Advancing Active Authentication for User Privacy and Revocability with BioCapsules

Edwin Sanchez
edwsanch@iu.edu
Indiana University-Purdue University Indianapolis
Indianapolis, Indiana, USA

Anthony Weyer
antweyer@iu.edu
Indiana University-Purdue University Indianapolis
Indianapolis, Indiana, USA

Joseph Palackal
joppakool@gmail.com
Byram Hills High School
Armonk, New York, USA

Kai Wang
kwang@georgiasouthern.edu
Georgia Southern University
Statesboro, Georgia, USA

Tyler Phillips
tyler.phillips@alumni.iu.edu
Indiana University-Purdue University Indianapolis
Indianapolis, Indiana, USA

Xukai Zou
xzou@iupui.edu
Indiana University-Purdue University Indianapolis
Indianapolis, Indiana, USA

ABSTRACT

Biometric Facial Authentication has become a pervasive mode of authentication in recent years. With this surge in popularity, concerns over the security and privacy of biometrics-based systems have grown. Therefore, there is a need for a system that can address security and privacy issues while remaining user-friendly and practical. The BioCapsule scheme is a flexible solution that can be embedded in existing biometrics systems in order to provide robust security and privacy protections. While BioCapsules have been evaluated for their static face authentication capabilities, this paper extends the scheme to Active Authentication, where a user is continuously authenticated throughout a session. We use the MOBIO dataset, which contains video recordings of 150 individuals using mobile devices over several sessions, in order to evaluate the BioCapsule scheme within the domain of Active Authentication. We find that the BioCapsule scheme not only performs comparably to baseline, unsecured system performance, but in some cases exceeds baseline performance in terms of False Acceptance Rate, False Rejection Rate, and Equal Error Rate. Through our experiments, we demonstrate that the BioCapsule scheme is a powerful and practical addition to existing biometrics-based Active Authentication systems to provide robust security and privacy protections.

CCS CONCEPTS

• **Security and privacy** → **Privacy-preserving protocols**; *Database and storage security*; *Domain-specific security and privacy architectures.*

KEYWORDS

Continuous Authentication, Active Authentication, Deep Neural Networks, Face Authentication, Biometrics, Mobile Authentication

ACM Reference Format:
Edwin Sanchez, Anthony Weyer, Joseph Palackal, Kai Wang, Tyler Phillips, and Xukai Zou. 2023. Advancing Active Authentication for User Privacy and Revocability with BioCapsules. In *The Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), October 23–26, 2023, Washington, DC, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3565287.3617624

MobiHoc '23, October 23–26, 2023, Washington, DC, USA

ACM ISBN 978-1-4503-9926-5/23/10…$15.00
https://doi.org/10.1145/3565287.3617624

1 INTRODUCTION

In recent years, biometrics have proven to be a useful method of authenticating users [8]. The reasons are three-fold. Sensors capable of sampling biometrics are now in the hands of many users as mobile devices and come in the form of cameras, microphones, and touch screens. Biometric-based authentication is also user-friendly, as there is no burden on the user to remember a password or maintain a physical token on their person. And finally, the introduction and proliferation of Deep Learning has greatly enhanced the performance of biometric systems [22], [19], [4].

While the main hindrances to the use of biometrics have been addressed, new limitations have taken their place in the form of *user privacy* and *revocability*. As more user devices come with biometric sensors and most notably face identification and recognition software pre-installed, some users have begun to push back against these systems due to fears of societal implications [2], [13]. Another key issue is revocability. If biometric data is compromised, one cannot simply change their biometrics as they might in password-based or physical token-based systems, as biometrics are drawn from physiological and behavioral traits of an individual. This makes some biometric authentication schemes extremely rigid and a risk to implement as a primary authentication method [16]. These are the issues that state-of-the-art biometric authentication systems aim to resolve.

This paper aims to apply a privacy-preserving biometric authentication scheme, called the BioCapsule (BC) scheme [14], [15], to the domain of facial recognition and authentication. More specifically, we measure the performance of the scheme in the context

of Active Authentication (AA), or continuously authenticating the user throughout the user's active use of a resource during a session. This category of authentication provides increased security in comparison to single authentication at the beginning of a session, helping to defend against post-login attacks. This paper also works to identify how the BC scheme affects the feature embeddings of extracted facial features during the authentication process.

2 RELATED WORK

Much of the recent previous work done with regard to biometric authentication focuses on the two concerns of *privacy* and *revocability*. The main categories of state-of-the-art schemes that have emerged to deal with these issues have been Biometric Cryptosystems (BCS) and Cancelable Biometrics (CB). While these categories focus on securing biometrics in a more general sense, some other schemes have been developed that focus more specifically on AA.

2.1 Secure Biometric Schemes

BCS schemes generate keys from sampled biometrics [21], [12]. These generated keys can then be used to authenticate the user into the system. CB schemes attempt to apply a set of transformations to given biometric features in a secure manner [18]. However, BCS schemes are brittle, as small changes in the input biometrics result in large changes in the generated keys. This means BCS schemes require a stabilizing mechanism to be usable [21], [9]. CB schemes are susceptible to the same problems, while also often reducing system performance [21], [9]. The BC scheme [14], [15] is a CB method that has shown promise as it offers robust security and privacy benefits while minimally impacting system performace.

2.2 Active Authentication

Several schemes have been developed to handle multi-modal biometric authentication for AA. These systems may use a blend of multiple biometrics, such as face and voice recognition, as well as gyroscopic information or screen touch patterns [11], [3]. However, these schemes can put excessive strain on the device's battery due to the processing power needed. The demand of these schemes can be lessened by widening the time intervals between authentication checks. However, this comes with the risk of allowing for an attacker to access sensitive information in the event of a post-login attack.

In 2023, Keykhaie and Pierre [10] propose a face-based AA system using SIM/eSIM technology to protect biometric templates. Their proposed system uses a combination of modern deep learning face preprocessing and feature extraction models. To fit the biometric templates and authentication process onto the small footprint of a SIM card, their system performs a process called quantization. The preprocessing and feature extraction steps are done on the mobile device, with the authentication decision happening on the SIM card. However, quantizing the system's deep learning models has measurable negative effects on the performance of the system.

3 OVERVIEW OF BIOCAPSULE SCHEME

The BC scheme is designed to solve the issues of privacy and revocability, while also maintaining a simplistic and easy to implement structure that is provably secure [20], [14], [15]. The BC scheme is generic and can be embedded into existing facial authentication system. BC generation is broken down into 3 main steps, performed during enrollment and at authentication time: signature extraction, key generation, and secure fusion (shown in Fig. 1).

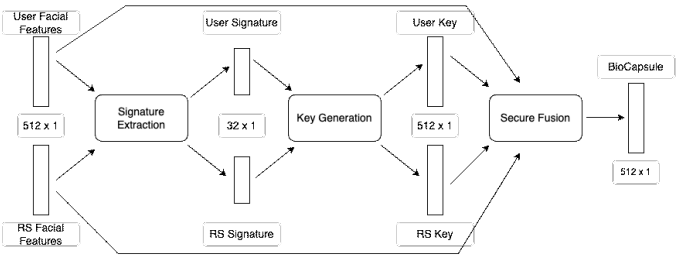

Figure 1: The BC generation process, fusing the biometrics of a user and their RS.

First, a feature vector is reshaped and averaged to produce a signature vector. Using this signature vector and a psuedo-random number generator (PRNG), a new vector is produced, of the same length as the original input feature vector. This new vector is binarized, resulting in a key vector consisting of 1s and -1s. This same process is applied to a selected Reference Subject (RS). The user's original feature vector is element-wise multiplied with the RS's key vector, and the user's key vector is element-wise multiplied with the RS's original feature vector. Finally, the two resultant vectors are element-wise added, generating a privacy-preserving BC. Later, if the generated BCs are compromised, the authentication system administrator can 'revoke' the compromised BCs. The impacted users' BCs conceal the users' true biometric traits from attackers. Later the users can re-enroll in the system using a new RS.

4 THE ACTIVE AUTHENTICATION SYSTEM

The AA begins once an authenticated user begins their session of device use. The system then captures an image from the device's camera. This image gets passed to the preprocessing step, which finds any faces in the image and generates a cropped frame for each detected face. If there are no detected faces, the process ends here and the system revokes the user. If multiple faces are detected, the center most face is selected. The cropped frame of the detected face is then passed to the feature extractor, which generates a feature vector representing the user's facial traits in Euclidean space. The next step is to generate a privacy-preserving BC if applicable, then pass the generated BC to a binary classifier. If the BC scheme is not used, then the unsecured feature vector is simply passed to a binary classifier. The binary classifier predicts the probability of whether the user should be authenticated and allowed continued access to the system. If the probability is above a certain threshold, then the authentication system waits idly for a set amount of time before repeating the full authentication process. If the classifier's predicted probability is below a certain threshold, the user is revoked from the system. Multiple authentication decisions during an open session can be combined, where probability of the last n authentication decisions are stored to aggregated for an overall authentication decision.

For enrollment, each subject is assigned a binary classifier that is trained to recognize their biometric feature vectors (or BCs). A

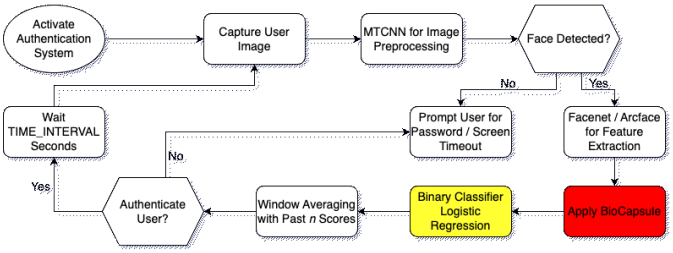

Figure 2: The Active Authentication system used for testing.

set of positive data is collected from the subject the classifier is trained for, along with samples from other subjects to be used as negative data. If the BC scheme is used, then a RS is passed through the preprocessing and feature extraction steps to create its own feature vector. With a subject's feature vector and a RS's feature vector, the BC generation process can be completed. These privacy preserving BCs are then used in place of unsecured feature vectors for the binary classifier training.

Since authentication decisions are based on a threshold, the enrollment process which trains the subjects' classifiers also tunes the threshold used for distinguishing between a true authentication and a false authentication. A fraction of the training data is used for threshold tuning, where the system aims to tune the threshold to maximize or minimize a certain target metric.

For testing purposes, users are not revoked following unsuccessful authentications. The probabilities and authentication decision are recorded. Testing also does not capture from an actual camera, and instead pulls from a preprocessed dataset for AA.

The following subsections describe the details of the AA system's preprocessing, feature extraction, BC generation, window averaging, and wait time steps.

4.1 Preprocessing

The preprocessing step is the first step in the AA process. Here, preprocessing refers to taking a raw input image and finding all of the faces that are in the image. At this stage the system is not concerned with the identity of the faces, only with finding all faces within a given image. The preprocessing step also detects key points with respect to all of the faces, finding both eyes, the nose, and the left and right corners of the mouth. The model used to perform preprocessing in the system is MTCNN [22]. The MTCNN github repository can be found at [17].

Since MTCNN will generate cropped faces for each face found in the image, we need to decide what to do when there's multiple faces or no faces at all. If there are no faces, the authentication process ends and the user is revoked. If there are multiple faces, the authentication system selects the center-most face, making the assumption that the user of the device is the most likely to be centered in the sampled image. A less strict system may wish to allow the user continued device access if no faces are detected, and a stricter system may wish to revoke the user if more than one face is detected.

4.2 Feature Extraction

The feature extraction process is the second step in the AA process. This step takes the input of the previous step, preprocessing, and generates feature vectors from the input images. These features can then be used for an authentication decision. The feature vectors generated should denote important features from the cropped face image given, with similar feature vectors generated for the same face, but dissimilar feature vectors generated for different faces. The feature extraction step uses one of two state-of-the-art face feature extraction models: FaceNet [19] and ArcFace [4]. An implementation of FaceNet can be found at [17]. An ArcFace implementation can be found at [7].

4.3 BioCapsule Generation

The next step in the process is to generate a BC, as described in the Section 3. If using the underlying, unsecured system, this step can be skipped. The feature vector generated from the feature extraction step can be directly passed to the binary classifier for either enrollment training or AA if the classifier is already trained. If the BC scheme is used, then a RS is needed to generate resulting BCs. As described in [20], [14], [15], a single RS can be used for all enrolled users, or a unique RS can be selected for each user. During testing, faces from the Labeled Faces in the Wild (LFW) [6] dataset are used as RSs.

4.4 Binary Classifier

The binary classifier used to generate authentication decisions is the next step in the process. During the enrollment process, the classifier is trained on feature vectors from the feature extraction process. If the BC scheme is used, then the classifier is trained on the generated BCs instead. Each subject's binary classifier is trained with both positive and negative samples. Positive samples refer to feature vectors or BCs generated for the positive subject. Negative samples refer to feature vectors or BCs generated from all other subject samples used in training, in a one-vs-all strategy. Also during enrollment, a fraction of the samples are used for threshold tuning. Threshold tuning determines a threshold that maximizes or minimizes the system's performance with respect to the samples given, targeting a performance metric.

4.5 Authentication Decision

The final step in the AA process is the authentication decision, using the tuned threshold. A trained binary classifier is given a feature vector (or BC) corresponding to a user that must be authenticated. The classifier outputs a probability that the user should be authenticated. If the predicted probability is less than the threshold value, the user is unsuccessfully authenticated and revoked. If the probability is above the threshold, then the user has been successfully authenticated and allowed continued access to the device. This process is repeated during the open session to confirm the originally authenticated user is still the person accessing the system. The overall AA authentication process goes unnoticed by the user during their session unless they are revoked.

Figure 3: Sample images of subjects from the MOBIO dataset [11].

5 EXPERIMENT

The following subsections describe our experiment details and the results found during testing. The experiment aims to answer the following questions: (1) does the underlying, unsecured system perform reasonably during AA and (2) does the BC-embedded system perform comparably during AA. Code for replicating this experiment can be found at [5].

5.1 The MOBIO Dataset

The MOBIO dataset [11] is designed for AA experiments. The dataset includes videos of 150 different subjects over a 2-year time span. The videos were taken in 5 different countries and 6 different locations in total. The devices used in this dataset for recording were a 2008 MacBook and a Nokia phone. There were 12 sessions recorded in total. The first session was recorded on both laptop and phone. The remaining 11 sessions were recorded on phone only. Each session has 21 videos, where a subject speaks directly into the camera of the mobile device or laptop, reading from a prompt given to the subject. The tests in this paper ignore the audio data and focus solely on the videos.

We attempt to mimic the experimental setup in [10] which also relies on the MOBIO dataset. The first session of each subject is reserved for training each subject's respective binary classifier. The remaining sessions are used for testing. To run a test on a single subject, the single subject's sessions are regarded as positive samples, while the remaining subjects' sessions are used as negative samples. Testing was done with two different settings with respect to the MOBIO dataset: single platform and cross platform. Single platform refers to training on samples extracted from the same device as testing is run on. This simulates the scenario where the classifier is trained using the same camera that is used during AA. Cross platform refers to training on samples extracted using a different camera during training than the camera used during testing. This simulates the scenario where a user's data is sampled for training the system using a different camera than what the user would normally use for AA.

Subjects *f-210* and *f-218* were removed due to an insufficient number of sessions. The former has only the laptop session, while the latter has all sessions but the laptop session.

5.2 Metrics

The metrics used for testing are False Acceptance Rate (FAR) (Eq. 1), False Rejection Rate (FRR) (Eq. 2), and Equal Error Rate (EER). FAR is a ratio measuring the number of false positives (a person passes the authentication check who should not have) that were let in by the system with respect to the total number of negative samples tested. FRR is a ratio measuring the number of false negatives (a person who does not pass the authentication check but should have) that the system failed to let in with respect to the total number of positive samples tested. The EER represents where these two metrics are equal in a system. This can be found by generating the probabilities for a set of data samples, then sliding the threshold to where these two rates are equal.

Model Type	BC	RS	Platform	FAR (%)	FRR (%)	EER (Test) (%)
ArcFace	No BC	N/A	Single	0.419	0.873	0.010
			Cross	0.527	0.865	0.020
	BC	Single	Single	0.440	0.892	0.021
			Cross	**0.361**	0.920	0.031
		Multi	Single	0.458	**0.854**	**0.007**
			Cross	0.587	0.862	0.013
FaceNet	No BC	N/A	Single	0.393	6.349	0.863
			Cross	0.396	9.521	1.332
	BC	Single	Single	**0.365**	13.106	1.960
			Cross	0.423	17.902	2.549
		Multi	Single	0.488	**1.140**	**0.086**
			Cross	0.532	1.715	0.180

Table 1: The performance of the system with different settings, where each score represents the mean performance of the system averaged across all subjects in MOBIO.

$$FAR(\%) = (FP/(FP + TN)) * 100 \quad (1)$$

$$FRR(\%) = (FN/(FN + TP)) * 100 \quad (2)$$

5.3 Results

Table 1 shows the performance of the system with and without the BC scheme applied, as well as with different feature extraction models, RS settings, and single vs. cross platform training and testing. Across the board, cross platform EER performance is worse when compared to their single platform counterparts. This can be attributed to the classifier fitting to the camera's image quality on one device during training, and then under-performing when being showed samples from another camera's images. When comparing *No BC* settings to *BC with Single RS*, we see slight performance degradation, although still comparable performance. The degradation can be attributed to the BC process losing some information when the fusion process happens, as the BC scheme sacrifices some underlying system performance in exchange for securing the system. Additionally, with *Single RS*, the transformations applied to the user's features are the same for all users, resulting in lower inter-class separation as the RS features are weighted equally with each user's [20]. Table 2 shows the performance of the system when compared to the SIM card based systems (CA-MMOC & F-MMOC) designed in [10], which once again validate the comparable performance and solidness of the BC technique.

Surprisingly we see that the performance of systems set with *Multi RS* outperform both *Single RS* systems and the *No BC* underlying systems. This, again, can be attributed to BC's fusion process. While using a *Single RS* has the effect of reducing inter-class variation by fusing every subject with the same RS, *Multi RS* has the opposite affect as each new RS applies different transformations on the user's feature vector, increasing inter-class variation. In data with initially low inter-class variation, the BC scheme can increase inter-class variation by selecting diverse RSs for each user, as the variation in RSs will be reflected in the output BC. Figure 4 demonstrates this phenomenon with images of similar looking people

Site	Architecture	BC Type	Alg.	Single Platform	Cross Platform
BUT	CA-MMOC	No BC	L-SVM	0.1 (0.4)	0.2 (0.4)
			LDA	0.3 (0.4)	3.5 (3.1)
			LR	0.1 (0.4)	0.2 (0.4)
	F-MMOC		L1	0.1 (0.2)	0.1 (0.2)
			L2	0.1 (0.1)	0.1 (0.1)
	D-CSLDA		L_inf	0.8 (1.6)	0.9 (1.0)
			CSLDA	13.5 (4.2)	21.9 (5.2)
	ArcFace	Single RS-BC	LR	0.0 (0.0)	0.0 (0.0)
		Multi RS-BC		0.0 (0.0)	0.0 (0.0)
	FaceNet	Single RS-BC		1.6 (1.4)	2.3 (2.3)
		Multi RS-BC		0.1 (0.8)	0.2 (0.7)
IDIAP	CA-MMOC	No BC	L-SVM	0.0 (0.0)	0.5 (0.8)
			LDA	0.2 (0.2)	11.5 (12.3)
			LR	0.0 (0.0)	0.3 (0.4)
	F-MMOC		L1	0.1 (0.1)	2.6 (9.1)
			L2	0.1 (0.1)	2.4 (8.9)
	D-CSLDA		L_inf	0.2 (0.1)	2.8 (2.1)
			CSLDA	12.8 (6.2)	27.1 (10.2)
	ArcFace	Single RS-BC	LR	0.0 (0.0)	0.0 (0.0)
		Multi RS-BC		0.0 (0.0)	0.0 (0.0)
	FaceNet	Single RS-BC		1.2 (1.7)	1.8 (2.7)
		Multi RS-BC		0.0 (0.0)	0.0 (0.1)
LIA	CA-MMOC	No BC	L-SVM	1.4 (4.2)	1.5 (3.2)
			LDA	1.6 (3.0)	2.1 (3.2)
			LR	1.4 (3.8)	1.5 (3.0)
	F-MMOC		L1	1.2 (2.5)	1.3 (2.3)
			L2	1.1 (3.0)	1.2 (2.9)
	D-CSLDA		L_inf	1.3 (2.6)	1.4 (2.6)
			CSLDA	19.1 (8.2)	24.7 (8.7)
	ArcFace	Single RS-BC	LR	0.1 (0.3)	0.1 (0.5)
		Multi RS-BC		0.0 (0.2)	0.1 (0.2)
	FaceNet	Single RS-BC		2.7 (3.2)	2.5 (2.3)
		Multi RS-BC		0.1 (0.3)	0.1 (0.4)
UMAN	CA-MMOC	No BC	L-SVM	0.1 (0.1)	1.1 (0.2)
			LDA	0.4 (0.4)	3.0 (2.7)
			LR	0.1 (0.1)	0.1 (0.2)
	F-MMOC		L1	0.1 (0.2)	0.1 (0.1)
			L2	0.1 (0.1)	0.1 (0.1)
	D-CSLDA		L_inf	0.7 (1.3)	1.1 (1.1)
			CSLDA	16.1 (4.6)	23.1 (10.2)
	ArcFace	Single RS-BC	LR	0.0 (0.1)	0.0 (0.0)
		Multi RS-BC		0.0 (0.0)	0.0 (0.0)
	FaceNet	Single RS-BC		2.6 (4.4)	3.6 (6.6)
		Multi RS-BC		0.2 (0.6)	0.4 (1.8)
UNIS	CA-MMOC	No BC	L-SVM	0.1 (0.2)	0.1 (0.2)
			LDA	0.4 (0.4)	0.3 (0.4)
			LR	0.1 (0.2)	0.1 (0.2)
	F-MMOC		L1	0.3 (0.3)	0.5 (0.8)
			L2	0.2 (0.2)	0.4 (0.7)
	D-CSLDA		L_inf	0.7 (1.1)	1.0 (1.1)
			CSLDA	15.1 (7.1)	21.0 (8.4)
	ArcFace	Single RS-BC	LR	0.0 (0.0)	0.0 (0.0)
		Multi RS-BC		0.0 (0.0)	0.0 (0.0)
	FaceNet	Single RS-BC		1.6 (3.2)	1.7 (2.8)
		Multi RS-BC		0.0 (0.1)	0.1 (0.3)
UOULU	CA-MMOC	No BC	L-SVM	0.1 (0.1)	0.8 (0.6)
			LDA	0.6 (0.4)	9.3 (6.5)
			LR	0.1 (0.1)	0.5 (0.9)
	F-MMOC		L1	0.2 (0.1)	7.3 (11.1)
			L2	0.1 (0.1)	6.8 (13.1)
	D-CSLDA		L_inf	0.5 (0.6)	7.1 (10.8)
			CSLDA	22.5 (9.2)	31.1 (11.5)
	ArcFace	Single RS-BC	LR	0.0 (0.5)	0.0 (0.1)
		Multi RS-BC		0.0 (0.1)	0.0 (0.1)
	FaceNet	Single RS-BC		2.2 (2.6)	3.9 (4.3)
		Multi RS-BC		0.1 (0.3)	0.3 (0.5)

Table 2: The performance of the systems designed in [10] compared to ours (BioCapsule schemes, highlighted green).

from the VGG2 dataset [1]. Figure 4 also shows that BC reduces the intra-class variation of the generated feature vectors compared to the original feature vectors. This again is due to the RS applying a constant transformation on the input feature vectors, smoothing out high variation in input images.

When comparing the baseline feature vectors (the top two graphs of figure 4) with both feature vectors generated using BC with both *Single* and *Multi RS* (the bottom four graphs), we see that the clusters for each person end up in a new location in the space, implying that BC performed a spacial transformation on the features, as expected.

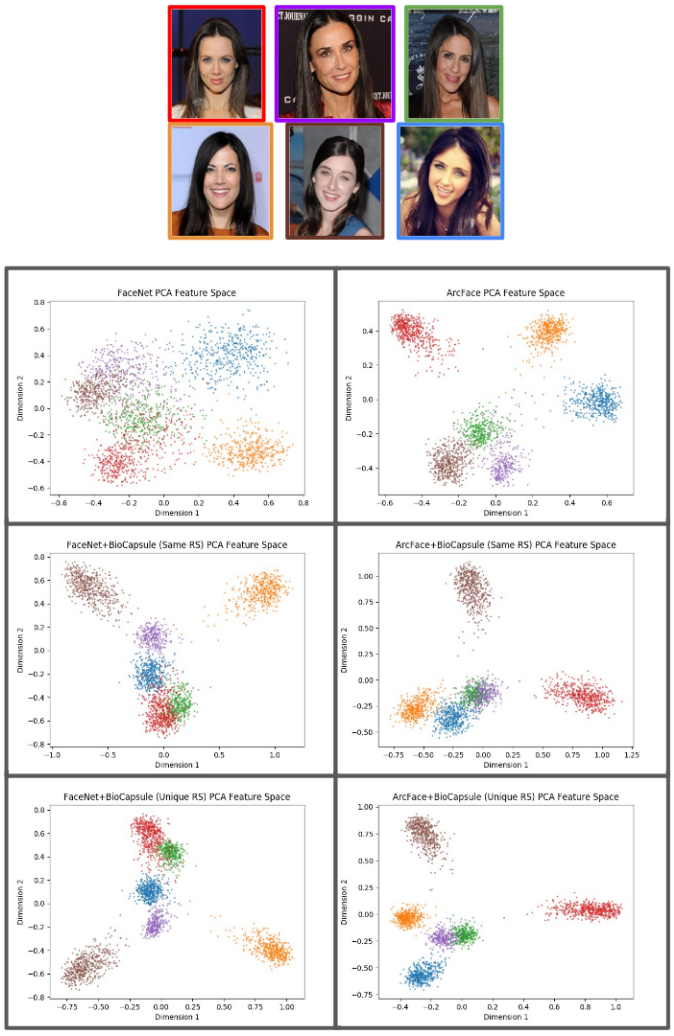

Figure 4: Visualization of feature vectors generated from face images sampled from the VGGFace2 dataset [1].

However, we can also see the clusters tighten when BC is applied in both the *Single* and *Multi RS* variations (lower intra-class variation). We can further see that *Multi RS* further separates clusters (higher inter-class variation) while *Single RS* brings them closer together (lower inter-class variation).

6 CONCLUSION

Biometrics has grown to play an important role in user authentication in recent years, due to the rise of mobile devices. With this, there is a need for better security around these mobile devices. AA is one way to provide a stronger layer of security. While this works well on its own, AA using biometrics does not address the privacy concerns of today's users, nor does it deal with the problem of template revocability that hinders the proliferation of biometric authentication.

The BC scheme can solve these issues, while remaining secure and preserving the representational power of the underlying system.

Our tests find that the BC scheme can be applied to face-based AA systems and can perform comparably to these systems, while providing more security benefits for the system and users.

7 ACKNOWLEDGEMENTS

Our reseach was made possible by the support of IUPUI's REU program, funded by the National Science Foundation (NSF) through grant CNS-1852105.

REFERENCES

[1] Qiong Cao, Li Shen, Weidi Xie, Omkar M. Parkhi, and Andrew Zisserman. 2017. VGGFace2: A dataset for recognising faces across pose and age. *CoRR* abs/1710.08092 (2017). arXiv:1710.08092 http://arxiv.org/abs/1710.08092

[2] JV Chamary. 2017. No, Apple's face ID is not a "secure password". https://www.forbes.com/sites/jvchamary/2017/09/18/security-apple-face-id-iphone-x/

[3] David Crouse, Hu Han, Deepak Chandra, Brandon Barbello, and Anil K. Jain. 2015. Continuous authentication of mobile user: Fusion of face image and inertial Measurement Unit data. In *2015 International Conference on Biometrics (ICB)*. 135–142. https://doi.org/10.1109/ICB.2015.7139043

[4] Jiankang Deng, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. 2019. ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*.

[5] T. Phillips E. Sanchez. [n. d.]. BioCapsule Active Authentication Github Repository. *https://github.com/Edwin-Sanchez2003/BioCapsule* ([n. d.]).

[6] Gary B. Huang, Manu Ramesh, Tamara Berg, and Erik Learned-Miller. 2007. *Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments.* Technical Report. University of Massachusetts, Amherst.

[7] Deep Insight. 2019. *Face Analysis Project using MXNET Repository.* Available at: https://github.com/deepinsight/insightface.

[8] A.K. Jain, A. Ross, and S. Prabhakar. 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* (2004), 4–20. https://doi.org/10.1109/TCSVT.2003.818349

[9] Ganiyev Salim Karimovich and Khudoykulov Zarif Turakulovich. 2016. Biometric cryptosystems: Open issues and challenges. In *ICISCT*. 1–3. https://doi.org/10.1109/ICISCT.2016.7777408

[10] Sepehr Keykhaie and Samuel Pierre. 2021. Lightweight and secure face-based active authentication for mobile users. *IEEE Transactions on Mobile Computing* (2021).

[11] Elie Khoury, Laurent El Shafey, Christopher McCool, Manuel Günther, and Sébastien Marcel. 2014. Bi-modal biometric authentication on mobile phones in challenging conditions. *Image and Vision Computing* (2014), 1147–1160. https://doi.org/10.1016/j.imavis.2013.10.001

[12] Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, and Dimitris Hatzinakos. 2009. Face recognition with biometric encryption for privacy-enhancing self-exclusion. In *2009 16th International Conference on Digital Signal Processing*. 1–8. https://doi.org/10.1109/ICDSP.2009.5201257

[13] Paul Mozur. 2018. Inside China's dystopian dreams: A.I., shame and lots of cameras. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

[14] Tyler Phillips, Xiaoyuan Yu, Brandon Haakenson, Shreya Goyal, Xukai Zou, Saptarshi Purkayastha, and Huanmei Wu. 2020. AuthN-AuthZ: Integrated, User-Friendly and Privacy-Preserving Authentication and Authorization. In *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. 189–198. https://doi.org/10.1109/TPS-ISA50397.2020.00034

[15] Tyler Phillips, Xukai Zou, Feng Li, and Ninghui Li. 2019. Enhancing Biometric-Capsule-Based Authentication and Facial Recognition via Deep Learning. In *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies* (Toronto ON, Canada) *(SACMAT '19)*. Association for Computing Machinery, New York, NY, USA, 141–146. https://doi.org/10.1145/3322431.3325417

[16] S. Prabhakar, S. Pankanti, and A.K. Jain. 2003. Biometric recognition: security and privacy concerns. *IEEE Security Privacy* (2003), 33–42. https://doi.org/10.1109/MSECP.2003.1193209

[17] D. Sandberg. 2015. *FaceNet and MTCNN Github Repository.* Available at: https://github.com/davidsandberg/facenet.

[18] M. Savvides, B.V.K. Vijaya Kumar, and P.K. Khosla. 2004. Cancelable biometric filters for face recognition. In *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.* 922–925 Vol.3. https://doi.org/10.1109/ICPR.2004.1334679

[19] Florian Schroff, Dmitry Kalenichenko, and James Philbin. 2015. FaceNet: A Unified Embedding for Face Recognition and Clustering. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

[20] Yan Sui, Xukai Zou, Eliza Y. Du, and Feng Li. 2014. Design and Analysis of a Highly User-Friendly, Secure, Privacy-Preserving, and Revocable Authentication Method. *IEEE Trans. Comput.* (2014), 902–916. https://doi.org/10.1109/TC.2013.25

[21] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain. 2004. Biometric cryptosystems: issues and challenges. *Proc. IEEE* (2004), 948–960. https://doi.org/10.1109/JPROC.2004.827372

[22] Kaipeng Zhang, Zhanpeng Zhang, Zhifeng Li, and Yu Qiao. 2016. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. *IEEE Signal Processing Letters* (2016), 1499–1503. https://doi.org/10.1109/LSP.2016.2603342