Enhancing Biometric-Capsule-based Authentication and Facial Recognition via Deep Learning

Tyler Phillips
Indiana University-Purdue University Indianapolis
Department of Computer and Information Science
phillity@iupui.edu

Xukai Zou
Indiana University-Purdue University Indianapolis
Department of Computer and Information Science
xzou@iupui.edu

Feng Li
Indiana University-Purdue University Indianapolis
Department of Computer and Information Technology
fengli@iupui.edu

Ninghui Li
Purdue University
Department of Computer Science
ninghui@cs.purdue.edu

ABSTRACT

In recent years, developers have used the proliferation of biometric sensors in smart devices, along with recent advances in deep learning, to implement an array of biometrics-based authentication systems. Though these systems demonstrate remarkable performance and have seen wide acceptance, they present unique and pressing security and privacy concerns. One proposed method which addresses these concerns is the elegant, fusion-based BioCapsule method. The BioCapsule method is provably secure, privacy-preserving, cancellable and flexible in its secure feature fusion design. In this work, we extend BioCapsule to face-based recognition. Moreover, we incorporate state-of-art deep learning techniques into a BioCapsule-based facial authentication system to further enhance secure recognition accuracy. We compare the performance of an underlying recognition system to the performance of the BioCapsule-embedded system in order to demonstrate the minimal effects of the BioCapsule scheme on underlying system performance. We also demonstrate that the BioCapsule scheme outperforms or performs as well as many other proposed secure biometric techniques.

CCS CONCEPTS

• **Security and privacy → Biometrics**; **Privacy-preserving protocols**.

KEYWORDS

Biometrics, Privacy, Authentication, Deep Learning, BioCapsule

ACM Reference Format:
Tyler Phillips, Xukai Zou, Feng Li, and Ninghui Li. 2019. Enhancing Biometric-Capsule-based Authentication and Facial Recognition via Deep Learning. In *The 24th ACM Symposium on Access Control Models and Technologies (SACMAT '19), June 3–6, 2019, Toronto, ON, Canada.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3322431.3325417

SACMAT '19, June 3–6, 2019, Toronto, ON, Canada

ACM ISBN 978-1-4503-6753-0/19/06…$15.00
https://doi.org/10.1145/3322431.3325417

1 INTRODUCTION

Within biometric recognition systems, users utilize their physiological and behavioral biometric traits in order to be recognized. This grants the user the convenience of not needing to carry with them a traditional means of authentication. Though biometrics offer this convenience, they also present unique, pressing security and privacy concerns [12]. If an attacker is able to steal the biometric template of a victim, the victim's biometrics are forever lost to the attacker. The victim cannot reasonably revoke and reset their physiological or behavioral traits, as they could a stolen password or smart card. Furthermore, through analysis of a biometric template, an attacker may be able to derive private, personal information about the victim user, such as: ethnicity, age, gender, and health condition [7, 8].

In paper [20], the authors propose the BioCapsule (BC) scheme to address these security and privacy concerns. This fusion-based cancellable biometric scheme involves the introduction of a reference subject (RS). Each user chooses (or is assigned) a RS. Then, during registration or authentication, a user's sampled biometrics are securely fused with the biometrics of their corresponding RS. This secure fusion yields a BC which can be used for biometric recognition. Through the BC scheme's secure fusion process, the contributions of the user and RS features toward the resulting BC are masked. Therefore, analysis of the resulting BC does not reveal the user or RS biometric features, even in the case most favorable to an adversary.

In this paper, we enhance the BioCapsule method by incorporating deep learning techniques for preprocessing and feature extraction tasks. This allows us to demonstrate the BC scheme's ability to be embedded within any deep learning based recognition which uses the most current and robust techniques. We extend the BC scheme from the domain of iris recognition (the initial biometric trait used for testing the BC scheme) to facial recognition. This allows us to demonstrate the BC scheme's general applicability to any biometric recognition system irrespective of which biometric trait it uses. We will robustly evaluate the BC scheme's security and privacy benefits as well as its effect on the performance of an underlying biometric recognition system. We conducted extensive experiments on BC-embedded facial recognition systems and compared the performance of the BC scheme against other cancellable biometric techniques as well. The experimental results demonstrate

that the BC scheme has minimal or no effect on the performance of the underlying systems which it is embedded into and that the BC scheme performs as well, or outperforms many other secure biometrics techniques.

The paper is organized as follows. In Section 2 we offer a brief summary of related work. In Section 3 we overview the BC scheme by highlighting BC's primary components and its seamless integration with any biometric recognition techniques, processes and systems. In Section 4 we propose an underlying biometrics system for the domain of facial authentication which leverages state-of-the-art biometric recognition, deep learning, and machine learning techniques. In Section 5 we provide the specific details of how the BC scheme can be embedded into the proposed underlying system. In Section 6 we perform a comprehensive experiment which compares the performance of the BC-embedded system against the performance of the underlying system. We also compare the proposed BC-embedded system to many previously proposed, popular secure biometrics techniques. In Section 7 we offer concluding remarks and we outline future work directions.

2 RELATED WORK

In recent years, many methods have been proposed and investigated in hopes of securing biometric templates. Two broad classes of approaches for securing biometric templates have emerged: biometric cryptosystems (BCS) and cancellable biometrics (CB).

BCS approaches generate authentication keys from sampled biometrics, rather than using sampled biometrics directly for authentication. BCS approaches yield biometric dependant public data, known as helper data, which can be used to derive corresponding authentication keys. This helper data must not reveal too much about user biometrics and must be stored by the system during registration. Based on how this helper data is used, BCS can be split into two subclasses of approaches: key binding and key generation schemes. In key binding schemes, a user must provide secret information, such as a PIN, which is combined with their biometric template in order to generate helper data [1, 24]. In key generation schemes, helper data is derived directly from the original biometric template [5, 9]. In both key binding and key generating schemes, keys are derived from the resulting helper data.

CB approaches involve applying transformations to a biometric template and using the altered (cancellable) template for authentication. If a cancellable template is stolen, the attacker cannot derive the personal information of the user. In addition, the user can revoke, or cancel, the cancellable biometric template and alter their biometrics differently for future authentication tasks. CB approaches can be divided into two subclasses: salting schemes and noninvertible transformations. In salting schemes, users provide secret information such as a password or PIN. Their biometric template is then transformed by an invertible function with respect to the provided secret information [17, 22]. Since these transformations are typically invertible to some extent, the secure storage of each user's corresponding secret information becomes of the utmost importance. In noninvertible transformations schemes, a biometric template is transformed using a noninvertible (or one-way) function [4, 14]. Unfortunately, many noninvertible transformations systems are not provably secure, and are indeed invertible under certain conditions [13]. For both salting and noninvertible transformations schemes, the transformations applied to biometric templates must be chosen with care. On one hand, the transformations must conceal user biometrics if transformed templates are compromised. Furthermore, the transformations must preserve user privacy. On the other hand, if these transformations raise interclass similarity or raise intraclass variability, the performance of the biometric recognition system will suffer [12].

3 OVERVIEW OF THE BC SCHEME

The BC scheme is elegant, yet simple in design. Its secure fusion process involves three main steps (see Figure 1). First, representative signatures are extracted from both user and RS features. Next, the extracted signatures are mapped to multiple values of 1 and -1 in order to generate keys. Finally, fusion takes place. The key derived from user features is used to alter RS features through element-wise multiplication. Similarly, the RS key is used to alter user features. The altered user and RS features are finally fused using an unweighted vector addition. This fusion process can be represented in the following formula:

$$F^{User,RS} = F^{User} * K^{RS} + F^{RS} * K^{User}$$

where F^{User} and F^{RS} are the user and RS features respectively, K^{User} and K^{RS} are the user and RS keys respectively, $*$ is element-wise multiplication, $+$ is vector addition, and $F^{User,RS}$ is the resulting BC.

In a BC-embedded biometric recognition system, the BC scheme is used to alter all biometrics sampled by the system. Each time the user's biometrics are sampled by the system, they are fused with the biometrics of the user's corresponding RS. As a result, BCs, rather than the original user templates, are used for authentication. Therefore, if an attacker infiltrates the system, BCs are compromised rather than users' true biometric templates. The attackers will not be able to derive information about the user from stolen BCs, as they are privacy-preserving. Furthermore, if any security concern arises, users can revoke compromised BCs and can use a different RS for BC generation in the future. In addition, [20] have indicated that the BC approach has only very minor affects on underlying iris recognition system accuracy.

The elegant, simple design of the BC scheme yields highly advantageous properties. Rather than dictating which preprocessing, alignment, segmentation, feature extraction, or classification steps occur within a biometric recognition system in order to accommodate it, the BC scheme's flexible design allows it to instead embed itself within existing systems. As shown in Figure 1, only the BC scheme's secure fusion process, involving signature extraction, key generation and feature fusion steps (which themselves could be flexible), must be embedded into the existing system. This gives system designers the flexibility to design an underlying biometric system how they wish, with no direct consideration for the BC scheme. After designing an underling system, the system designer can then embed the BC scheme within their system in order to secure it and the privacy of its users. Due to this elegant design, the BC scheme is uniquely fit to secure biometric recognition systems which utilize these techniques.

Though the BC scheme introduces no constraints upon a system's recognition pipeline, the BC scheme does require the introduction of RSs. Furthermore, anytime a user wishes to be authenticated,

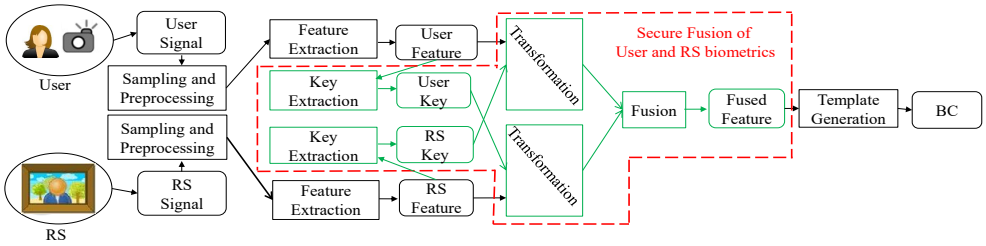

Figure 1: BioCapsule secure fusion process and its ability to be embedded into existing systems

a RS must be provided to (or selected by) the system. This is because, without a RS, BC fusion is not possible.

The incorporation of RSs in a BC-embedded system is quite flexible. A user can choose or be assigned a corresponding RS. The user can decide to keep their RS public or private (with no loss in template privacy benefits). All users can choose (or be assigned) a unique RS, or sets of users can choose (or be assigned) the same RS. Since user and RS biometrics contribute equally in BC fusion, multiple users having the same RS introduces no security concerns (though it may reduce system performance as seen in Section 6). When being authenticated, the user could provide their RS to the system in many different ways. A few examples are:

- In high security scenarios, the RS could be a physical object the user could provide at authentication time. In this type of system, only a database of registered BCs would need to be maintained by the system. Storing RSs and information about which user(s) each RS corresponds to would not be unnecessary.
- A set of RSs could also be provided by the system for the user to choose from at authentication time. In this type of system, a database of registered BCs and RSs would need to be maintained by the system.
- The system could store and automatically use the user's corresponding RS at authentication time. This method would provide the most convenience to the user as they would not need to keep track of their RS. The user would still be protected by the BC scheme's robust security and privacy benefits. In this type of system, a database of registered BCs, RSs and information about which user(s) each RS corresponds to would need to be maintained.

In addition to being flexible in design, the BC scheme also offers robust, provably secure and privacy-preserving benefits. Since the signature extraction, key generation and fusion steps of the BC scheme each have one-way properties, the resulting BC scheme can be shown to be essentially a one-way function. In paper [20], authors formally proved many security and privacy benefits of the BC scheme. These benefits include that the BC scheme is robust in defending against the following four types of attacks. (1) The first type of attack is the case in which a BC is stolen and the attacker then attempts to derive the user's biometric feature vector, which is impossible since it will be equivalent to solving an underdetermined equation. (2) The next type of attack is the case in which the attacker has stolen a user's BC and the user's corresponding RS. This will result in the attacker deriving two possibilities for each value of the user's feature vector (as they will need to guess 1 or -1 for each value within the user's key). This means that the number of possible user feature vectors will grow exponentially with respect to size of the user feature vector. In our proposed system, $O(2^{512}) \approx O(10^{154})$ possible feature vectors can be derived, making obtaining the user's true feature vector computationally infeasible. (3) The third type of attack is the case in which the attacker attempts to derive the RS from multiple stolen BCs of one or multiple users, which is to solve an underdetermined system of equations and thus is impossible. (4) The final type of attack is the case the attacker has stolen multiple BCs (where the BCs belong to several or one user) and their corresponding RSs, which results in many sub-cases of (2), which are computationally infeasible. The detailed proofs can be found in [20].

4 UNDERLYING SYSTEM DESIGN INVOLVING DEEP-LEARNING MECHANISMS

In this section we propose a biometric recognition system for facial authentication. This underlying system will be used to embed the BC scheme within. Since the BC scheme is flexible in design, we only aimed at using the most state-of-the-art deep learning techniques in these systems, and did not directly consider how the chosen techniques would work in conjunction with the BC scheme.

The first step of the biometric recognition systems is to perform alignment and segmentation. We chose to utilize the popular Multi-Task (Cascaded) Convolutional Neural Network (MTCNN) method [25] within our biometric recognition systems. This method was quite robust and outperformed other alignment\segmentation methods which we tried. This method uses a cascade (ensemble) of three convolutional neural networks (CNNs) to perform facial and facial landmark detection. The output of the cascade is a set of facial detection windows, each with five corresponding facial landmark points (left\right eyes, nose, left\right sides of mouth). We were able to find and utilize an open source implementation of MTCNN given by [16].

After we retrieved the (center-most) facial detection bounding box and five corresponding facial landmark points for a given input image, we performed alignment and segmentation. To perform alignment, we rotated the face such that angle between the two eye points would be zero. We then performed segmentation by forwarding the aligned image through the MTCNN a second time. This gave us a facial bounding box for the rotated, aligned image. We used this bounding box to segment the face from the image. We chose to include a 42 pixel margin around the bounding box in order to capture more facial details such as chin shape, hair line, color and style, ears, etc.

The second step of the biometric authentication system is feature extraction. For facial feature extraction we use the popular FaceNet method [18]. The FaceNet method involves extracting facial features using a CNN and embedding the resulting extracted facial features into a compact Euclidean space (with 512 dimensions in our case).

Within this Euclidean space, Euclidean distance between facial feature embeddings directly denotes facial dissimilarity.

We were able to find and utilize an open source FaceNet model given by [16]. This open source FaceNet model extracts facial features using a CNN with an Inception-ResNet-v1 architecture [21].

After we have extracted features from an image, we are ready to perform classification. To perform classification, each registered subject in the biometric authentication system is given a linear binary Support Vector Machine (SVM) classifier. Each subject's SVM is trained with all registered features of the subject as positive samples. Every other subject's registered features are then used as negative samples. Given a test feature and a subject the test feature claims to be, the authentication system classifies the test feature using the chosen subject's binary SVM. This results in a classification decision indicating that the test feature is the subject whom they claim to be or is not this subject. If the classifier indicates the test feature is the more likely subject, the feature is authenticated by the system and rejected otherwise.

5 BIOCAPSULE GENERATION

BC generation involves the secure fusion process. This process utilizes the output of the previously discussed alignment, segmentation and feature extraction steps. It should be noted that the resulting BC-embedded system pipeline only differs from the underlying system with the inclusion of the RS and the BC secure fusion process.

Using a 2-core Intel Core i7-6500u CPU, generating each BioCapsule takes ~0.012 seconds. It should be noted that the BC generation time is substantially faster than alignment\segmentation and feature extraction steps which take ~0.2 and ~0.185 seconds respectively using the same Intel Core i7-6500u CPU. Therefore, the BC scheme does not have significant effects upon the scalability of an underlying biometric recognition system.

The first step in the secure fusion process is signature extraction. For signature extraction, we use the three-level averaging method described by [6], although a different signature extraction method could be used if the system designer wishes. The chosen method involves first reshaping the input 512x1 feature vector into a 32x16 matrix. Then, two averaging convolutions of different sizes are applied to the feature matrix. The resulting matrices are subtracted and a row-wise average is taken of the 32x16 difference. Finally, the resulting 32x1 vector values are multiplied by 10^2 and rounded to integer values to obtain the input feature matrix's signature.

The second step of the secure fusion process is key generation. The key generation process utilizes a feature's extracted signature. Each of a signature's 32 values are used as seeds in a pseudo random number generator to generate 16 uniformly random values (for a total of 512 random values) between 0 and 1. These randomly generated values are placed into a key vector of shape 512x1 (the same size as the initial FaceNet feature vector) and rounded to integer values of 0 or 1. All values within the key that were rounded to 0 are then changed to -1.

Since the key values are derived directly from a signature (which in turn is derived directly from a user feature vector), key stability and distinguishability are directly related to signature stability and distinguishability. Therefore, it can be expected that keys which were derived from similar signatures will, as a result, be more similar than keys derived from less similar signatures. This is not certain though, as all key values are mapped to 1 or -1 using pseudo random number generation and rounding. It is possible for two different signatures to be mapped to the same key 16 values, but the probability of this occurring is $\frac{1}{2^{16}} = \frac{1}{65536} \approx 0.0015\%$. Therefore, it is indeed possible, though very unlikely, for dissimliar signatures to produce similar keys.

The final step of the secure fusion process is the fusion step. From this fusion step we obtain a resulting BioCapsule. A pair of keys are obtained from both a user's feature vector and the feature vector of the user's RS. The user key is used to alter the RS feature through element-wise multiplication. Likewise, the RS key is used to alter the user feature through element-wise multiplication. Through this alteration, the contribution of the features to the final resulting BC is masked. Finally the altered biometrics are fused through an unweighted addition operation to obtain a BC.

After a BC is generated, it can be used for authentication. BCs are classified using the same aforementioned method which the underlying system uses in order to classify regular, unsecured biometric templates.

6 EXPERIMENT

For our experiment, we compare the performance of the proposed underlying authentication system with the performance of the BC-embedded system. This comparison will reveal how embedding the BC scheme into an existing biometric recognition system will affect the underlying system's performance. We also compare the BC scheme to many popular CB and BCS approaches.

For each BC-embedded system test, we consider two cases. The first test case, which we will refer to as the Same RS case, is an adversarial test case which is the most unfavorable possible case for the BC scheme. In this test case all registered users within the training data and all test users in the testing data use the same RS for BC generation. As a result, any BC fusion that takes place will use the same RS feature vector and key. This will, in effect, make all resulting BCs more similar due to the similarity of the RS feature and key used to generate them.

The second test case, which we will refer to as the Unique RS case, is the most favorable possible case for the BC scheme. In this test case, all subjects are assigned a unique RS. In this case, it is likely the BC-embedded scheme will outperform the underlying system. This is because each subject will have a single, unique RS to use to generate it's resulting BCs. Therefore, different subjects will have different RSs which, as a result, will make their resulting BCs dissimilar. This, as a result, will raise interclass variability and lower interclass similarity.

For each test, we report several metrics commonly used to evaluate biometric recognition systems [13], such as: accuracy (ACC), false acceptance rate (FAR), false rejection rate (FRR) and equal error rate (EER). For all tests, RSs were taken from the 10k US Adult Faces dataset [3].

6.1 Authentication Experiment

For our authentication experiment, we utilize the Caltech Faces 1999 dataset [23] and the Georgia Tech Face Database dataset [2]. The Caltech Faces 1999 dataset contains 450 images of 31 subjects. The database features variation in image setting, illumination and facial

Table 1: Authentication Experiment Results

Method	Dataset	ACC	FAR	FRR	EER
Underlying System	[23]	99.98%	0%	0.45%	0%
BC (Same RS)	[23]	99.98%	0%	0.45%	0%
BC (Unique RS)	[23]	99.98%	0%	0.45%	0%
Underlying System	[2]	99.99%	0%	0.267%	0%
BC (Same RS)	[2]	99.98%	0%	0.8%	0%
BC (Unique RS)	[2]	100%	0%	0%	0%

expression. We chose to remove five subjects from our experiment. This was because each of these subjects only had one corresponding image. Furthermore, three of the subjects were not actual humans, but were drawings. This resulted in a dataset of 445 images of 26 subjects. The Georgia Tech Face Database dataset contains 750 images of 15 subjects. The dataset features variation in illumination, facial expression, facial pose and clothing.

We performed an authentication experiment using the previously proposed systems. We used a 5-fold cross validation test on each dataset. Each subject's binary SVM made acceptance and rejection classifications simply based on which was more likely. Therefore, if the probability of a test feature\BC belonging to the positive class was more likely (above 50%), the test feature\BC was accepted. Otherwise it was rejected. The results of this experiment can be seen in Table 1.

For the Caltech Faces 1999 dataset, the underlying system, the Same RS BC-embedded system and the Unique RS BC-embedded system perform identically. For the Georgia Tech Face Database dataset, the three systems perform slightly differently. The underlying system achieves a FAR of 0% with a FRR of 0.267%. The Same RS BC-embedded system performs slightly worse with a FAR of 0% and a FRR of 0.8%. As expected, the Unique RS BC-embedded system performs the best with perfect results of a FAR of 0% and a FRR of 0%.

For all authentication tests, an EER of 0% is achieved. This means that all the systems in each of the tests were capable of performing perfectly. Had we performed a validation step after training each subject's binary SVM and before performing testing, we could have better chosen the SVM authentication threshold. From a validation step, we may have seen that the binary SVM thresholds could have actually been set below 50%. With these lower thresholds, we could have prevented some of the false rejections while, at the same time, preventing any false acceptances.

Though not perfect, these results are quite encouraging. They give clear indication that the BC scheme can be embedded into a state-of-the-art facial authentication system and provide robust security and privacy benefits while, at the same time, only slightly affecting the underlying system performance.

6.2 Comparison with Existing Methods

We also compared the BC scheme with many popular CB and BCS methods. We tested the proposed BC-embedded system in the Same RS and Unique RS cases using the same dataset and testing method of several popular secure biometric methods. This allows us to compare the BC scheme's performance against other proposed secure biometric schemes. The results of each of these comparisons can be seen in Table 2. We report our results in terms of the metric(s) used in the original paper of the technique which we compare the BC scheme with.

The first CB method we compared the BC scheme to was the MACE cancellable filtering based method [17]. In this method, secret PINs are used to generate minimum average correlation energy (MACE) filters. These filters are then applied to facial images in order to create cancellable, secure templates. The MACE authors report a verification EER of 0% which we were also able to achieve using both the Same RS and Unique RS BC-embedded systems.

The second CB method we compared the BC scheme with was the Cancellable 2DPCA method proposed by [4]. The authors use polynomial functions and co-occurrence matrices in order to modify facial images. They then use principal component analysis (PCA) for dimensionality reduction and classification. They report an authentication accuracy of 96%. The Same RS and Unique RS BC-embedded systems were able to achieve accuracies of 99.92% and 99.98% respectively.

The next method we compared the BC scheme to was the BCS Fuzzy Vault based method for faces [24]. This method fuses the biometric template of a user with a key the user must also provide. The authors perform an authentication experiment and report a best FAR of 5.26% and a best FRR of 26%. The Same RS BC-embedded system was able to achieve a FAR of 0% with a FRR of 3%. The Unique RS BC-embedded system was able to achieve a FAR of 0% with a FRR of 0.5%.

Next, we compared the BC scheme to the CB Mixing Biometrics (MB) method [14]. In many respects, this method is more similar to the BC scheme than any other method we compared the BC method with. The MB method uses the facial landmarks of a user facial image and the facial landmarks of a RS-like image in order to fuse the two faces. Classification is then performed using the fused face. Though this method is similar to the BC method in some respects, the BC method has some clear advantages. The MB method requires certain predefined alignment steps to take place for facial fusing. The BC requires no fixed alignment steps. The BC approach also preserves user privacy. From a stolen BC, an attacker cannot derive personal information about the victim, even when the RS image is also stolen. Unfortunately, from MB fused faces, it would not be difficult for attackers to derive personal information of the user. The personal information (such as gender, ethnicity, age, etc.) of the user are clearly visible in the MB fused face. Furthermore, if the attacker obtained the fused face and the

Table 2: Comparison of BC with other Methods

Method	Dataset	Metric	Result
MACE [17]	[19] (Subset)	EER	0%
BC (Same RS)	[19] (Subset)	EER	0%
BC (Unique RS)	[19] (Subset)	EER	0%
Can. 2DPCA [4]	[15]	ACC	96%
BC (Same RS)	[15]	ACC	99.92%
BC (Unique RS)	[15]	ACC	99.98%
Fuzzy Vault [24]	[15]	FAR,FRR	5.26%,23%
BC (Same RS)	[15]	FAR,FRR	0%,3%
BC (Unique RS)	[15]	FAR,FRR	0%,0.5%
MB [14]	[10]	EER	6%
BC (Same RS)	[10]	EER	0%
BC (Unique RS)	[10]	EER	0%
SCiFI [11]	[19] (Subset)	TPR	80%
BC (Same RS)	[19] (Subset)	TPR	99.26%
BC (Unique RS)	[19] (Subset)	TPR	99.85%

RS-like image used for facial fusion in the MB method, the attacker would certainly be able to derive the personal information of the victim user by reversing the fusing process. The MB authors use the IMM face dataset [10] for an identification experiment, as the IMM face dataset has preannotated facial landmarks. The authors report an identification EER of 6%. Both the Same RS and Unique RS BC-embedded systems are able to achieve an EER of 0%.

The final method we compared the BC scheme to was the CB Secure Computation of Face Identification method (SCiFI) [11]. This method uses a secure Principal Component Analysis (PCA) computation in order to identify faces. The authors report a identification (rank one) true positive rate of 80%. The Same RS and Unique RS BC-embedded systems are able to achieve true positive rates of 99.26% and 99.85% respectively.

Each of these comparisons demonstrates that the BC is able to outperform or perform as well as other proposed secure biometric methods. In addition to the BC's superior performance, the BC provides many advantages that not necessarily all of the compared methods do. The BC scheme is flexible in design, provably secure and privacy-preserving unlike most of the compared methods.

7 CONCLUSION AND FUTURE WORK

We have shown that the BC method can be used effectively for facial authentication. The BC scheme can be embedded seamlessly into an existing biometric authentication system with virtually no constraint on how the underlying system operates. This flexible design of the BC scheme allowed us to embed the BC scheme in a recognition system which used state-of-the-art biometric recognition, deep learning techniques. The BC scheme offers an underlying system robust security and privacy benefits while, at the same time, only affecting the underlying system's performance slightly. Furthermore, we have shown that the BC system performs as well as or outperforms many popular secure biometric techniques.

As future work, we believe the BC scheme could be used effectively to facilitate a hierarchical role-based access control (RBAC) scheme. In such a scheme, during authentication a user could specify their RS. In addition to this RS being used for BC generation and protection of the user's biometric information, the RS could also denote the user's role. Based on this role, the user could be granted corresponding privileges as defined by the RBAC scheme. Another future work direction is investigating the intraclass and interclass similarity of BCs formed by the fusion of a user's biometrics with biometrics of multiple RSs. In the proposed BC scheme, if the BC database is compromised, users are able to securely revoke their compromised BCs and register new ones. If users could instead fuse their compromised BCs with new, secondary RSs, the new BCs could then be used for future recognition tasks. In the future, users would simply need to form BCs using their biometrics and their first RS and then fuse the resulting BC with the new, secondary RS.

ACKNOWLEDGMENTS

This work is partially supported by a U.S. NSF grant (NSF-CICI #1839746) and a Purdue University SoS near-the-miss grant.

REFERENCES

[1] Meng Ao and Stan Z. Li. 2009. Near Infrared Face Based Biometric Key Binding. In *Proceedings of the Third International Conference on Advances in Biometrics (ICB '09)*. Springer-Verlag, Berlin, Heidelberg, 376–385. https://doi.org/10.1007/978-3-642-01793-3_39

[2] Monson H. Hayes Ara V. Nefian, Mehdi Khosravi. 1997. Real-time detection of human faces in uncontrolled environments. , 3024 - 3024 - 9 pages. https://doi.org/10.1117/12.263232

[3] Wilma A. Bainbridge, Phillip Isola, and Aude Oliva. 2013. The intrinsic memorability of face photographs. *Journal of experimental psychology. General* 142 4 (2013), 1323–34.

[4] M. A. Dabbah, W. L. Woo, and S. S. Dlay. 2007. Secure Authentication for Face Recognition. In *2007 IEEE Symposium on Computational Intelligence in Image and Signal Processing*. 121–126. https://doi.org/10.1109/CIISP.2007.369304

[5] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. 2008. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* 38, 1 (March 2008), 97–139. https://doi.org/10.1137/060651380

[6] Y. Du, R. Ives, D. M. Etter, and T. Welch. 2006. Use of one-dimensional iris signatures to rank iris pattern similarities. *Optical Engineering* 45, 3 (March 2006). https://doi.org/10.1117/1.2181140

[7] E. Eidinger, R. Enbar, and T. Hassner. 2014. Age and Gender Estimation of Unfiltered Faces. *IEEE Transactions on Information Forensics and Security* 9, 12 (Dec 2014), 2170–2179. https://doi.org/10.1109/TIFS.2014.2359646

[8] X. Geng, Z. Zhou, and K. Smith-Miles. 2007. Automatic Age Estimation Based on Facial Aging Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, 12 (Dec 2007), 2234–2240. https://doi.org/10.1109/TPAMI.2007.70733

[9] Qiming Li, Yagiz Sutcu, and Nasir Memon. 2006. Secure Sketch for Biometric Templates. In *Proceedings of the 12th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT'06)*. Springer-Verlag, Berlin, Heidelberg, 99–113. https://doi.org/10.1007/11935230_7

[10] M. M. Nordstrøm, M. Larsen, J. Sierakowski, and M. B. Stegmann. 2004. The IMM Face Database - An Annotated Dataset of 240 Face Images. http://www2.imm.dtu.dk/pubdb/p.php?3160

[11] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. 2010. SCiFI - A System for Secure Face Identification. In *2010 IEEE Symposium on Security and Privacy*. 239–254. https://doi.org/10.1109/SP.2010.39

[12] S. Prabhakar, S. Pankanti, and A. K. Jain. 2003. Biometric recognition: security and privacy concerns. *IEEE Security Privacy* 99, 2 (March 2003), 33–42. https://doi.org/10.1109/MSECP.2003.1193209

[13] Christian Rathgeb and Andreas Uhl. 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. Information Security* 2011 (2011), 3. http://dblp.uni-trier.de/db/journals/ejisec/ejisec2011.html#RathgebU11

[14] A. Ross and A. Othman. 2011. Visual Cryptography for Biometric Privacy. *IEEE Transactions on Information Forensics and Security* 6, 1 (March 2011), 70–81. https://doi.org/10.1109/TIFS.2010.2097252

[15] F. S. Samaria and A. C. Harter. 1994. Parameterisation of a stochastic model for human face identification. In *Proceedings of 1994 IEEE Workshop on Applications of Computer Vision*. 138–142. https://doi.org/10.1109/ACV.1994.341300

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

[17] 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.*, Vol. 3. 922–925 Vol.3. https://doi.org/10.1109/ICPR.2004.1334679

[18] F. Schroff, D. Kalenichenko, and J. Philbin. 2015. FaceNet: A unified embedding for face recognition and clustering. In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. 815–823. https://doi.org/10.1109/CVPR.2015.7298682

[19] Terence Sim, Simon Baker, and Maan Bsat. 2001. *The CMU Pose, Illumination, and Expression (PIE) Database of Human Faces.* Technical Report CMU-RI-TR-01-02. Carnegie Mellon University, Pittsburgh, PA.

[20] Y. Sui, X. Zou, E. Y. Du, and F. Li. 2014. Design and Analysis of a Highly User-Friendly, Secure, Privacy-Preserving, and Revocable Authentication Method. *IEEE Trans. Comput.* 63, 4 (April 2014), 902–916. https://doi.org/10.1109/TC.2013.25

[21] Christian Szegedy, Sergey Ioffe, and Vincent Vanhoucke. 2017. Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning. In *AAAI*.

[22] A. B. J. Teoh, A. Goh, and D. C. L. Ngo. 2006. Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 28, 12 (Dec 2006), 1892–1901. https://doi.org/10.1109/TPAMI.2006.250

[23] M. Weber. 1999. Caltech Faces 1999. Available at: http://www.vision.caltech.edu/html-files/archive.html.

[24] L. Wu and S. Yuan. 2010. A Face Based Fuzzy Vault Scheme for Secure Online Authentication. In *2010 Second International Symposium on Data, Privacy, and E-Commerce*. 45–49. https://doi.org/10.1109/ISDPE.2010.13

[25] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao. 2016. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. *IEEE Signal Processing Letters* 23, 10 (Oct 2016), 1499–1503. https://doi.org/10.1109/LSP.2016.2603342