Remote Cancelable Biometric System for Verification and Identification Applications

Hatef Otroshi Shahreza[1,2], Amina Bassit[3], Sébastien Marcel[1,4], Raymond Veldhuis[3,5]
[1]Idiap Research Institute, Martigny, Switzerland
[2]École Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland
[3]University of Twente, Enschede, Netherlands
[4]Université de Lausanne (UNIL), Lausanne, Switzerland
[5]Norwegian University of Science and Technology, Gjøvik, Norway

***Abstract*—Cancelable biometric schemes protect the privacy of biometric templates by transforming them, with the help of a key, into an irreversible form that can be replaced if compromised. While these schemes provide more advantages in the user-specific key setting, their application with the user-specific key setting is limited in the identification scenario. Alternatively, the application-specific key setting can be used to employ cancelable biometric systems for the identification scenario. However, in an application-specific key setting, cancelable biometric schemes become static with respect to the protected template replacement; if a protected template or the key is compromised, then the replacement of all the protected templates stored within the same application is mandatory. In addition, experimental results show a degradation of performance for the application-specific key setting in cancelable biometric systems. In this paper, we consider a remote recognition protocol based on cancelable biometric schemes in the identification and verification scenarios so that trusted users can generate protected templates and send them to a server. The server can compare the protected query with the protected templates enrolled in the database for recognition. We investigate the user-specific key setting for cancelable biometric schemes for both verification and identification scenarios, which provides those systems with a dynamic replacement of compromised templates. In our experiments, we analyze different cancelable biometric schemes, including BioHashing, Multi-Layer Perceptron (MLP) Hashing, and Index-of-Maximum (IoM) Hashing. We evaluate their performances when applied within our proposed protocol for face recognition and speaker recognition on the IARPA Janus Benchmark C (IJB-C) and NIST-SRE04-16 datasets for user-specific key and application-specific key settings. The source code of all our experiments is publicly available to facilitate the reproducibility of our work.**

***Index Terms*—biometric template protection, cancelable biometric, face recognition, identification, speaker recognition, user-specific, verification.**

I. Introduction

Biometric recognition systems became wildly deployed in authentication and identification solutions. However, in practice, the constant use of biometric data raises serious security and privacy concerns. In particular, it has been shown that the stored templates in the database of a biometric system can be used to reconstruct the underlying biometric data [1]–[5], which can lead to a crucial privacy threat for the enrolled users. Data regulations, such as EU General Data Protection Regulation (GDPR) [6], consider biometric data as sensitive information, which must be protected. To address privacy-related issues in biometric systems, several biometric template protection (BTP) methods have been proposed in the literature. The ISO/IEC 24745 standard [7] has also defined four requirements for each BTP scheme, including renewability, unlinkability, irreversibility, and performance preservation.

In general, BTP methods can be categorized into *cancelable biometrics* and *biometric cryptosystems*. In *cancelable biometric* schemes, a transformation function, dependent on a key, is used to generate protected templates, and the recognition is based on the comparison of protected templates [8]–[12]. In *biometric cryptosystems*, a key is either bound with (i.e., key binding schemes) or generated (i.e., key generation schemes) from the unprotected template, and then the recognition is based on correct generation or retrieval of the key [13]–[16].

In general, *cancelable biometric* schemes involve the use of a key in the process of generating protected templates. This key can either be *application-specific*, where the same key is used to protect all the templates within the same application, or *user-specific*, where a different key is used to protect the template of each user, even within the same application. However, in an application-specific key setting, if the key is compromised, then all the protected templates are affected. Moreover, a compromised template can affect the protection of the other protected templates within the same application, with an overwhelming probability the key can be recovered from that compromised template. Since the same key was used, then these require the replacement of all protected templates stored within the same application, which affects the dynamism of such cancelable systems. This limitation does not appear in the user-specific key setting because it only affects the compromised template and the compromised key of the same subject. This motivates us to investigate the user-specific key setting for *cancelable biometric* schemes specifically for the identification scenario.

In this paper, we focus on *cancelable biometric* methods and explore the application of user-specific key and application-specific key settings in these methods for identification and verification scenarios. While most works in the literature

This research is based upon work supported by the H2020 TReSPAsS-ETN Marie Skłodowska-Curie early training network (grant agreement 860813). This work was also supported by the PriMa project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie (grant agreement 860315).

focus on the application of *cancelable biometrics* in the verification scenario, few works studied their application for the identification purposes [17]–[20]. In [18], a fingerprint identification method is proposed in which each user has a sensor that has a symmetric key and is time-synchronized with the server. In [17], a format-preserving encryption method is used along with Bloom filters [21], as a cancelable biometric, with an application-specific symmetric key in the identification scenario. In [19], [20], authors proposed indexing protected cancelable templates to accelerate the identification process. The main limitation of applying cancelable biometric systems for the identification scenario is that these systems are often employed in a centralized configuration, and thus the application of user-specific key setting in a centralized system is more suitable for verification, where each subject provides their own key and the system verifies the identity accordingly. Nevertheless, the user-specific key setting in a centralized system has limited application for identification in practice. Alternatively, the application-specific key setting can be used to employ cancelable biometric systems for both identification and verification scenarios. However, compared to user-specific key setting, application-specific key setting suffers from security concerns in case the key or a template is compromised and also has inferior performance than the unprotected system.

In this paper, we present a remote recognition protocol, where trusted users can generate canceblable protected templates and send to the server. The server can compare the protected query with the templates enrolled in the database and return recognition result. In contrast to most cancelable biometric methods which are used for verification scenario in centralized systems, our remote protocol can be used for both identification and verification applications and can be used with both user-specific and application-specific key settings. In particular, our protocol enables application of user-specific key setting for identification scenario. In our experiments, we consider different *cancelable biometric* methods, including BioHashing [8], Multi-Layer Perceptron (MLP) Hashing [9], and Index-of-Maximum (IoM) Hashing [11] (i.e., Gaussian random projection-based hashing, shortly IoM-GRP). We evaluate the performance of each scheme in our proposed protocol for face recognition and speaker recognition in identification and verification scenarios on the IARPA Janus Benchmark C (IJB-C) [22] dataset (face recognition) and NIST-SRE04-16 [23] dataset (speaker recognition) for user-specific key and application-specific key setups.

In the rest of the paper, we first present the protected remote biometric recognition protocol in Section II. Next, we present our experiments in Section III. Finally, the paper is concluded in Section IV.

II. Remote Cancelable Biometric System

In this section, we present our proposed protocol for a remote cancelable biometric system, which is illustrated in Figure 1 (enrollment) and Figure 2 (recognition) for both one-to-one (i.e., verification) and one-to-many (i.e., identification)

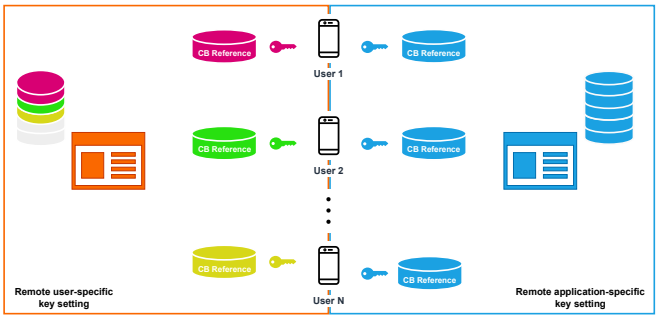


Fig. 1: Enrollment in the Remote Cancelable Biometric System.

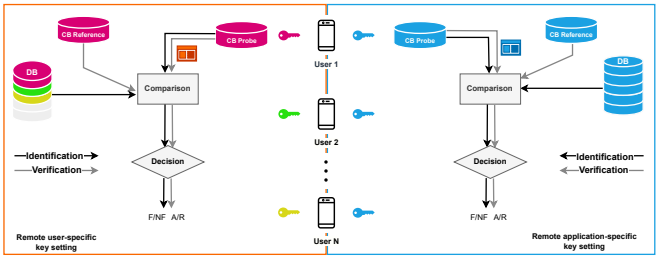
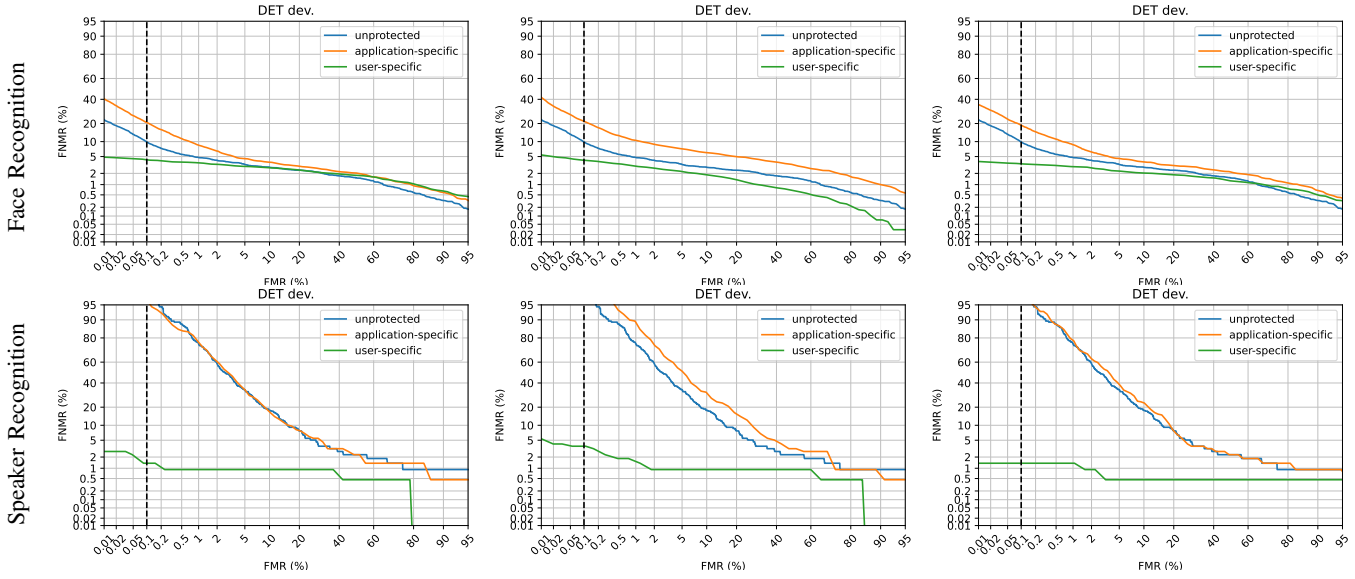


Fig. 2: Recognition (identification/verification) in the Remote Cancelable Biometric System.

comparison scenarios. We consider a remote system where protected templates are generated on the users' end, and then the protected templates are sent to the server. We assume that each user is able to generate their own key that is safely kept with the user (e.g., as a token, or a seed stored at the user's device, etc.). This key is used to generate its protected reference during the enrollment phase (respectively registration phase) and its protected probe during the verification phase (respectively identification phase).

For the one-to-one comparison, the protected probe needs to be compared to the corresponding protected reference, and based on the comparison score a decision is made. For the one-to-many comparison, the protected probe needs to be compared to all protected references stored in the database, and based on the identification scenario (closed-set or open-set based) decision is made. In the case of closed-set identification, the rank of references is considered and the identity of the reference with the highest similarity is returned. In the open-set scenario, in addition to the value of the highest similarity is also compared to the threshold to avoid false identification.

In order to show the difference between the application-specific and user-specific scenarios, Fig. 1 and Fig. 2 present an overview of the system in both application-specific and user-specific key settings. In the application-specific key setting, we consider that for the same application, the users are sharing the same key that was distributed among the users during the setup phase. The risk of doing so is that this multiplies the chances of getting this key exposed. Therefore, for a remote biometric recognition scenario, it is safer to consider a user-specific key setting instead of an application-



(a) BioHash (b) MLP-Hash (c) IoM-GRP

Fig. 3: DET curves of remote cancelable biometric system for face recognition (first row) and speaker recognition (second row) using (a) BioHashing, (b) MLP-Hashing, and (c) IoM-GRP schemes.

specific key setting in order to restrict the impact of the damage resulting from a leaked key.

III. Experiments

A. Experimental Setup

To evaluate the performance of the remote cancelable biometric system presented in Section II, we consider face and speaker recognition in our experiments. For the face recognition system, we use ArcFace [24] as our feature extractor and use the IARPA Janus Benchmark C (IJB-C) [22] dataset. The IJB-C dataset, which is one of the most challenging evaluation datasets in face recognition research, contains 31,334 images of 3,531 subjects. We use the *test4-G1* protocolin our experiments. For speaker recognition, we use ECAPA-TDNN [25] as our feature extractor and use the NIST-SRE04-16 [23] dataset. We use the *development* set of this dataset,which includes 1407 samples from 85 identities.

In our experiments, we consider different *cancelable biometric* methods, including BioHashing [8], Multi-Layer Perceptron (MLP) Hashing [9], and Index-of-Maximum (IoM) Hashing [11] (i.e., Gaussian random projection-based hashing, shortly IoM-GRP). We apply these schemes for face recognition and speaker recognition for both verification and identification scenarios. We should note that we do not evaluate the security aspect of this system (such as irreversibility and unlinkability) since the security of the mentioned *cancelable biometric* methods have been studied in the literature [8], [9], [11], [26].

We use the Bob[1] toolbox [27], [28] for implementation of the biometric pipeline in our experiments. To implement the *cancelable biometric* methods (i.e., BioHashing, MLP-Hashing, and IoM-GRP), we use the open-source implementation of these BTP schemes in Bob [9], [12], [29], [30]. The source code from our experiments is publicly available to facilitate the reproducibility of our results[2].

B. Analaysis

In order to evaluate the effect of the key with respect to the protected template generation, we compare the biometric performances of both application-specific key and user-specific key settings. We consider verification and identification (both open-set and closed-set) for the above scenarios in our experiments, and distinguish between the following experimental scenarios for verification (and respectively for identification):

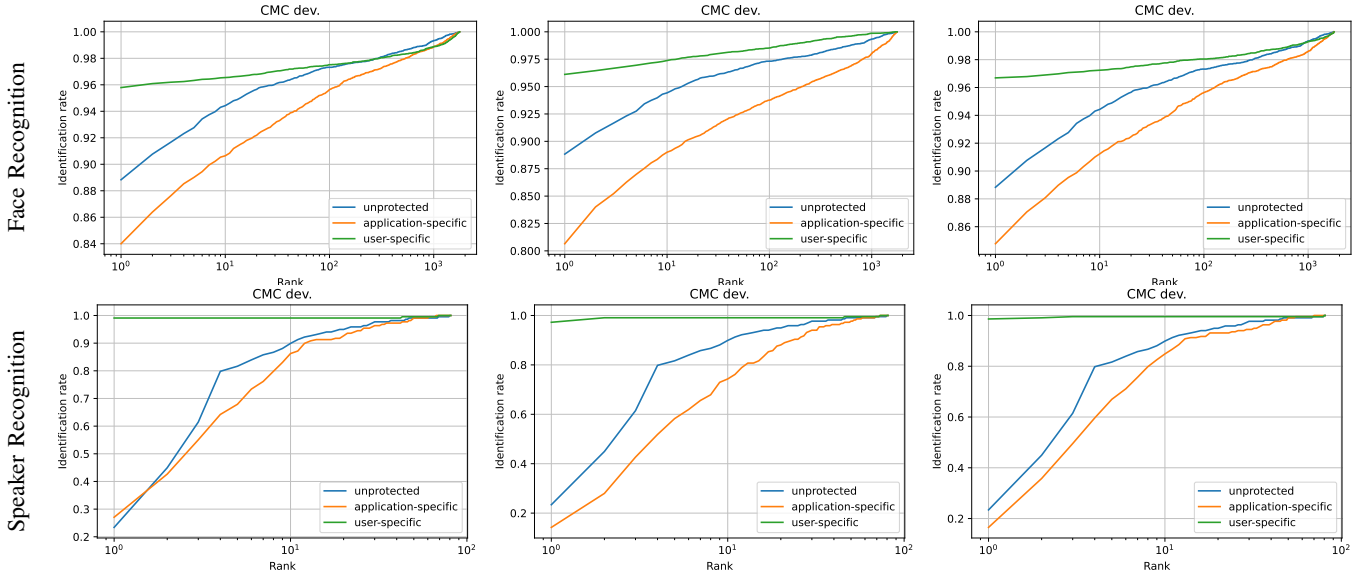
- **Unprotected scenario (baseline):** an unprotected probe P_i is compared against an unprotected reference R_j (respectively references $\{R_j\}_j$).
- **Application-specific key scenario:** a protected probe P_i generated with the key K is compared against a protected reference R_j (respectively references $\{R_j\}_j$) generated with the same key K.
- **User-specific key scenario:** a protected probe generated with a key K_i is compared against a protected reference (respectively references $\{R_j\}_j$) generated with its corresponding key K_j.

We consider verification and identification (both open-set and closed-set) for the above scenarios in our experiments.

1) Verification Evaluation: Fig. 3 shows the Detection Error Tradeoff (DET) curves for evaluation of the remote cancelable biometric system using different BTP schemes for

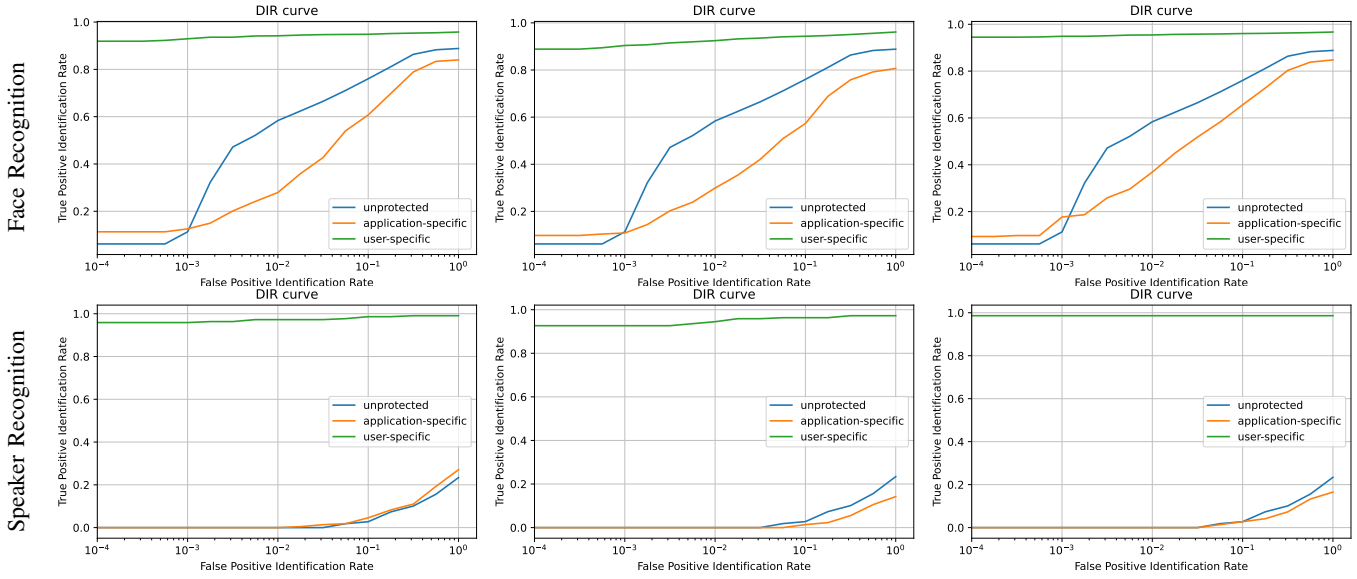
[1]Available at https://www.idiap.ch/software/bob/

[2]Source code: https://gitlab.idiap.ch/bob/bob.paper.biosig2023_remote_cb



(a) BioHash (b) MLP-Hash (c) IoM-GRP

Fig. 4: CMC curves (closed-set identification) of remote cancelable biometric system for face recognition (first row) and speaker recognition (second row) using (a) BioHashing, (b) MLP-Hashing, and (c) IoM-GRP schemes.



(a) BioHash (b) MLP-Hash (c) IoM-GRP

Fig. 5: DIR curves (open-set identification) of remote cancelable biometric system for face recognition (first row) and speaker recognition (second row) using (a) BioHashing, (b) MLP-Hashing, and (c) IoM-GRP schemes.

face and speaker recognition. As the results in this figure show the user-specific key achieves superior performance than the application-specific key and unprotected settings.

2) Identification Evaluation: Fig. 4 and Fig. 5 show the Cumulative Match Characteristics (CMC) plots (closed-set identification) and Detection and Identification Rate (DIR) plots (open-set identification) for face and speaker recognition in our remote cancelable biometric system using different BTP schemes. Similar to the verification scenario, these results also show that the user-specific key can lead to superior performance. We should highlight that as also discussed in Section II, in application-specific key setup, the system is at risk that if the key is leaked all the templates need to be replaced with new protected templates. However, the use of a user-specific key can enable dynamic management of protected template storage. In the event that the key for one template is leaked, the revocation of that specific template is sufficient, preserving the protection of the remaining protected templates.

IV. Conclusion

In this paper, we presented a remote cancelable biometric system and investigated its application for verification and identification (open-set or closed-set) applications. In the proposed protocol, trusted users can use a key to generate and send the protected templates to the server, and the server can use the protected template for comparison and decision making for recognition. We explored both user-specific and application-specific key scenarios in our remote cancelable biometric system. In contrast to the application-specific key setting, our experiments demonstrate that the user-specific key setting enhances biometric performance and mitigates the spread of damage caused by a compromised user's key. In addition to the application-specific key setting, our remote cancelable biometric system enables employing the user-specific key setting for verification and identification scenarios.

References

[1] H. Otroshi Shahreza and S. Marcel, "Comprehensive vulnerability evaluation of face recognition systems to template inversion attacks via 3d face reconstruction," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2023.

[2] G. Mai, K. Cao, P. C. Yuen, and A. K. Jain, "On the reconstruction of face images from deep face templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 5, pp. 1188–1202, 2018.

[3] H. Otroshi Shahreza and S. Marcel, "Template inversion attack against face recognition systems using 3d face reconstruction," in *Proc. of the IEEE/CVF International Conference on Computer Vision (ICCV)*. IEEE, 2023.

[4] H. Otroshi Shahreza, V. Krivokuća Hahn, and S. Marcel, "Face reconstruction from deep facial embeddings using a convolutional neural network," in *Proc. of the IEEE International Conference on Image Processing (ICIP)*. IEEE, 2022, pp. 1211–1215.

[5] H. Otroshi Shahreza and S. Marcel, "Blackbox face reconstruction from deep facial embeddings using a different face recognition model," in *Proc. of the IEEE International Conference on Image Processing (ICIP)*. IEEE, 2023, pp. 2435–2439.

[6] G. D. P. Regulation, "Regulation EU 2016/679 of the european parliament and of the council of 27 april 2016," *Official Journal of the European Union*, 2016.

[7] *ISO/IEC 24745:2022(E) Information technologyy, cybersecurity and privacy protection – Biometric information protection*, International Organization for Standardization International Standard, Feb. 2022.

[8] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[9] H. Otroshi Shahreza, V. Krivokuća Hahn, and S. Marcel, "Mlp-hash: Protecting face templates via hashing of randomized multi-layer perceptron," *arXiv preprint arXiv:2204.11054*, 2022. [Online]. Available: https://arxiv.org/abs/2204.11054

[10] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Proceedings of the International Conference on Biometrics (ICB)*. IEEE, 2013, pp. 1–8.

[11] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 393–407, 2017.

[12] H. Otroshi Shahreza, P. Melzi, D. Osorio-Roig, C. Rathgeb, C. Busch, S. Marcel, R. Tolosana, and R. Vera-Rodriguez, "Benchmarking of cancelable biometrics for deep templates," *arXiv preprint arXiv:2302.13286*, 2023. [Online]. Available: https://arxiv.org/abs/2302.13286

[13] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[14] C. Rathgeb, J. Merkle, J. Scholz, B. Tams, and V. Nesterowicz, "Deep face fuzzy vault: Implementation and performance," *Computers & Security*, vol. 113, p. 102539, 2022.

[15] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.

[16] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[17] V. Bansal and S. Garg, "A cancelable biometric identification scheme based on bloom filter and format-preserving encryption," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5810–5821, 2022.

[18] J. Bringer, H. Chabanne, and B. Kindarji, "Anonymous identification with cancelable biometrics," in *2009 Proceedings of 6th International Symposium on Image and Signal Processing and Analysis*. IEEE, 2009, pp. 494–499.

[19] T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio, and K. Takahashi, "Cancelable permutation-based indexing for secure and efficient biometric identification," *IEEE Access*, vol. 7, pp. 45 563–45 582, 2019.

[20] D. Osorio-Roig, C. Rathgeb, H. O. Shahreza, C. Busch, and S. Marcel, "Indexing protected deep face templates by frequent binary patterns," in *2022 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2022, pp. 1–8.

[21] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On application of bloom filters to iris biometrics," *IET Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.

[22] B. Maze, J. Adams, J. A. Duncan, N. Kalka, T. Miller, C. Otto, A. K. Jain, W. T. Niggel, J. Anderson, J. Cheney *et al.*, "Iarpa janus benchmark-c: Face dataset and protocol," in *2018 international conference on biometrics (ICB)*. IEEE, 2018, pp. 158–165.

[23] S. O. Sadjadi, T. Kheyrkhah, A. Tong, C. Greenberg, D. Reynolds, E. Singer, L. Mason, and J. Hernandez-Cordero, "The 2016 nist speaker recognition evaluation," in *Proc. of Interspeech 2017*, 2017, pp. 1353–1357.

[24] J. Deng, J. Guo, X. Niannan, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4690–4699.

[25] B. Desplanques, J. Thienpondt, and K. Demuynck, "Ecapa-tdnn: Emphasized channel attention, propagation and aggregation in tdnn based speaker verification," in *Proc. of Interspeech 2020*, 2020, pp. 3830–3834.

[26] H. Otroshi Shahreza, Y. Y. Shkel, and S. Marcel, "Measuring linkability of protected biometric templates using maximal leakage," *IEEE Transactions on Information Forensics and Security*, 2023.

[27] A. Anjos, L. E. Shafey, R. Wallace, M. Günther, C. McCool, and S. Marcel, "Bob: a free signal processing and machine learning toolbox for researchers," in *Proceedings of the 20th ACM Conference on Multimedia Systems (ACMMM)*, Oct. 2012.

[28] A. Anjos, M. Günther, T. de Freitas Pereira, P. Korshunov, A. Mohammadi, and S. Marcel, "Continuously reproducing toolchains in pattern recognition and machine learning experiments," in *ICML 2017 Reproducibility in Machine Learning Workshop*, 2017, pp. 1–8. [Online]. Available: https://openreview.net/forum?id=BJDDItGX-

[29] H. Otroshi Shahreza and S. Marcel, "Towards protecting and enhancing vascular biometric recognition methods via biohashing and deep neural networks," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 3, pp. 394–404, 2021.

[30] H. Otroshi Shahreza, V. Krivokuća Hahn, and S. Marcel, "On the recognition performance of biohashing on state-of-the-art face recognition models," in *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2021, pp. 1–6.