem, but even in such systems the authentication process is performed only once and an unauthorized access could occur after the initial identity verification. Continuous authentication addresses this problem by verifying if the authorized person is using the protected resource during the entire access [4]. A typical example of application of continuous authentication is a subject using a computer. While the authorized person is using the computer, the system must grant access for the whole session. If the authorized person leaves the computer and another person starts using the computer, the system must detect the intrusion and deny access to the impostor.

Different biometrics features have been used for continuous authentication in the literature: keystrokes [5]–[7], electrocardiograms [8], faces [9]–[12], touchscreen interactions [13]–[15], fingerprints [4], [16] and multimodal features [4], [16], [17]. Each of them has advantages and disadvantages (*e.g.* fingerprints are more discriminant then faces, but are hard to be continuously captured), so most continuous authentication works mostly focus on the chosen biometric feature and not on the continuous evaluation itself. For this reason, they rely on precomputed biometric-specific models that depend on the databases used for training. As it is very hard to create a database that represents well all kinds of variations that may occur during a real access, it is common to have certain biases or assumptions in those works. Thus, a continuous authentication method should ideally be invariant to the biometric feature and should not require any kind of training.

In this work, as our main contribution, we propose and validate the use of the Possibilistic C-Means (PCM) algorithm [18] for continuous authentication. Continuous authentication systems can me modeled as a two-cluster problem, where one cluster represents the genuine user and the other one the impostor. Therefore, the PCM can be performed on a history of biometric observations to compute the degree of membership to each cluster, and these values can be fused over time to decide whether an access is still safe or not.

In our experiments, we use facial biometrics because it can be represented through different features: texture (2D images) [4], shape (3D images) [11] and infrared reflectance (near-infrared images (NIR)). Nowadays, all those facial features can be captured simultaneously using sensors like the Microsoft Kinect One[1] and the Intel RealSense[2]. Taking advantage of that, we were able to evaluate the performance of our training-free continuous authentication method on different biometric features in very similar acquisition conditions. This way, we eliminate user behavior during acquisition as a cause for atypical experimental results.

The remainder of this paper is organized as follows: Section II describes our PCM-based method for continuous authentication; Section III shows our experimental results; and Section IV presents our discussion and conclusions.

II. Continuous Face Authentication using PCM

Figure 1 presents a flowchart of our continuous authentication system. The initial three steps are commonly found in any kind of biometric system, continuous or not. They consist in digitally acquiring a biometric trait and preparing it for future matching. Depending on the chosen biometric, slightly different tasks are performed. For faces, it is necessary to determine the location of the face, eliminate unwanted variations (*e.g.* pose, illumination, expressions), and then extract a concise and discriminative set of features, which we call a biometric sample. Biometric samples are used for two distinct purposes: to identify the user during login, or to confirm the identity of a logged user during the continuous authentication. The sample used for login is saved as the user template (genuine medoid), and the following samples will form a history of observations. Both are later used by the PCM algorithm to compute the degree of membership of the current sample to two clusters:

[1]https://www.xbox.com/en-US/xbox-one/accessories/kinect
[2]https://software.intel.com/en-us/realsense

genuine and impostor. High membership values to the genuine cluster indicate that it is safe to maintain the access, while high membership values to the impostor cluster indicate that the current user should be logged off the system. Therefore, membership values are fused over time to aid the continuous process of classifying each instant as safe or unsafe, which will cease the access if necessary. More details are given in the following sections.

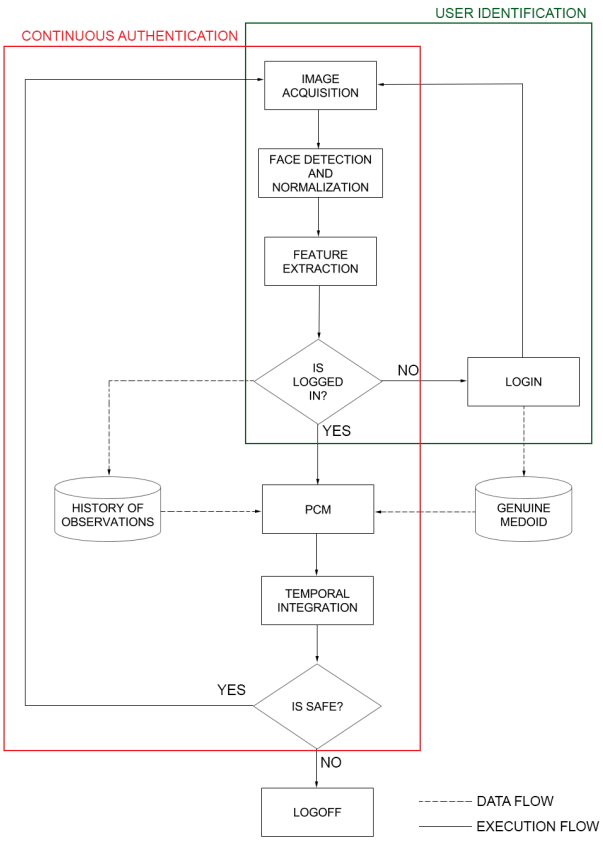


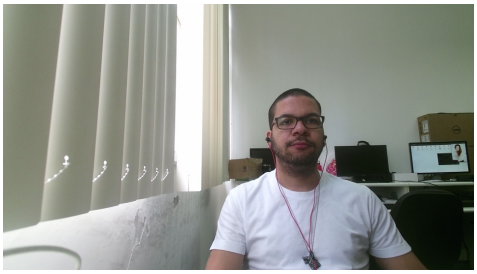
Fig. 1. Flowchart of our continuous authentication system.

A. Image Acquisition

Both Microsoft Kinect One and Intel RealSense sensors are able to capture 2D, 3D and NIR images simultaneously. Figure 2 illustrates one acquisition using the Kinect. Each of these images represent different facial properties that constitute different biometric features. Thus, both sensors would allow the evaluation of different biometrics in our continuous authentication system. We picked the Kinect because its images have better quality in comparison to the Realsense.

B. Face Detection and Normalization

For 2D and NIR images, we used a state-of-the-art face and landmark detector based on Multi-Task Convolutional Neural Networks (MTCNN) [19]. Although it was trained for 2D images only, it performs reasonably well for NIR images. The MTCNN finds the location of eye centers, nose tip and

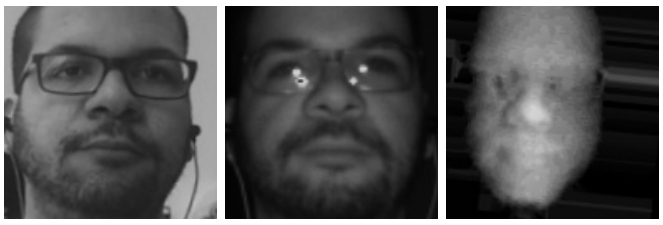


(a) 2D

(b) NIR (c) 3D

Fig. 2. Examples of face image acquisition using a single sensor to capture (a) color, (b) infrared and (c) depth information.

mouth corners for each face. With this information, detected faces are then rescaled to 128×128 pixels. Pose variations are corrected by the angle between eye centers, scale variations are reduced by enforcing the distance between eyes and mouth to 48 pixels, and translation variations are eased by setting the distance between eyes and the top border to 40 pixels [20]. 3D faces are detected by a cascade classifier of Haar-like features [21] and then aligned to an average face model for pose normalization [11]. Later, it is interpolated as a 128×128 image with scale similar to the other two modalities. Figure 3 shows the result of the normalization step for a face in all three modalities considered in this work.



(a) 2D (b) NIR (c) 3D

Fig. 3. Normalization result for faces in (a) color, (b) infrared and (c) depth images.

C. Feature Extraction

We extracted a feature vector with 256 values for each normalized image using a state-of-the-art Convolutional Neural Network (CNN) released by Wu *et al.* [20]. Originally trained for 2D images, Wu *et al.*'s CNN achieved good performance in NIR and 3D images in the literature [22], although it gets higher accuracy for modalities that are more consistent with its training. Equal Error Rates (EER) for 2D, NIR and 3D images

in controlled datasets were approximately 0.5%, 2% and 7%, respectively, in Dahia *et al.*'s work [22]. This difference in performance allowed us to analyze the impact of the feature discriminability in the continuous authentication process.

D. PCM-based Membership Value Estimation

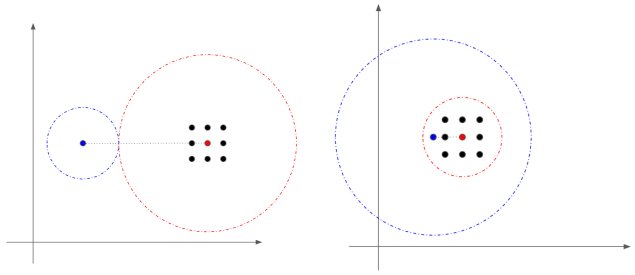
At the login step, one feature vector is stored as the user template, which will serve as the genuine medoid for the entire access. After the login, the last 10 faces are kept as the history of observations. The PCM algorithm is performed on this history and the degrees of membership to genuine and impostor clusters for the last observation are calculated. The PCM parameters utilized were fuzziness value of 1.5 and maximum number of iterations of 100. The fuzziness value of 1.5 is recommended by the authors of PCM, Krishnapuram and Keller, as the most adequate for their proposed membership function [23]. Due to the small number of observations kept, convergence is usually achieved in less than 5 iterations, so a maximum of 100 iterations is more than enough for our application. The centroid of genuine cluster is always the genuine medoid, since this is the only sample that is known to be genuine. The impostor centroid is initialized as the farthest observation from the genuine centroid and its final value is calculated by the PCM algorithm. The distance metric used to compare feature vectors is the cosine distance transformed to a range of $[0, 100]$, with 0 being the most similar and 100 being the least. As the history size and the feature vector are relatively small, the entire clustering process is very fast (*i.e.* runs thousands of times per second).

Ideally, when the genuine user is using the system, the last observation z_t should be close to the genuine centroid and consequently should have a high membership to the genuine cluster ($w_{t,genuine}$) and a low membership to the impostor cluster ($w_{t,impostor}$). On the other hand, when an impostor is using the system, the history will be composed of impostor samples only. Thus, z_t should be closer to the impostor centroid and have low $w_{t,genuine}$ and high $w_{t,impostor}$. However, when the genuine user is using the system, both centroids are very close to each other, causing $w_{t,impostor}$ to be high, too. To address this problem, we use the distance between the two centroids to infer the reliability of the system. If the two centroids are close, probably the genuine user is accessing the system. If they are far, probably the impostor is accessing it instead. Knowing that, the key to calculate meaningful membership values $w_{t,genuine}$ and $w_{t,impostor}$ is to establish good zones of influence $\eta_{genuine}$ and $\eta_{impostor}$ for PCM. The parameter η_j defines the distance in which the membership value of an observation to the cluster j becomes 0.5 [18]. We expect $\eta_{genuine}$ to be high and $\eta_{impostor}$ to be low when the centroids are close, easing the drops in $w_{t,genuine}$ caused by intraclass variations (*e.g.* pose variations and face expressions). When the centroids are far, $\eta_{genuine}$ is expected to be low and $\eta_{impostor}$ high. This reduces the chance of an impostor successfully impersonating the genuine user. The values of $\eta_{genuine}$ and $\eta_{impostor}$ are given by Equations 1 and 2:

$$\eta_{genuine} = max\_dist - dist(c_{genuine}, c_{impostor}) \quad (1)$$

$$\eta_{impostor} = dist(c_{genuine}, c_{impostor}) \quad (2)$$

where max_dist is the maximum distance of the distance metric (in this work, $max\_dist = 100$) and $dist(c_{genuine}, c_{impostor})$ is the distance between the two centroids. Figures 4(a) and 4(b) illustrate the idea behind Equations 1 and 2 in the Euclidean space. Figure 4(a) illustrates the case of distant centroids, in which $\eta_{genuine}$ is far lower than $\eta_{impostor}$. In Figure 4(b) the centroids are close, and $\eta_{genuine}$ is higher than $\eta_{impostor}$.



(a) (b)

Fig. 4. Illustration of (a) distant and (b) close centroids. Blue and red points are respectively genuine and impostor centroids. The blue dashed line represents the value of $\eta_{genuine}$, and the red one $\eta_{impostor}$.

Finally, the membership values are defined by Equations 3 and 4:

$$w_{t,genuine} = \frac{1}{1 + (\frac{dist(z_t, c_{genuine})^2}{\eta_{genuine}})^{\frac{1}{p-1}}} \quad (3)$$

$$w_{t,impostor} = \frac{1}{1 + (\frac{dist(z_t, c_{impostor})^2}{\eta_{impostor}})^{\frac{1}{p-1}}} \quad (4)$$

where p is the fuzziness value. With our centroid initialization and η_j estimation, we settled some of the some weaknesses of the PCM algorithm (*e.g.* coincident clusters and initialization dependency).

E. Temporal Integration

Temporal integration was originally proposed by Altinok and Turk [16] and later adapted by Sim *et al.* [4] and Pamplona Segundo *et al.* [11], the latter being the one employed in this work. At any time, the system uses Equation 5 to calculate the probability of being safe, called P_{safe}, given a history of score observations $Z_t = \{z_1, z_2, \ldots, z_t\}$ with $z_i = \{w_{i,genuine}, w_{i,impostor}\}$ and t being the time of the last observation:

$$P_{safe} = \frac{2^{\frac{-\Delta t}{k}} \times P(safe|\mathcal{Z}_t)}{P(safe|\mathcal{Z}_t) + P(unsafe|\mathcal{Z}_t)} \quad (5)$$

where k determines how fast P_{safe} drops in the absence of observations ($k = 15$ as in [11]) and Δt is the time passed

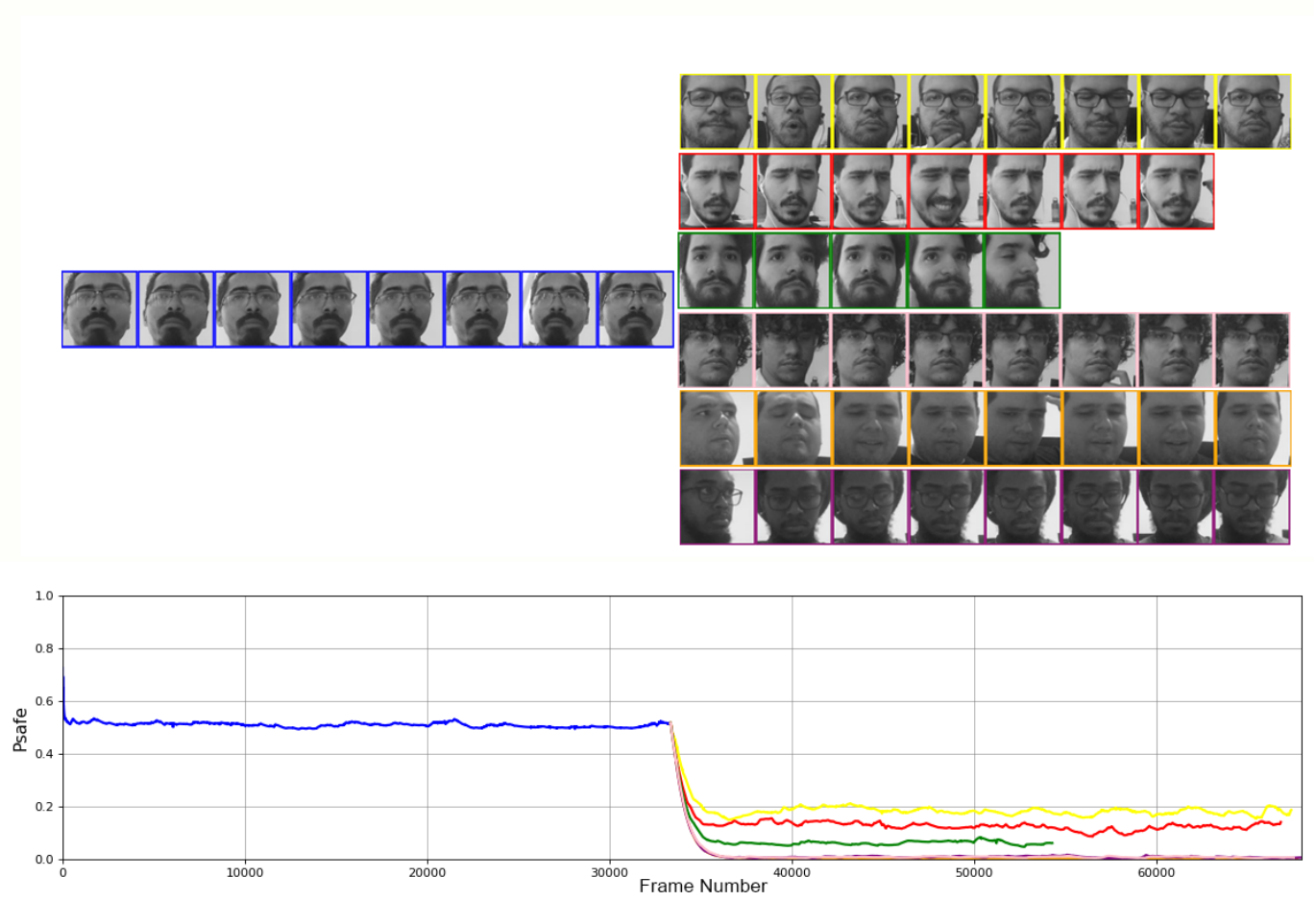


Fig. 5. Illustration of P_{safe} values along time. The blue line is the P_{safe} values when the allowed user was using the system. The other ones are when the intruders were using instead. The faces with blue contour represents examples of frames when the allowed user is using the system. The other ones belong to the intruders.

since the last observation z_t was obtained. $P(safe|\mathcal{Z}_t)$ and $P(unsafe|\mathcal{Z}_t)$ are given by Equations 6 and 7:

$$P(safe|\mathcal{Z}_t) \propto P(z_t|safe) + 2^{\frac{u-t}{k}} \times P(safe|\mathcal{Z}_u) \quad (6)$$

$$P(unsafe|\mathcal{Z}_t) \propto P(z_t|unsafe) + 2^{\frac{u-t}{k}} \times P(unsafe|\mathcal{Z}_u) \quad (7)$$

where u is the time of the penultimate observation. Finally, $P(z_i|safe)$ and $P(z_i|unsafe)$ are directly obtained from the membership values, as shown in Equations 8 and 9:

$$P(z_t|safe) \propto w_{t,genuine} \quad (8)$$

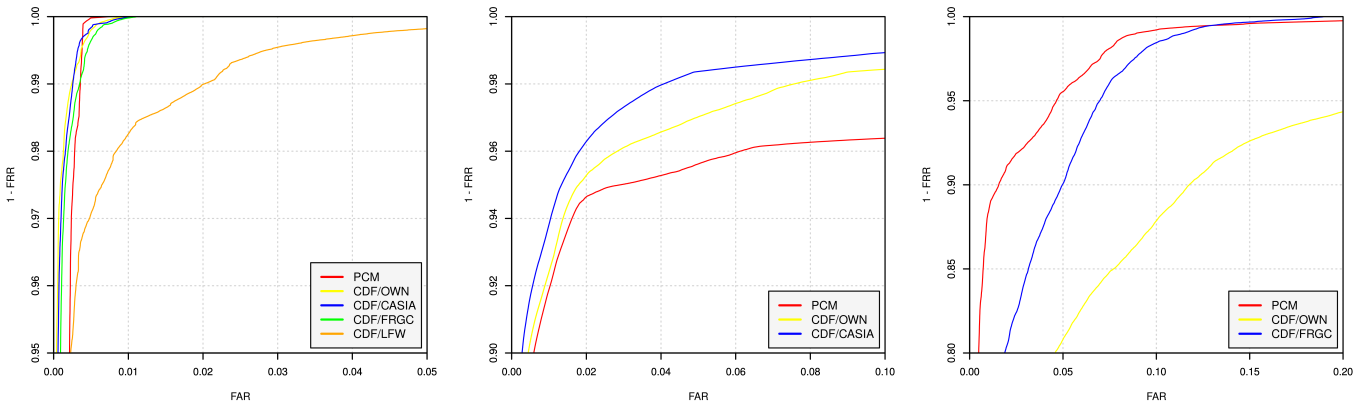
$$P(z_t|unsafe) \propto w_{t,impostor} \quad (9)$$

Equations 8 and 9 represent the main difference between this work and previous temporal integration versions [4], [11], [16]. While previous works rely on pretrained models for specific biometrics in order to estimate $P(z_t|safe)$ and $P(z_t|unsafe)$, our method requires only a small history of observations of the biometric feature in use. This reduces the effort to build a continuous authentication system as we do not need to process large amounts of data to precompute models or parameters. In addition, if the descriptor or biometric trait used for continuous authentication are changed, our work requires no modification.

III. Experiments

For the experiments, we recorded 7 videos from different users in 2D, 3D and NIR. The Kinect was positioned in between the computer screen and the table. Each video has an average duration of 40 minutes at a rate of 15 frames per second. As intraclass variations play a major role in continuous authentication, long videos of a few users are preferable over short videos of many users. In our case, users were asked to use a computer for at least 30 minutes, and no further instructions were provided.

As each video contains a single user, we concatenate every permutation of two videos to simulate several genuine accesses followed by an impostor takeover (*i.e.* 42 combined videos in



(a) (b) (c)

Fig. 6. ROC curves using PCM-based and CDF-based continuous authentication for (a) 2D, (b) NIR and (c) 3D modalities.

total), as illustrated in Figure 5. We compute the value of P_{safe} over time for each of the resulting videos in order to evaluate the accuracy of the continuous authentication. An example of a composite plot with the P_{safe} value over time using our approach is shown in Figure 5, in which a blue line represents the genuine access and each other color represents one of the possible takeovers. The bigger the gap between the blue line and other lines in the y-axis is, the higher the accuracy will get.

In order to assess the effectiveness of the proposed approach, we compare our results to Pamplona Segundo *et al.*'s method [11]. To this end, instead of using PCM to compute $P(z_i|safe)$ and $P(z_i|unsafe)$, we train cumulative distribution functions (CDF) for genuine and impostors using different databases. This is done by estimating the parameters μ_j and σ_j for the Equations 10 and 11:

$$P(z_t|safe) \propto \frac{1}{2}\left[1 + erf\left(\frac{s - \mu_{genuine}}{\sigma_{genuine}\sqrt{2}}\right)\right] \quad (10)$$

$$P(z_t|unsafe) \propto 1 - \frac{1}{2}\left[1 + erf\left(\frac{s - \mu_{impostor}}{\sigma_{impostor}\sqrt{2}}\right)\right] \quad (11)$$

where s is the cosine similarity between the last observation and the genuine medoid (user template). Given a training set, $\mu_{genuine}$ and $\sigma_{genuine}$ are the average and the standard deviation of cosine similarities for matchings between images of the same subject, and $\mu_{impostor}$ and $\sigma_{impostor}$ for matchings between images from different subjects.

Four databases were used to train CDFs. The first one is our own private collection containing 5565 images from 97 subjects acquired by a Realsense in 2D, 3D and NIR. The second one is the CASIA NIR-VIS 2.0 database [24], which contains 17,580 images from 725 subjects in 2D and NIR. The third one is the Face Recognition Grand Challenge (FRGC) database [25], with 4,950 registered 2D and 3D images of 556 subjects. The last one is the Labeled Faces in the Wild (LFW) database [26], with over 13,000 2D images from 1,680 subjects. These databases have different levels of intraclass and interclass variations and not necessarily represent the challenges of a continuous authentication scenario. Such variations result in different CDF parameters, as presented in Table I, that will later affect the recognition performance.

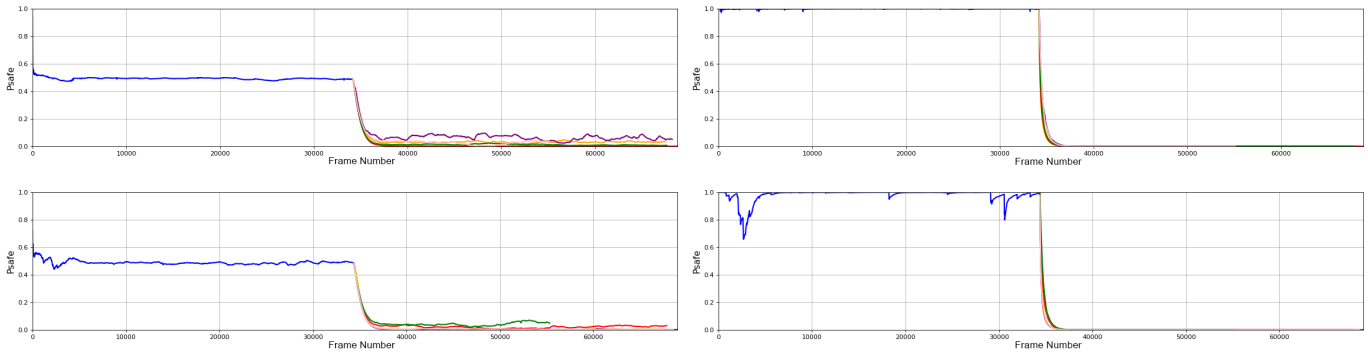
TABLE I
CDF PARAMETERS OBTAINED FROM DIFFERENT DATABASES TO BE USED IN PAMPLONA SEGUNDO ET AL.'S APPROACH [11].

Dataset	**Type**	$\mu_{genuine}$	$\sigma_{genuine}$	$\mu_{impostor}$	$\sigma_{impostor}$
OWN	2D	0.725852	0.126884	0.084115	0.113743
	3D	0.602357	0.152128	0.506733	0.135946
	NIR	0.721015	0.138441	0.216271	0.136031
CASIA	2D	0.908512	0.098547	0.091035	0.144248
	NIR	0.904982	0.122205	0.167486	0.148112
FRGC	2D	0.780994	0.108019	0.044956	0.106242
	3D	0.835823	0.100811	0.459365	0.135612
LFW	2D	0.626883	0.127443	0.009360	0.092923

For each of the considered modalities, we evaluated Pamplona Segundo *et al.*'s CDF-based approach [11] using all possible parameters from Table I and our PCM-based approach for all concatenated videos. The P_{safe} values for all videos in each of these tests were then compiled into a receiver operating characteristic (ROC) curve, and the results are shown in Figure 6. These curves show how good is the separation between genuine and impostor P_{safe} values. As may be observed, our results are comparable to the best results for 2D faces, are better for 3D and worse for NIR. Table II shows the EER for each of these curves to better illustrate the previous observation.

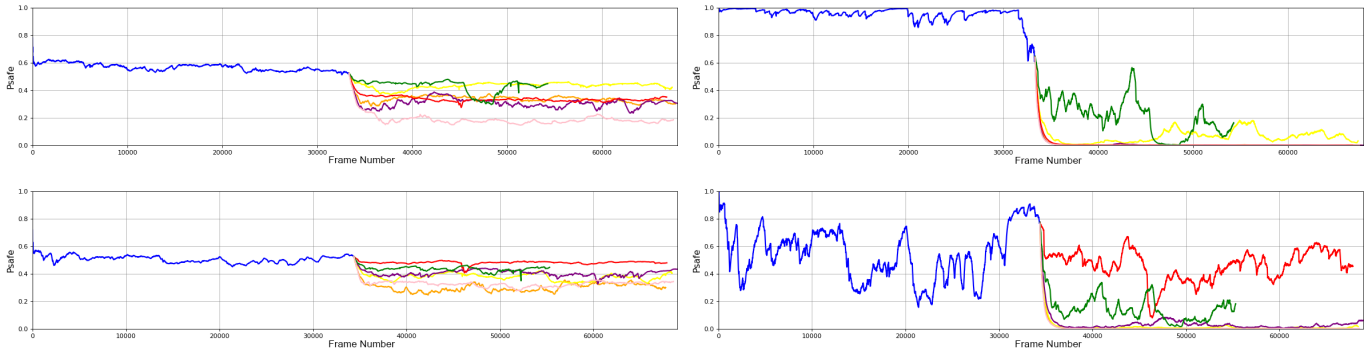
In order to understand these results, we created composite plots like the one presented in Figure 5 for all experiments reported in Figure 6 and Table II. Then we looked for anomalies that could explain this difference across modalities. As the acquisition was carried out simultaneously for the three modalities, variations in user behavior were automatically discarded as a possible cause.

Four composite plots for 2D faces illustrating the best and



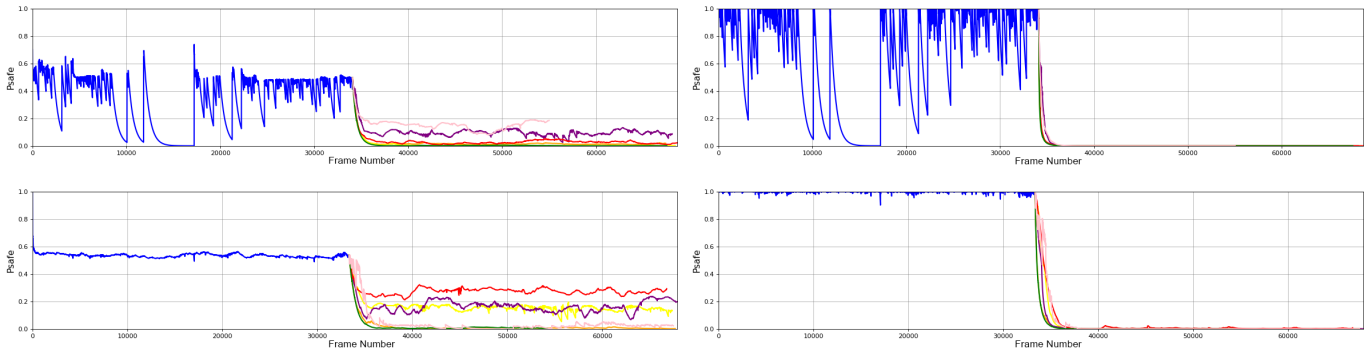
(a) (b)

Fig. 7. P_{safe} values along time for the (top) best and (bottom) worst testing case of (a) PCM and (b) CDF [11] when using 2D face images. The blue line shows the P_{safe} value while the genuine user is accessing the system, and each other color shows the changes in P_{safe} when one of the other users takes over the access as an impostor. CDF curves were obtained using CASIA/2D parameters (see Table I).



(a) (b)

Fig. 8. P_{safe} values along time for the (top) best and (bottom) worst testing case of (a) PCM and (b) CDF [11] when using 3D face images. CDF curves were obtained using FRGC/3D parameters (see Table I).



(a) (b)

Fig. 9. P_{safe} values along time for the (top) worst and (bottom) best testing case of (a) PCM and (b) CDF [11] when using NIR face images. CDF curves were obtained using CASIA/NIR parameters (see Table I).

the worst case scenarios for PCM and CDF are shown in Figure 7. For CDF, we picked the parameters with the best result in Table II. As Wu *et al.*'s CNN [20] was trained on 2D images, we expected to obtain this level of separation for both approaches. The major difference is that PCM does not take advantage of the entire range of P_{safe} values. This occurs because the membership degree to the impostor cluster is never close to zero (see Figure 4(b)), as we do not have a medoid for impostors like we have for genuine users. On the other hand, CDF has previous knowledge about both genuine and impostor classes and is able to better exploit the P_{safe} range. However, if the training is not performed on an adequate database, like LFW in Table II, the accuracy will be considerably affected.

Similar plots for 3D faces are presented in Figure 8. In this case, Wu *et al.*'s CNN [20] is not as discriminative, causing CDF to fail in maintaining P_{safe} values close to 1 for

TABLE II
EERS FOR CONTINUOUS AUTHENTICATION BASED ON 2D, 3D AND NIR FACIAL FEATURES USING OUR PCM-BASED APPROACH AND PAMPLONA SEGUNDO ET AL.'S CDF-BASED APPROACH [11].

Method	Training	2D	3D	NIR
PCM	-	0.00384	0.04763	0.04553
CDF	OWN	0.00401	0.11000	0.03607
CDF	CASIA	0.00357	-	0.02825
CDF	FRGC	0.00461	0.06343	-
CDF	LFW	0.01410	-	-

genuine accesses and 0 for impostors as we saw in Figure 7(b). Although the gap between genuine and impostor classes for 3D faces is not as large as for 2D faces, the P_{safe} behavior under PCM is much more stable across 2D and 3D when compared to CDF. Therefore, it ended up with the lowest EER in Table II. This indicates that our approach can be robust even when less discriminative features are considered, without any adjustment or tuning.

For NIR, PCM was not able to match or outperform CDF. As PCM is training-free, we anticipated that it might not achieve the best accuracy every time. However, in this specific case, we observed that another factor may have caused this low performance. As may be seen in Figure 9, in both methods we have a significant amount of drops in the P_{safe} value for a genuine user, which is explained by MTCNN failing to detect faces in NIR images (*i.e.* MTCNN was trained for 2D images). CDF has a better separation due to the preexisting training, so it is not as affected as PCM. In addition, PCM is completely based on a history of observations, so the absence of that definitely affects the performance. This is a limitation of our approach, as it is only comparable to other training-based methods when a constant feed of biometric samples is supplied.

IV. CONCLUSION

At the best of our knowledge, this is the first work to use PCM for continuous authentication purposes. We use PCM to clusterize a history of biometric samples in order to estimate the safety of the system, and by doing so we eliminate the need for a training stage. This is a major advantage, as it is very hard to create a training set that contains all kinds of variations that happen in a real access.

We analyzed the performance of our approach using three different biometric features: 2D, 3D and NIR face images. We achieved results better than the state-of-the-art for 3D faces, and comparable to the state-of-the-art for 2D faces. These results show that our approach is capable of handling biometric features with different discriminability levels. For NIR faces, we observed that PCM has problems when it is not possible to maintain a constant feed of biometric samples. In our case, this was caused by a faulty face detector. However, some biometric features are not continuous by nature, like voice, keystrokes and touchscreen interactions, and our PCM-based may not be the most appropriate approach for them. Still, we have other features that are even more suitable for our approach than faces, such as electrocardiograms, electroencephalograms and and other biomedical signals.

Despite the encouraging results, the proposed method can be improved. Ideally the value of P_{safe} should be close to 1 when the genuine user is accessing the system and close to 0 when an impostor takes over. The P_{safe} value currently resides right above 0.5, which means the degree of membership to the two clusters is nearly the same. This is due to the value of $\eta_{impostor}$ not being low enough. Thus, as a future work, we intend to investigate other training-free alternatives to compute membership values that expand interclass variations while maintaining the low intraclass variations obtained so far.

ACKNOWLEDGMENT

This research was funded in part by Fundação de Amparo à Pesquisa do Estado da Bahia (FAPESB), Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Universidade Federal da Bahia (UFBA) and Akyiama Soluções Tecnológicas. The Titan Xp used for this research was donated by the NVIDIA Corporation.

REFERENCES

[1] H. M. Wood, *The use of passwords for controlled access to computer resources*. US Department of Commerce, National Bureau of Standards, 1977, vol. 500, no. 9.

[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006.

[3] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[4] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 687–700, 2007.

[5] D. Gunetti and C. Picardi, "Keystroke analysis of free text," *ACM Transactions on Information and System Security*, vol. 8, no. 3, pp. 312–347, 2005.

[6] J. Leggett, G. Williams, M. Usnick, and M. Longnecker, "Dynamic identity verification via keystroke characteristics," *International Journal of Man-Machine Studies*, vol. 35, no. 6, pp. 859–870, 1991.

[7] J. V. Monaco, N. Bakelman, S.-H. Cha, and C. C. Tappert, "Developing a keystroke biometric system for continual authentication of computer users," in *European Intelligence and Security Informatics Conference*, 2012, pp. 210–216.

[8] F. Agrafioti and D. Hatzinakos, "Ecg biometric analysis in cardiac irregularity conditions," *Signal, Image and Video Processing*, vol. 3, no. 4, p. 329, 2009.

[9] R. Janakiraman, S. Kumar, S. Zhang, and T. Sim, "Using continuous face verification to improve desktop security," in *IEEE Workshops on Application of Computer Vision*, vol. 1, 2005, pp. 501–507.

[10] K. Niinuma, U. Park, and A. K. Jain, "Soft biometric traits for continuous user authentication," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 771–780, 2010.

[11] M. P. Segundo, S. Sarkar, D. Goldgof, L. Silva, and O. Bellon, "Continuous 3d face authentication using rgb-d cameras," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 64–69, 2013.

[12] D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, "Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data," in *International Conference on Biometrics*, 2015, pp. 135–142.

[13] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "Hmog: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2016.

[14] A. Roy, T. Halevi, and N. Memon, "An hmm-based behavior modeling approach for continuous mobile authentication," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2014, pp. 3789–3793.

[15] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," in *Sicherheit, Schutz und Zuverlässigkeit*, 2014, pp. 1–12.

[16] A. Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics," in *Workshop on Multimodal User Authentication*, 2003.

[17] I. G. Damousis, D. Tzovaras, and E. Bekiaris, "Unobtrusive multimodal biometric authentication: The humabio project concept," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 265767, 2008.

[18] R. Krishnapuram and J. M. Keller, "A possibilistic approach to clustering," *IEEE Transactions on Fuzzy Systems*, vol. 1, no. 2, pp. 98–110, 1993.

[19] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," *IEEE Signal Processing Letters*, vol. 23, no. 10, pp. 1499–1503, 2016.

[20] X. Wu, R. He, Z. Sun, and T. Tan, "A light cnn for deep face representation with noisy labels," *arXiv preprint arXiv:1511.02683*, 2015.

[21] M. P. Segundo, L. Silva, O. Bellon, and S. Sarkar, "Orthogonal projection images for 3d face detection," *Pattern Recognition Letters*, vol. 50, pp. 72–81, 2014, depth Image Analysis.

[22] G. Dahia, M. Santos, and M. Pamplona Segundo, "A study of cnn outside of training conditions," in *IEEE International Conference on Image Processing*, 2017.

[23] R. Krishnapuram and J. M. Keller, "The possibilistic c-means algorithm: insights and recommendations," *IEEE Transactions on Fuzzy Systems*, vol. 4, no. 3, pp. 385–393, 1996.

[24] S. Li, D. Yi, Z. Lei, and S. Liao, "The casia nir-vis 2.0 face database," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2013, pp. 348–353.

[25] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the face recognition grand challenge," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 1, 2005, pp. 947–954.

[26] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," University of Massachusetts, Amherst, Tech. Rep. 07-49, October 2007.