Machine Intelligence Research
www.mi-research.net

20(6), December 2023, 855-871
DOI: 10.1007/s11633-023-1432-x

OTB-morph: One-time Biometrics via Morphing

Mahdi Ghafourian Julian Fierrez Ruben Vera-Rodriguez
Aythami Morales Ignacio Serna

Biometrics and Data Pattern Analytics Laboratory (BiDA Lab), Universidad Autonoma de Madrid, Madrid 28049, Spain

Abstract: Cancelable biometrics are a group of techniques to transform the input biometric to an irreversible feature intentionally using a transformation function and usually a key in order to provide security and privacy in biometric recognition systems. This transformation is repeatable enabling subsequent biometric comparisons. This paper introduces a new idea to be exploited as a transformation function for cancelable biometrics aimed at protecting templates against iterative optimization attacks. Our proposed scheme is based on time-varying keys (random biometrics in our case) and morphing transformations. An experimental implementation of the proposed scheme is given for face biometrics. The results confirm that the proposed approach is able to withstand leakage attacks while improving the recognition performance.

Keywords: Biometrics, face recognition, template protection, morphing, security.

Citation: M. Ghafourian, J. Fierrez, R. Vera-Rodriguez, A. Morales, I. Serna. OTB-morph: One-time biometrics via morphing. *Machine Intelligence Research*, vol.20, no.6, pp.855–871, 2023. http://doi.org/10.1007/s11633-023-1432-x

1 Introduction

Biometrics are unique methods of identifying people based on their biological and behavioral characteristics. The advantage of biometric recognition in authentication systems compared to conventional methods such as using passwords or smart cards, has resulted in attracting much attention to this field. However, the widespread usage of biometrics has raised serious security and privacy concerns[1, 2]. In addition, standard cryptographic approaches failed to address these concerns due to the noisy nature of biometrics[3]. Therefore, a new class of protection methods called biometric template protection (BTP) has emerged as a solution[4–8]. Biometric template protection is a set of techniques to preserve the security and privacy of the subject′s acquired biometric features. The main goal is to generate a protected biometric reference out of original biometric data that guarantees desired attributes: noninvertibility (irreversibility), revocability (renewability), and unlinkability (nonlinkability) without degrading the recognition performance. Noninvertibility refers to the computational difficulty of obtaining the original biometric template from someone′s protected biometric reference. Revocability refers to the ability to change the biometric reference (template) for the same raw input biometric data without affecting the system performance. Unlinkability refers to the computational difficulty of ascertaining the subject′s identity by linking multiple biometric references of him. To this end, BTP methods have been introduced and commonly divided into three categories: cancelable biometrics, biometric cryptosystems, and biometrics in encrypted domains[9].

Among these methods, cancelable biometrics[10] are very promising due to their unique features such as providing revocability in the case of leakage reports. In general, cancelable biometrics refers to a group of template protection techniques with the primary aim of improving template security and privacy by transforming the original feature using an irreversible transformation function such that the recognition can still be performed but in the transformed domain. These methods should maintain four characteristics for the transformed feature: diversity, revocability, non-invertibility, and recognition performance. During enrollment in a biometric verification scenario, some biometric data are extracted upon presentation, then the corresponding cancelable biometric transformation is applied to these features (mainly by using auxiliary data) and finally, the result (transformed template) is stored on the server′s database. During verification, when the client presents her biometric feature, the transformed template is extracted similarly to the enrollment phase but by applying the previously stored or known auxiliary data. Finally, matching takes place between the generated cancelable template at the verification phase and the one stored at the enrollment phase called the reference. A general taxonomy of all cancelable biometric methods containing six major categories was proposed recently in [11].

In the present paper, we adopted the concept of the one-time-pad method[11] to derive one-time biometrics as

Research Article
Manuscript received on September 27, 2022; accepted on March 2, 2023; published online on June 1, 2023
Recommended by Associate Editor Hao Dong
Colored figures are available in the online version at https://link.springer.com/journal/11633
© Institute of Automation, Chinese Academy of Sciences and Springer-Verlag GmbH Germany, part of Springer Nature 2023

a new cancelable biometrics method. The core elements of our proposed scheme are: 1) to use biometric data generated randomly with natural appearance as time-variant keys[12], 2) combining these keys (random biometrics) with real input biometric data using image/signal morphing techniques[13], and 3) keeping track of the key/template variations in time in a specific secure exchange protocol to enable biometric comparisons while protecting against potential attacks.

The present paper is the extended version of our preliminary research[14]. In this paper, we extend our previous results by experimenting in a wider range of settings. In particular, first, we increased the number of verification sessions to demonstrate the superiority of the proposed method against iterative optimization attacks in longer runs compared to other protection methods. Second, we used another dataset, Face Mask Lite, a GAN-generated face image dataset, as random biometrics in addition to face images taken from the labeled faces in the wild (LFW) dataset in order to produce our morphed templates. Third, we used the pre-trained ArcFace and AdaFace models on top of ResNet-50 to report the result of the proposed method in a wider range of face recognition systems.

The rest of this paper is organized as follows: Section 2 summarizes related works in cancelable biometrics. Section 3 describes the threat model under which we have conducted our experiments and compared the security improvement of our proposed method with other scenarios. Section 4 describes our proposed cancelable biometrics method called one-time biometrics (OTB)-morph. The experimental results for implementing the proposed method on face biometrics and its advantages compared to existing methods are reported in Section 5. Finally, Section 6 concludes the paper.

2 Related works

Over the past two decades, many cancelable biometrics studies have been carried out due to the increasing usage of biometric-based authentication. In this section, we provide a brief description of the most noticeable attempts in this area.

The concept of cancelable biometrics was first introduced in [15] to enhance security and privacy in biometric-based authentication systems. Among early noticeable attempts, Jin et al.[16] proposed a random projection-based technique called BioHashing. This method projects biometric features to a random space by taking the inner product between a tokenized pseudo-random number and the subject′s fingerprint. In 2005, Ang et al.[17] proposed a key-dependent cancelable template where a geometric transformation was applied to features extracted from a fingerprint so as to protect minutiae templates. In 2006, Lee et al.[18] presented a work securing iris features coined as S-Iris encoding. To this end, they iterated inner products between secret pseudo-random numbers and the iris features. In 2007, the first alignment-free cancelable biometrics method was introduced by Lee et al. They protected fingerprint templates by extracting rotational and translational invariant features from each minutia. Later that year, Ratha et al.[19] suggested three different methods (Cartesian, polar, and surface folding) to transform minutia positions extracted from a fingerprint image. These transformations were aimed at distorting original biometrics and offering noninvertibility and revokability. However, soon after Quan et al.[20] showed that most of the transformed minutia in [19] could be exactly inversed.

More recently Maiorana et al.[21] proposed a convolution-based noninvertible transformation named BioConvolving, which can be applied to any sequence-based biometric. They practiced their approach on online signature biometrics and its security relies on the difficulty of solving a blind deconvolution problem. In the same year, Ouda et al.[22] proposed a cancelable biometric scheme for protecting iris-codes. Their method extracts consistent bits from iris-codes and further encodes them using a random encoding process referred to as BioEncoding. Another study[23] generated cancelable iris biometrics using sectored random projections that year. This method mitigates the performance degradation due to eyelids and eyelashes. In 2012, Ferrara et al.[24] provided noninvertibility based on dimensionality reduction and binarization to protect minutia-cylinder-code, which is a local minutia representation. Later, Gomez-Barrero et al.[25–27] proposed an alignment-free cancelable iris template based on bloom filters. They argued that successive mapping of parts of a binary biometric template to a bloom filter represents a noninvertible transformation. Chin et al.[28] proposed another template protection technique in 2014 by fusing fingerprints and palmprints at the feature level using client-specific keys. Three years later, Lai et al.[29] introduced a cancelable iris template generation method coined as indexing-first-one (IFO) hashing. The method is inspired by Min-hashing and extended by using modulo threshold functions and P-order Hadamard products. In 2019, Sadhya and Raman[30] generated a cancelable iris template using randomized bit sampling. Their method (LSC) is functionally based on the notion of locality sensitive hashing (LSH) in which two items that are relatively close to each other, are hashed into the same location[3]. In 2020, Kirchgasser et al.[31] compared cancelable approaches using finger vein biometrics in both the signal and the feature domains. They reported that for most experimental settings, it is possible to track a subject across several instances generated with various keys. In the same year, the same research group reported in [32] that considering state-of-the-art deep-learning methods, warping-based cancellable biometrics is no longer a protection scheme. The next year, Badr et al.[33] presented a cancellable face recognition scheme that is based on face image encryption with fractional-order (FO) Lorenz

chaotic system. In 2022, Dong et al.[34] proposed a deep learning-based cancellable biometric scheme for face identification (one-to-many matching). In this research, they used a deep rank hashing (DRH) network and a randomized lookup table function to transform a raw face image into discriminative yet compact binary face hash codes. Finally, Chang et al.[35] proposed a multi-biometric cancelable approach using the fuzzy extractor and a bit-wise encryption scheme to transform a biometric template to a protected template by means of a secret key generated from another biometric template.

What makes our research different from these works, is addressing the iterative optimization attacks. This is very important, because with the appearance of adversarial examples as a branch of iterative optimization, the possibility of this threat has increased tangibly. To the best of authors knowledge, there is no prior biometric template protection method taking into account addressing the threat of iterative optimization attacks.

3 Threat model

Biometric systems can be the target for an attacker to conduct malicious activities, including impersonation. The possible attack points are positioned in a generic biometric system in Fig. 1[1, 2].

This paper is focused on addressing three challenges: 1) privacy leakages at attack point AP6, 2) injection attacks at AP4, and 3) leakage threats at AP7. This threat model specifies the adversary's goal, capabilities, and knowledge under which the aforementioned attacks are feasible. In particular, we assume that:

1) The attacker is able to eavesdrop on the communication channel from AP6 where genuine clients request verification.

2) The similarity score of biometric templates at the matching phase is leaked to the attacker through any wide-range means of leakage attacks such as backdoors, trojans, side-channel attacks[36, 37], etc.

3) The attacker is able to obtain the similarity score between an arbitrary biometric input and the feature reference of victims from AP7 for some verification sessions, not necessarily being consecutive.

4) The attacker possesses the knowledge of the underlying model with which the protected template (victim's reference) is generated from the input biometric data (i.e., the biometric feature extractor).

5) The attacker is able to obtain at least one biometric input of the victim.

6) The attacker is able to override the feature extractor and can inject his biometric features in AP4.

Using this leaked score or the obtained biometric input, the attacker can maximize the similarity of his arbitrary input biometric compared to the victim's reference by iterative optimization, an adversarial perturbation that is added to the attacker image after each comparison with the victim image gradually in order to lower the similarity score, e.g., deep leakage from gradient[38], and hill-climbing[39–41].

4 Proposed scheme: OTB-morph

The aim of the proposed scheme is to address both privacy leakages at attack point 6 (AP6, see Fig. 1) and leakage attacks at attack point 7 (AP7). The block diagram showing the architecture and data flow of the proposed scheme in a generic biometric system is shown in Fig. 2.

There are three parties involved during biometric verification. A Client who wants to be verified in a Server using a temporary identity that has been assigned to him by a trusted third party (TTP). We refer interested readers in trusted systems to [42]. It is assumed that enrollment phases in both server and TTP are already accomplished and the corresponding auxiliary data (AD) and pseudonyms are stored on a secure element in the client's device or his smartcard (note that the complete process of the proposed method is explained in detail later with an

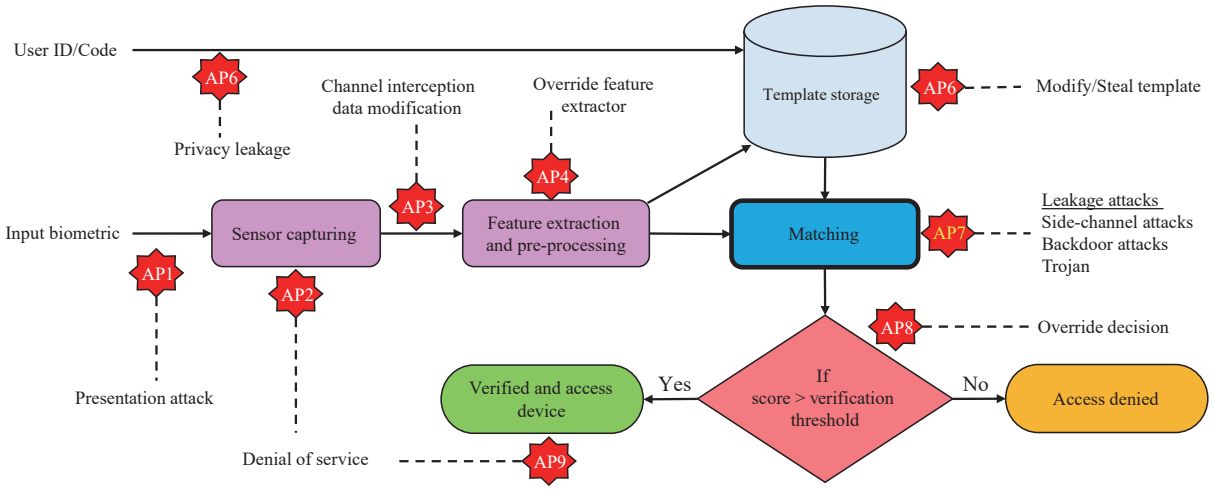


Fig. 1 Attack points (AP) in a generic biometric system

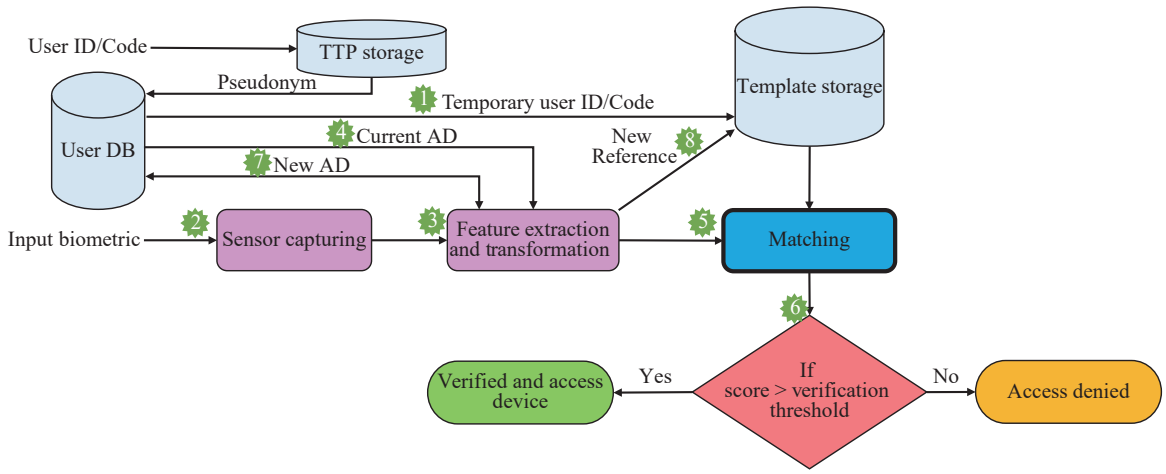


Fig. 2 Architecture of the proposed one-time biometrics scheme (OTB-morph)

example in face biometrics). In this regard, the client starts the verification session by sending his request to the server using one of his stored pseudonyms (num 1). Pseudonyms are temporary identities that have been assigned to the client previously by the TTP. We adopted the pseudonym architecture described in Section 4.1 from [43] for our problem. Upon receiving the answer from the server, the client presents his biometric to the input sensor (num 2) and the extracted feature will be transformed to a cancelable biometric template (num 3) using the current AD (num 4) that he has stored on his device/smartcard from the enrolment process. In the next step, the produced cancelable biometric template is sent to the server domain to be compared in the biometric matcher with the feature reference of the client (num 5). Depending on the verification threshold, access is granted or denied (num 6). Generally, most cancelable biometric techniques need AD to compute the transformation of biometric features. This AD can be a password, a random number, etc., and it is usually permanent until a leakage on the respective cancelable template is reported. In our proposed method, these auxiliary data are random biometrics (e.g., GAN-generated synthetic faces[12], LSTM-generated synthetic handwriting[44], etc.), sent to the client inside the pseudonym sets managed by the TTP. When the matching is successful, we propose to re-enroll by picking a new random biometric (AD) (num 7) and combining it with the already extracted feature. The resulting cancelable template is stored as a new reference (num 8) in the server′s database. Finally, the new AD is stored on the client′s device replacing the previous one. Here with OTB-morph, we propose to combine the random and the input raw biometrics via image-morphing or signal-morphing, depending on the nature of the biometrics at hand.

The notations used in this paper are described in Table 1.

Table 1 Notations used in this paper

Notation	Description
N_x	The nonce generated by the party x
d_x	The private key of the party x
Q_x	The public key of the party x
PN_C^i	The i-th pseudonym set of client
LT_C^i	The lifetime of the i-th pseudonym set of client
ID_x	The identifier of the party x in the transport protocol
PID_{TTP}	The permanent identity of TTP
TID_C^i	The i-th temporary identity of client
SK_{SC}^i	The i-th pseudonym set shared secret key
RF_C^i	The i-th randomly generated face image using as AD
F_C^i	Client presented face at the i-th session
R_C^i	Client feature reference at the i-th session
MF_C^i	The morphed face of client used at the i-th session
MGF	The morph generation function
$Mtch$	The face matching function
KGF	The symmetric key generation function
$AEnc(k, m)$	Asymmetric encryption of the message m with the key k
$Enc(k, m)$	Symmetric encryption of the message m with the key k
$Sig(k, m)$	Signing the message m with the key k
$resp_x$	The response of party x
$\|\|$	The concatenation operation

4.1 Enrollment in the trusted third party

The client registers in the TTP by sending his ID_C and his public key Q_C. Then the TTP stores these data and sends back n temporary identities (called pseudonym) PN_C^i, $i = 1, 2, \cdots, n$ with his ID_{TTP} to the client. Upon receiving n pseudonym sets, the client stores all of them protected in his device. These pseudonym sets are meant to be used per verification session. The structure

of the pseudonym and corresponding signature for client C is as follows:

$$PN_C^i = \{TID_C^i \parallel AEnc(Q_c, RF_C^i) \parallel PID_{TTP} \parallel LT_C^i \parallel S_{TTP}^i\} \quad (1)$$

$$S_{TTP}^i = Sig(d_{TTP}, TID_C^i \parallel AEnc(Q_c, RF_C^i) \parallel PID_{TTP} \parallel LT_C^i \parallel S_{TTP}^i). \quad (2)$$

4.2 Enrollment in server

The genuine client enrolls in the server by presenting his face. Upon this, the system picks a random pseudonym and applies a random face image as auxiliary data to the cancelable method. This face image is an arbitrary face image (real or artificial) that is not repeated in any pseudonym sets before or in the future. Then, a face morphing transformation is applied to both face images to generate the protected template. Next, the cancelable template is stored on the server's database as the client's biometric reference. Finally, the arbitrary face extracted earlier from the pseudonym set is recorded as the current auxiliary data (current AD) in a secure element at the client's device and the corresponding pseudonym is discarded. The process of client C registering in the server through a secure channel is described in the following steps:

Step 1. The client presents his face F_C^i and picks a random pseudonym set from his storage, extracts RF_C^i by performing $ADec(d_C, AEnc(Q_C, RF_C^i))$ and computes $MF_C^i = MGF(F_C^i, RF_C^i)$, then sends the message $M_1 = \{ID_C, MF_C^i, PN_C^i\}$ to the server to request registration.

Step 2. Upon receiving M_1, the server first checks whether LT_C^i is valid. If it does not hold, the server terminates the registration; otherwise, it tries to verify the authenticity of PN_C^i by decrypting S_{TTP}^i in PN_C^i using Q_{TSM} and compares the obtained parameters with the corresponding ones existing in the pseudonym content. If this authenticity does not hold, the server terminates the session; otherwise, it generates a random secret SK_{SC}^i corresponding to the client's i-th pseudonym set. Then, the server stores PN_C^i, MF_C^i and SK_{SC}^i for the client's temporary identity TID_C^i on its database. Finally, it sends the message $M_2 = \{ID_S, N_S, SK_{SC}^i\}$ to the client. Henceforth, we call the MF_C^i, the one that the server stores on its database, client's reference R_C^i.

Step 3. Upon receiving the message M_2, the client stores $\{TID_C^i, RF_C^i, SK_{SC}^i\}$ on his device protected as the current credentials and drops PN_C^i.

4.3 Verification protocol using the proposed method

In order to establish a face verification between the client and the server using the proposed method, the following steps are provided. A summary of these steps is given in Fig. 3.

Step 1. The client starts the session by picking a random pseudonym PN_C^i, extracting $TID_C^{(i-1)}$ from his storage, and generating a nonce N_C. Then, he sends the message $M_1 = \{ID_C, N_C, PN_C^i, TID_C^{(i-1)}\}$ to the server.

Step 2. Upon receiving M_1, the server first checks whether LT_C^i is valid. If it does not hold, the server terminates the session; otherwise, it tries to verify the authenticity of PN_C^i by decrypting S_{TTP}^i in PN_C^i using Q_{TSM} and compares the obtained parameters with the corresponding ones existing in the pseudonym content. If this authenticity does not hold, the server terminates the session; otherwise, the server extracts $SK_{SC}^{(i-1)}$ corresponding to $TID_C^{(i-1)}$ from its database, and then computes $resp_S = Enc(SK_{SC}^{(i-1)}, TID_C^{(i-1)})$ by performing symmetric encryption. Finally, the server generates a nonce and replies to the client by sending the message $M_2 = \{ID_S, N_S, resp_S\}$.

Step 3. Upon receiving the message M_2, the client verifies $resp_S$ by checking whether (3) holds. If it does not hold, client terminates the session and starts a new

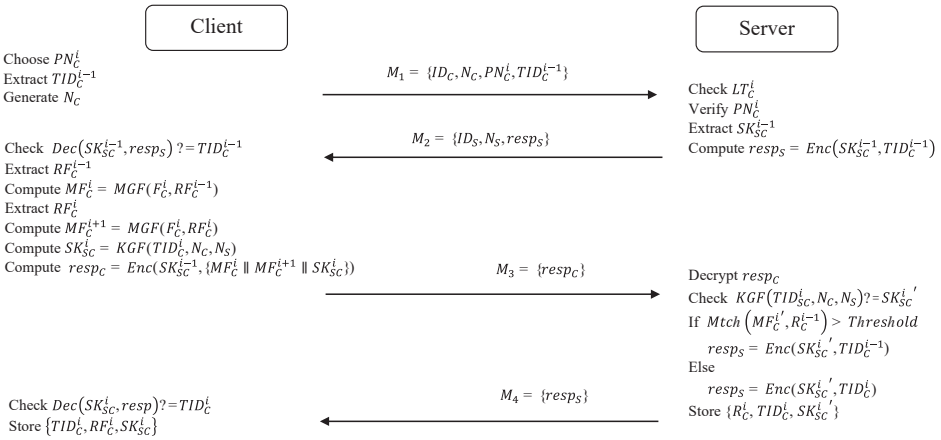


Fig. 3 Biometric verification protocol using the proposed method

one; otherwise, he presents his face F_C^i to his device's camera, extracts $RF_C^{(i-1)}$ from his storage and computes $MF_C^i = MGF(F_C^i, RF_C^{(i-1)})$. Next, he extracts RF_C^i from PN_C^i by doing $ADec(d_C, AEnc(Q_C, RF_C^i))$ and computes $MF_C^{(i+1)} = MGF(F_C^i, RF_C^i)$. Finally, the client computes $SK_{SC}^i = KGF(TID_C^i, N_C, N_S)$ and (4), then he sends the message $M_3 = \{resp_C\}$ to the server.

$$Dec(SK_{SC}^{(i-1)}, resp_S) = TID_C^{(i-1)} \tag{3}$$

$$resp_C = Enc(SK_{SC}^{(i-1)}, \{MF_C^i \parallel MF_C^{(i+1)} \parallel SK_{SC}^i\}). \tag{4}$$

Step 4. Upon receiving the message M_3, the server decrypts $resp_C$ using $SK_{SC}^{(i-1)}$ and checks whether (5) holds. If it does not hold, the server terminates the session; otherwise, it computes $Mtch(MF_C^{i\prime}, R_C^{(i-1)})$. If the corresponding result is not above the face matching threshold, the server computes $resp_S = Enc(SK_{SC}^{i\prime}, TID_C^{(i-1)})$ and sends the message $M_4 = \{resp_S\}$ to the client and terminates the session; otherwise, the server first drops $R_C^{(i-1)}$, $TID_C^{(i-1)}$, $SK_{SC}^{(i-1)}$ and replaces them with $MFC_C^{(i+1)\prime}$ as R_C^i, TID_C^i, and $SK_{SC}^{i\prime}$, respectively. Then, it computes $resp_S = Enc(SK_{SC}^{i\prime}, TID_C^i)$ and sends the message $M_4 = \{resp_S\}$ to the client.

$$KGF(TID_{SC}^i, N_C, N_S) = SK_{SC}^{i\prime}. \tag{5}$$

Step 5. Upon receiving the message M_4, client checks whether $Dec(SK_{SC}^i, resp_S) = TID_C^i$ holds. If it does not, he repeats Step 3 from face presentation part; otherwise, he drops previously stored credentials and replaces them with $\{TID_C^i, RF_C^i, SK_{SC}^i\}$.

For a better understanding of readers, the whole operation of the proposed cancelable biometrics method including client enrollment and verification is depicted in Fig. 4.

5 Experiments

In this paper, we implemented an attack framework using iterative optimization in which the adversary who obtained the matching score of the victim's biometric feature explained in Section 3, is able to update an arbitrary face image such that the corresponding score (Euclidean distance in our experiments, therefore dissimilarity score) of it with respect to the victim's reference becomes lower than the verification threshold[39]. In other words, using this attack framework, the adversary is able to manipulate his arbitrary face image and successfully impersonate a legal client. In order to confirm the weakness of current cancelable biometric methods against leakage attacks, we implemented our experiments with respect to seven scenarios: i) Face verification without applying any protection method; ii) Face verification protected by applying Gaussian noise as cancelable transformation; iii) Face verification protected by applying Lapla-

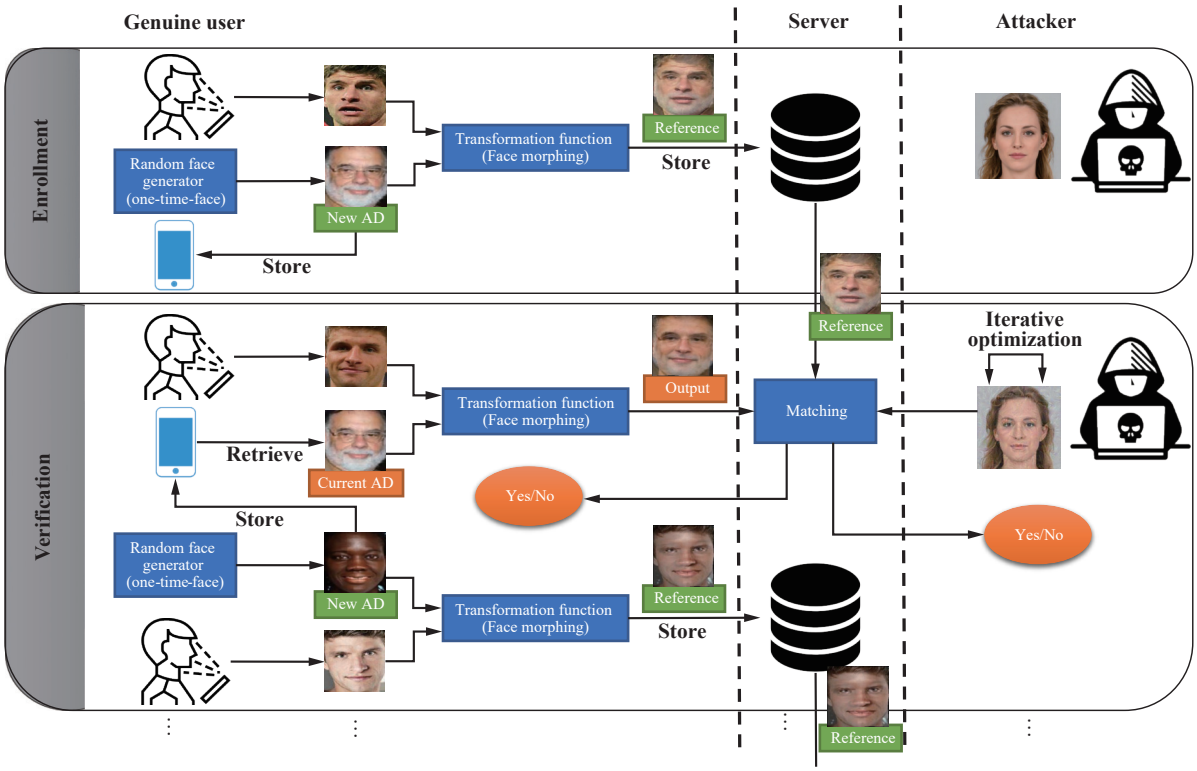


Fig. 4 Visual examples of the process of the proposed OTB-morph for enrollment and various verification sessions (genuine clients and attackers)

cian noise as cancelable transformation; iv) Face verification protected by applying spread, a transformation that replaces each pixel with a random pixel value found in a radius nearby; v) Face verification protected by applying imploding, a transformation that pulls pixels into the middle of the image; vi-a) Face verification protected by applying the proposed method using the LFW dataset as random biometric; and vi-b) Face verification protected by applying the proposed method using the Face Mask Lite dataset as random biometric. An example showing the input biometric of the experimented scenarios is depicted in Fig. 5. The experiments are conducted using the following face datasets: on the one hand, VGGFace2[45] and CASIA[46] are used as genuine client's biometrics, and on the other hand, LFW[47, 48] and Face Mask Lite[1] are used to select the random face images for the morphing operations[2].

5.1 Implementation details

We performed our implementation on pre-trained ResNet-50[49], pre-trained ArcFace[50] and pre-trained AdaFace[51], CNN models proposed for general image recognition tasks using two groups of datasets. As the first group, we used the VGGFace2[45] and Casia[46] datasets, two face datasets that contain multiple faces of the same individual. The images in these datasets are utilized as probe faces of genuine clients during verification sessions. Regarding the second group, we used LFW[47, 48] and Face Mask Lite (we used face images without masks) as the auxiliary data (a random seed) to create morph faces for our proposed OTB-morph scheme. In other words, our method takes two input faces, one from the first group as the probe biometric feature of the subject meant to be protected, and the second input is a randomly chosen face image from the second group to be morphed with the first image.

5.1.1 Image morphing

Image morphing is an image processing technique that can transform one image into another image. Applied to face images, morphing is being used to generate artificial faces which resemble the biometric characteristics of at least two input individuals in image and feature space[13]. Morphed faces can be generated using various methods from simple image overlaying to Generative Adversarial Networks (GAN). The most popular morphing method is landmark-based, which consists of three steps: 1) determining a correspondence between the two contributing face images; 2) warping, which means distorting both features such that the corresponding facial elements (e.g., eye, nose, mouth) are geometrically aligned; and 3) blending, which refers to the process of merging the color values of wrapped images. In our experiments, we use landmark-based morphing as a transformation function for our proposed cancelable biometrics method. There are many landmark detection algorithms such as [52] for face biometrics. Our morphing implementation is based on Dlib for landmark detection[13] and OpenCV for image processing[53].

The landmark locations obtained from both face images are warped by averaging the pixel positions. After moving the pixels we apply image warping based on Delaunay triangulation[54]. Our morphing method has a parameter α between 0 and 1 that trades off the contribution of each input image: a smaller α generates an output more similar to the first contributed face image (probe face in our case), and a higher α results in a morphed face more alike to the second contributed face image (random face). In these experiments, we selected $\alpha = 0.5$ to maintain the trade-off.

5.2 Performance and security metrics

We use the Equal Error Rate (EER) to evaluate and compare the verification performance of our proposed method with other scenarios. EER is the point where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are equal, where FAR is the percent of unauthorized clients (random impostors[3]) incorrectly verified as a valid client (genuine) while FRR is the percent of incorrectly rejected valid clients. The evaluation metric EER describes the overall accuracy of a biometric system. In general, the lower the EER value, the higher the accuracy of the biometric system.

Regarding security evaluation, the vulnerability of the compared cancelable biometrics schemes under the considered threat model (cf. Section 3) is analyzed by examining the capability of the attacker to minimize the dissimilarity score of his arbitrary face image by iterative optimization exploiting the leaked matching score. More specifically, we measure the Attack Success Rate (ASR) to assess and compare the vulnerability of all experimental scenarios[39].

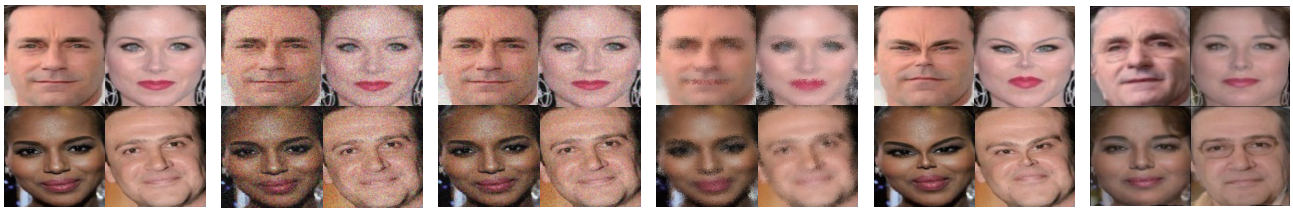
5.3 Results

The results of our experiments on ResNet-50, ArcFace, and AdaFace models are demonstrated in Figs. 6–8, respectively. In general, Figs. 6–8 consist of seven rows, each of them representing one of the seven scenarios we implemented: (a) not applying any protection method; (b) applying Gaussian noise; (c) applying Laplacian noise; (d) applying spread; (e) applying imploding; (f) applying our proposed OTB-morph method using the LFW data-

[1] https://www.kaggle.com/datasets/prasoonkottarathil/face-mask-lite-dataset

[2] Faces in Figs. 4 and 5 are selected from LFW publicly available at https://www.kaggle.com/datasets/jessicali9530/lfw-dataset

[3] This kind of impostors are different from the attackers considered in Section 3, who have much more information to attack the system compared to a random impostor that just tries to illegally access the system by using his own face input and no other methods to improve the attack success.



Scenario i (Normal faces) | Scenario ii (Gaussian noise) | Scenario iii (Laplacian noise) | Scenario iv (Spread) | Scenario v (Imploding) | Scenario vi (OTB-morph)

Fig. 5 Examples of experimented scenarios

set as the random biometric; and (g) applying our proposed OTB-morph method using face mask lite dataset as the random biometric. Figs. 6–8 also comprise four columns: the first column shows the attacking matching (dissimilarity) score evolution on the CASIA dataset. The second column shows the score distributions obtained for the seven scenarios considered with respect to the CASIA dataset. The last two columns are similar to the first two columns but with respect to the VGGFace2 dataset. In the plots representing attacking matching (dissimilarity) score evolution (Columns 1 and 3), in the vertical axis we can see multiple horizontal lines representing the decision threshold location at the EER point and various FAR points (see the figure legends). Additionally, these plots represent the time evolution of the attacking score in 180 consecutive iterations, which we call verification sessions (from left to right in each plot).

The scenarios that we used as transformation functions differ from each other in terms of the type of perturbation they apply to the input image. While some scenarios simply add different types of noises, others change the structure of images. Therefore, to compare the proportion of perturbations applied to input images in each experimental scenario, we used two full-reference image quality metrics: the mean square error (MSE) and the structural similarity index (SSIM). The outputs of these metrics are reported in Table 2.

Focusing on Fig. 6, the first chart in the first row, (row a), for the CASIA dataset (first two columns) shows that the attacker matching score on scenario i falls below the acceptance threshold (slightly above 0.9) from iteration 55 onwards even for a high-security threshold (FAR = 0.001) and ends at nearly 0.6 at iteration 180. Similarly, for the next four rows on the same column, cancelable biometrics applying Gaussian noise, Laplacian noise, spread, and imploding respectively, we can see that despite using these protection methods, the matching score plunges alike almost at iteration 100 below the threshold FAR = 0.001. However, this is not the case in the proposed OTB-morph method, (rows f and g), using both the LFW and Face mask lite dataset as random biometrics. The output indicates that the attacking matching score for the two scenarios of the proposed method plateaued above the threshold FAR = 0.001 after iteration 80. While the aforementioned score ends above 0.8 after 180 iterations on scenarios (vi-a and vi-b), it stands at 0.7 at best on scenario ii in the end. The proposed method withstands this iterative optimization attack in addition to offering better performance. If we focus now on the second column, it can be seen that the overlapping area of the impostor and genuine score distributions for the two scenarios of the proposed OTB-morph (Scenario vi-a (row d)) is smaller than in the other experimented cases. The same trends are seen for the case of the VGGFace2 (last two columns) although the attacker matching scores slightly go below the threshold for FAR < 0.001 in the case of the proposed method. Considering the first and third columns, the most apparent evolution that can be observed is the falling rate of the attacker matching score. While for the first three rows, it decreases drastically to a low Euclidean distance (between 0.6 and 0.7), this pace is far slower for the proposed method, keeping the attacker matching score above 0.8 on both the CASIA and the VGGFace2 datasets. With regard to the score distributions for the VGGFace2 (last column), while the performance drop is not as severe as in the second column, the performance of the proposed method is still better compared to the other scenarios.

Comparing the first graph with the third one, in the second row (b), it can be seen that the matching score in the VGGFace2 graph falls more than that of CASIA. This finding shows that the CASIA is slightly more robust against the iterative optimization attack than the VGGFace2. The reason behind this difference is that our experimental ResNet-50 model was pretrained on the VGGFace2 dataset. Thus it works better since we picked subjects of morphing from the same dataset. In related works around adversarial samples, this variation is called transferability[55].

For the experiments reported in Fig. 7, note that the genuine and impostor distributions are more overlapped than before. This happens because our attack framework on ResNet-50 has been built upon TensorFlow in the previous version. Therefore, in order to have the same experimental condition in terms of our threat model, we had to use the TensorFlow implementation of the ArcFace[4] which is an unofficial version and does not perform as well as Oxford VGGFace implementation used for ResNet-50[5]. Despite the low performance of this ArcFace ver-

[4] https://github.com/peteryuX/arcface-tf2

[5] https://github.com/rcmalli/keras-vggface

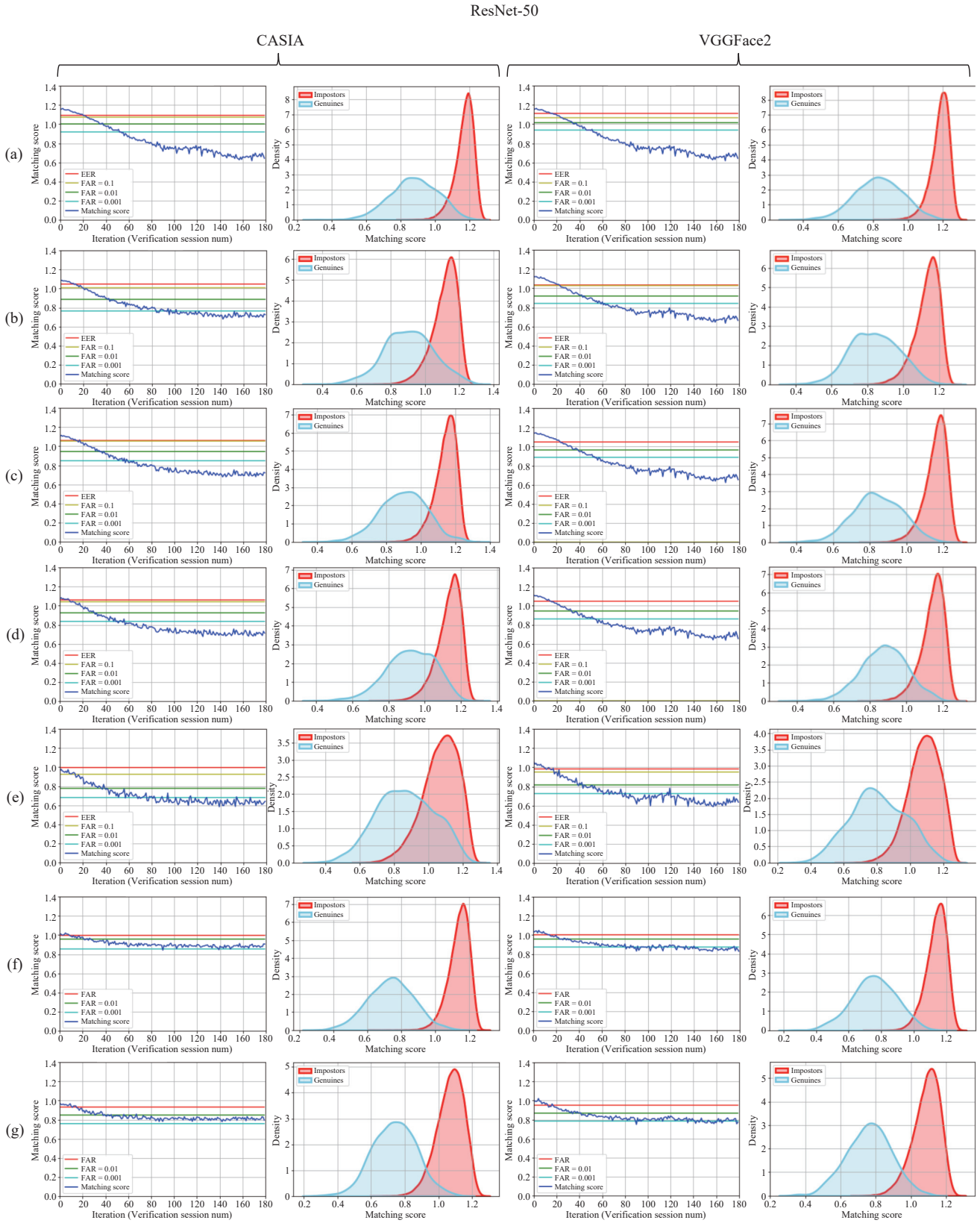


Fig. 6 Comparison of practiced scenarios on the ResNet-50 model: The first column is attacking matching (dissimilarity) score evolution on the CASIA dataset (positioned on top of decision thresholds at EER and various FAR). The second column is the genuine and random impostor distributions of the seven considered cancelable biometrics approaches on the CASIA dataset corresponding to different rows. Rows represent different scenarios: (a) Without applying cancelable biometrics; (b) Applying Gaussian noise; (c) Applying Laplacian noise; (d) Applying spreading; (e) Applying imploding; (f) Applying the proposed OTB-morph scheme using the LFW dataset as random biometric; (g) Applying the proposed OTB-morph scheme using Face Mask Lite dataset as random biometric. Third and fourth columns: Idem on VGGFace2 dataset.

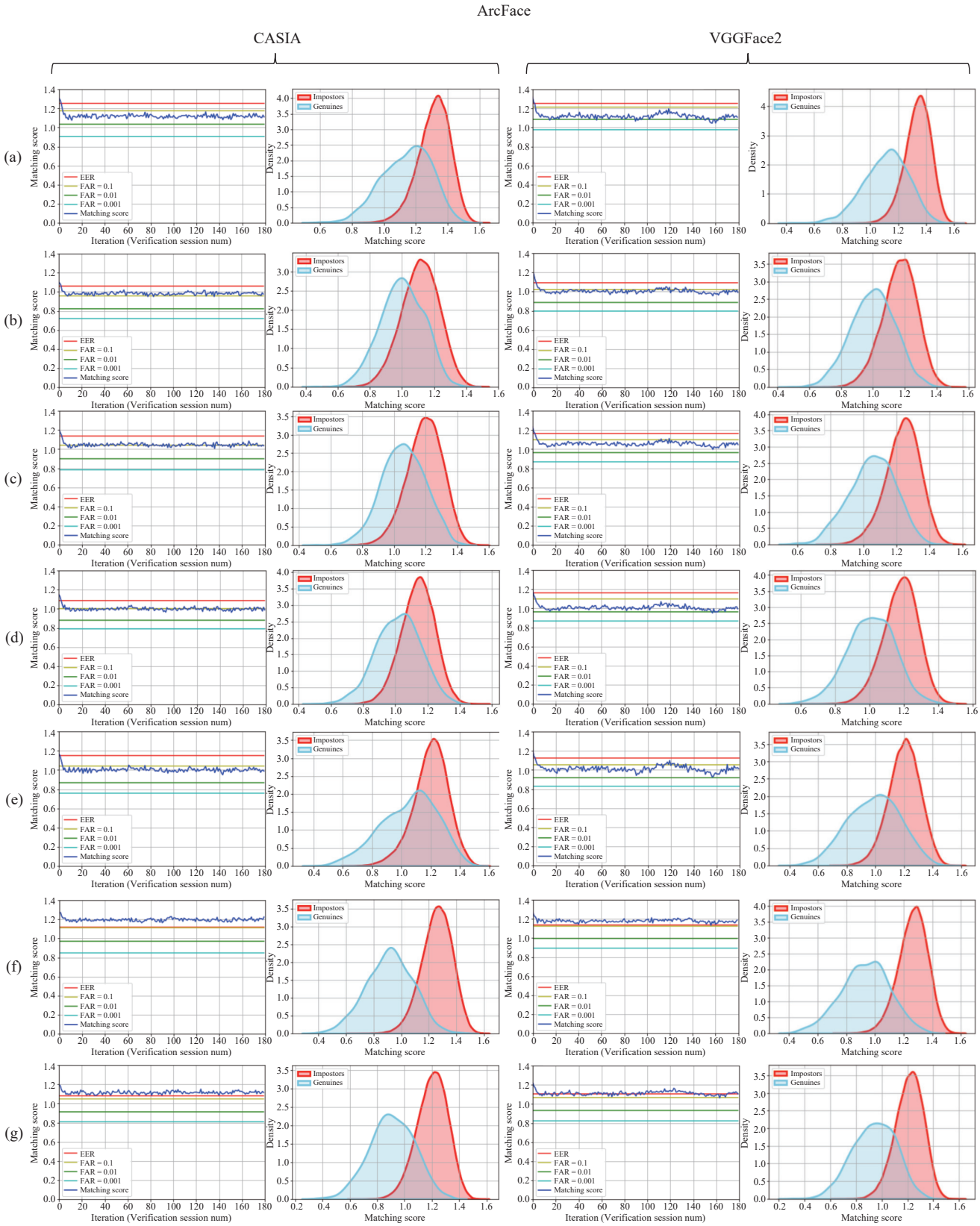


Fig. 7 Comparison of practiced scenarios on ArcFace model: Descriptions are the same as the caption in Fig. 6

sion, the results follow the same pattern as those of ResNet-50. The falling rate of the attacker matching score in the first five scenarios for both CASIA and VGGFace2 datasets (first and third columns, rows (a)–(e) are double

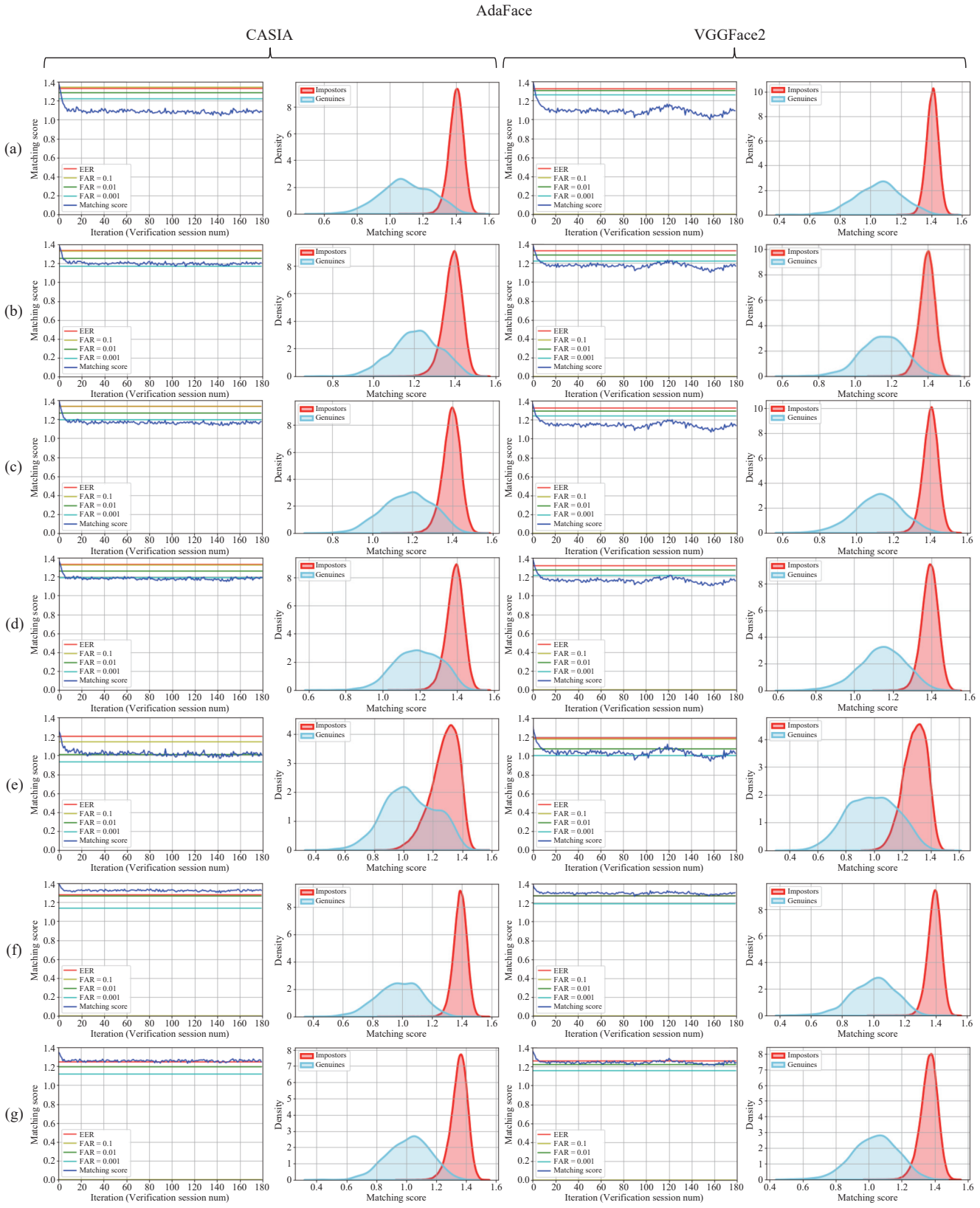


Fig. 8 Comparison of practiced scenarios on AdaFace model: Descriptions are the same as the caption in Fig. 6

that of the proposed method in the first 10 iterations. In addition, it can be seen in the same graphs that the attacker matching score falls below the threshold FAR = 0.1 for other scenarios except for the proposed ones which remained above the EER threshold.

Regarding AdaFace, we also had to use an unofficial

Table 2 Rate of perturbations applied to images in each experimented scenario. MSE stands for the mean square error (the lower the value, the more similar the perturbed image is to the original image), SSIM stands for the structural similarity index value (ranging between –1 and 1) where 1 means a perfect match between the perturbed image and the original image.

Metric	Scenarios					
	ii) Gaussian noise	iii) Laplacian noise	iv) Spread transformation	v) Imploding transformation	vi-a) OTB	vi-b) OTB
MSE	712.48	361.78	493.52	464.07	1 785	2 830
SSIM	0.21	0.30	0.23	0.58	0.20	0.13

version[6] implemented in TensorFlow but contrary to the ArcFace it performs very well. The corresponding results are depicted in Fig. 8. From the charts in the first and the third column, it is evident that while the attacker matching score for the proposed scenarios stands above EER, in all other scenarios, it falls either below FAR = 0.001 or oscillates between FAR = 0.01 and FAR = 0.001. Taking into account the performance results of the practiced methods demonstrated in the second and fourth columns in all these graphs, the superiority of the proposed method in terms of decreasing the overlapping region of the impostor and genuine score distributions while offering a higher protection rate is noticeable.

Additionally, we reported both EER and FRR values, as well as ASR against the attackers described in Section 3, for FAR = $\{0.1, 0.01, 0.001\}$ with respect to ResNet-50, ArcFace and AdaFace models in Tables 3–5, respectively. Starting with Table 3, we can see that the smallest EER and FRR values are obtained by the proposed method (Scenarios vi-a and vi-b) whereas the highest value (worst performance) is mainly reported on imploding (Scenario v) for both CASIA and VGGFace2. On the other hand, while the ASR for spread (Scenario iv) at EER and FAR = 0.1 on CASIA are above the values of other scenarios, the first scenario (unprotected biometric system) reported the highest ASR in both datasets overall. Out of the seven scenarios, although Gaussian noise (Scenario ii) performed very poorly for CASIA at FAR = 0.01 with the corresponding FRR = 67.9%, the reported FRR results for imploding are worse than all other scenarios in both datasets. Conversely, the proposed method acquired the best performance with FRR = 0.8% at FAR = 0.1 in both CASIA and VGGFace2.

In terms of ASR, while the highest percentage on CASIA (94%) belongs to Scenario iv at the EER point, on VGGFace2 it can be seen in Scenario at the EER with 90.3%. Regarding the proposed method, we observed that there is not much difference for ASR at the EER point between all scenarios because the attacker matching score plummets rapidly in some first iterations regardless of the protection method. However, the proposed method decreases the falling rate noticeably as the corresponding values for the ASR on Scenarios vi-a and vi-b at the FAR = 0.001 point are 28.2% and 23% on CASIA and 41.9% and 34.1% on VGGFace2, respectively. The reason we did not report the ASR for FAR = 0.1 in some scenarios is that the EER is higher than the FRR at FAR = 0.1.

Considering Table 4 we can observe that the results for the performance differ between CASIA and VGGFace2. Although the worst performance is observed in Scenario ii, Scenario v is almost as inferior as the former. Concerning ASR, the proposed method withstands the iterative optimization attack better while offering higher performance compared to all the other scenarios. Specifically, the ASR values at the EER point for both scenarios of the proposed method are all below 50%: 19.2% and 36.4% on CASIA and 31.7% and 48.6% on VGGFace2. These results are achieved where none of the other scenarios performed better than 80% at the same threshold.

Finally, with respect to the AdaFace, the results convey the same understanding as the previous tables. It can be seen that not only the proposed methods perform best, but also cancelable biometrics generated by this approach are further protective keeping the ASR less than 60% at the EER point where it stands above 90% for other scenarios at the corresponding setting. These results show the superiority of OTB-morph compared to related methods both for security protection and recognition performance.

5.4 Limitations

Despite the advantages that the proposed method introduces to biometric template protection methods in terms of higher performance and lower attack success rate against leakage attacks, there are some limitations that need to be taken into account:

1) The proposed method requires the acquisition of a reference face in each authentication session, which is computationally more expensive than other cancelable methods that change the reference once in a while or upon the leakage.

2) The proposed method might be slower than other cancelable approaches as it imposes morphing in each authentication attempt.

3) The proposed method requires a random face image to carry out the morphing in each authentication attempt. This random image can be produced by generat-

[6] https://github.com/leondgarse/Keras_insightface

Table 3 Comparison of the performance and security of the proposed method using LFW dataset as random biometric (Scenario iv-a) and using Face Mask Lite dataset (Scenario iv-b) with other scenarios on ResNet-50 model

Scenario	CASIA[46]				VGGFace2[45]			
	EER, ASR	FRR, ASR			EER, ASR	FRR, ASR		
		FAR = 0.1	FAR = 0.01	FAR = 0.001		FAR = 0.1	FAR = 0.01	FAR = 0.001
i)	6.6%, 88%	4.6%, 85.7%	18.9%, 76.5%	37.8%, 66%	3.68%, 90.3%	1.8%, 84.9%	8.7%, 78.2%	22.4%, 67.9%
ii)	16.6%, 90.3%	23.2%, 86.1%	67.9%, 12.8%	84%, 43.9%	8.8%, 86.3%	7.2%, 85.5%	28.4%, 71.2%	49.4%, 57.5%
iii)	11.29%, 89%	12.4%, 90%	37%, 75.4%	64%, 59.7%	5.7%, 84.5%	3.5%, –	17.7%, 74.7%	37.6%, 63%
iv)	14.97%, 94%	20%, 91%	50%, 76%	74.5%, 60%	8.6%, 89%	7.7%, –	30%, 76%	56.7%, 63.5%
v)	23.6%, 93.4%	37.1%, 86.3%	68.2%, 66.8%	86.3%, 51.4%	16.45%, 88.6%	22.1%, 84.2%	46%, 65.7%	67.5%, 50.6%
vi-a)	2.69%, 86%	0.8%, –	4.8%, 71.3%	19.5%, 28.2%	3.11%, 86.4%	0.8%, –	7.3%, 73.6%	19.8%, 41.9%
vi-b)	6.29%, 85%	4.3%, –	20.4%, 57.9%	44.6%, 23%	6%, 87.3%	4.1%, –	19.3%, 64.8%	43.8%, 34.1%

Table 4 Comparison of the performance and security of the proposed method using the LFW dataset as random biometric (Scenario iv-a) and using the Face Mask Lite dataset (Scenario iv-b) with other Scenarios on the ArcFace model

Scenario	CASIA[46]				VGGFace2[45]			
	EER, ASR	FRR, ASR			EER, ASR	FRR, ASR		
		FAR = 0.1	FAR = 0.01	FAR = 0.001		FAR = 0.1	FAR = 0.01	FAR = 0.001
i)	25.79%, 88.3%	44.3%, 70.4%	74.3%, 24.1%	93%, 2.5%	18.3%, 88.2%	26.8%, 78.5%	58.1%, 39.6%	79.3%, 13%
ii)	32.7%, 80.1%	62.8%, 39.9%	89.5%, 4.1%	97.6%, 0.1%	24.7%, 81.8%	44.9%, 56.6%	77.7%, 12.6%	92.3%, 1.8%
iii)	29.7%, 82.8%	54.4%, 50%	87.8%, 6.9%	97.2%, 0.3%	22.46%, 84.3%	39%, 65.7%	74.6%, 20%	89.5%, 0.4%
iv)	30.9%, 82.4%	55.3%, 51.8%	84%, 12%	94.6%, 1.7%	23.64%, 94%	41%, 82%	74%, 33.4%	90.4%, 10%
v)	32.37%, 87.7%	56.1%, 63.4%	80.9%, 16.5%	92.2%, 2.5%	24.14%, 80.2%	37%, 62.9%	63.8%, 24.9%	79.1%, 8.6%
vi-a)	11.59%, 19.2%	12.3%, 16.1%	37.5%, 0.5%	66.1%, 0.0%	11.3%, 31.7%	12.5%, 28.4%	37%, 2.5%	59.5%, 0.0%
vi-b)	14.9%, 36.4%	19.9%, 25.7%	48.3%, 1.9%	72.6%, 0.1%	16.79%, 48.6%	24.5%, 32.6%	53.4%, 2.7%	74.4%, 0.1%

Table 5 Comparison of the performance and security of the proposed method using the LFW dataset as random biometric (Scenario iv-a) and using the Face Mask Lite dataset (Scenario iv-b) with other scenarios on the AdaFace model

Scenario	CASIA[46]				VGGFace2[45]			
	EER, ASR	FRR, ASR			EER, ASR	FRR, ASR		
		FAR = 0.1	FAR = 0.01	FAR = 0.001		FAR = 0.1	FAR = 0.01	FAR = 0.001
i)	6.65%, 98.3%	5.3%,–	12.2%, 95.6%	22.7%, 88.6%	3.0%, 98%	1.5%, –	4.7%, 96.6%	8.5%, 91.5%
ii)	14.29%, 95.6%	17.1%, 94.2%	34.6%, 75.8%	63.28%, 36%	6.07%, 95.4%	4.5%, –	12.9%, 88.1%	29%, 69.7%
iii)	10.04%, 97%	10.0%, 96.9%	24.5%, 87.2%	46.05%, 63.2%	4.36%, 96.8%	2.7%, –	8.4%, 92.7%	15.8%, 82.6%
iv)	12.95%, 96.2%	14.7%, 95.18%	30.76%, 82.2%	49.4%, 55.1%	6.24%, 96%	4.8%, –	13.6%, 88.35%	28.6%, 70.6%
v)	21.33%, 91.6%	30%, 83.3%	54.8%, 51.1%	71.7%, 27%	13.44%, 89.82%	15.7%, 87.1%	33%, 65.6%	47.1%, 41.9%
vi-a)	1.4%, 17.3%	0.2%,–	1.8%, 13%	13.3%, 0.0%	1.09%, 31.3%	0.2%, –	1.1%, 30%	7.2%, 3.8%
vi-b)	4.1%, 42%	2.1%, –	9.5%, 16.5%	24.4%, 1.4%	3.7%, 59.2%	1.9%, –	8.2%, 36%	19.3%, 10.35%

ive networks. However, our experiments indicated that the highest protection will be achievable when the dissimilarity of the new random face is at the highest compared to its predecessors.

6 Conclusions

This work has extended our experiments on our introduced cancelable biometric method which can be categorized as a branch of visual cryptography with the aim of

protecting the biometric templates of clients against all kinds of leakage attacks. The original idea is to adopt the concept of the one-time-pad method to biometrics by using random biometrics as auxiliary data in a cancelable biometrics scheme called OTB-morph. To this end, we used morphing as the transformation function to generate an image that embodies two different identities. We then experimented with the proposed idea using a practical implementation for face biometrics. In the reported experiments we used a morphing algorithm based on Dlib and OpenCV for generating the cancelable templates. With respect to previously reported preliminary results[14], the present archival paper presents and discusses extended experiments by: increasing the number of iterations for the iterative optimization attacks, using GAN-generated faces as another mean for random biometric generation, and using pre-trained ArcFace and AdaFace models for additional evaluation. In conclusion, the proposed method improves both the biometric performance and security against the evaluated attacks.

In our future work, our main goal is to investigate how we can maximize the distance between two one-time biometrics of the same individual in subsequent sessions so that we can offer the lowest ASR in case of iterative optimization. Particularly, we would like to explore how a random biometric with opposite features to the given subject (e.g., ethnicity, skin color, age, sex, and other facial attributes) can help us to meet our goal.

Acknowledgements

This work was supported by PRIMA (No. H2020-MSCA-ITN-2019-860315), TRESPASS-ETN (No. H2020-MSCA-ITN-2019-860813), BBforTAI (No. PID2021-127641OB-I00 MICINN/FEDER), and INTER-ACTION (No. PID2021-126521OB-I00 MICINN/FEDER). M. Ghafourian was supported by PRIMA and I. Serna was supported by an FPI fellowship from University Autonoma de Madrid, Spain.

Declarations of conflict of interest

The authors declared that they have no conflicts of interest to this work.

References

[1] J. Fierrez, A. Morales, J. Ortega-Garcia. Biometrics security. *Encyclopedia of Cryptography, Security and Privacy*, S. Jajodia, P. Samarati, M. Yung, Eds., Berlin, Heidelberg, Germany: Springer, pp. 1–3, 2021. DOI: 10.1007/978-3-642-27739-9_1603-1.

[2] G. Jaswal, V. Kanhangad, R. Ramachandra. *AI and Deep Learning in Biometric Security: Trends, Potential, and Challenges*, Boca Raton, USA: CRC Press, 2021.

[3] M. R. Freire, J. Fierrez, J. Galbally, J. Ortega-Garcia. Biometric hashing based on genetic selection and its application to on-line signatures. In *Proceedings of International Conference on Biometrics*, Springer, Seoul, Republic of Korea, pp. 1134–1143, 2007. DOI: 10.1007/978-3-540-74549-5_118.

[4] M. Gomez-Barrero, J. Galbally, A. Morales, J. Fierrez. Privacy-preserving comparison of variable-length data with application to biometric template protection. *IEEE Access*, vol. 5, pp. 8606–8619, 2017. DOI: 10.1109/ACCESS.2017.2691578.

[5] K. Nandakumar, A. K. Jain. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015. DOI: 10.1109/MSP.2015.2427849.

[6] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, J. Fierrez. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognition*, vol. 67, pp. 149–163, 2017. DOI: 10.1016/j.patcog.2017.01.024.

[7] Q. Li, Z. N. Sun, R. He, T. N. Tan. Deep supervised discrete hashing. In *Proceedings of the 31st International Conference on Neural Information Processing Systems*, Long Beach, USA, pp. 2479–2488, 2017.

[8] M. Ghafourian, B. Sumer, R. Vera-Rodriguez, J. Fierrez, R. Tolosana, A. Moralez, E. Kindt. Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis, [Online], Available: https://arxiv.org/abs/2302.10883, 2023.

[9] V. M. Patel, N. K. Ratha, R. Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015. DOI: 10.1109/MSP.2015.2434151.

[10] Manisha, N. Kumar. Cancelable biometrics: A comprehensive survey. *Artificial Intelligence Review*, vol. 53, no. 5, pp. 3403–3446, 2020. DOI: 10.1007/s10462-019-09767-8.

[11] S. M. Bellovin. Frank miller: Inventor of the one-time pad. *Cryptologia*, vol. 35, no. 3, pp. 203–222, 2011. DOI: 10.1080/01611194.2011.583711.

[12] J. C. Neves, R. Tolosana, R. Vera-Rodriguez, V. Lopes, H. Proença, J. Fierrez. GANprintR: Improved fakes and evaluation of the state of the art in face manipulation detection. *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 1038–1048, 2020. DOI: 10.1109/JSTSP.2020.3007250.

[13] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch. Face recognition systems under morphing attacks: A survey. *IEEE Access*, vol. 7, pp. 23012–23026, 2019. DOI: 10.1109/ACCESS.2019.2899367.

[14] M. Ghafourian, J. Fierrez, R. Vera-Rodriguez, I. Serna, A. Morales. OTB-morph: One-time biometrics via morphing applied to face templates. In *Proceedings of IEEE/CVF Winter Conference on Applications of Computer Vision Workshops*, IEEE, Waikoloa, USA, pp. 321–329, 2022. DOI: 10.1109/WACVW54805.2022.00038.

[15] N. K. Ratha, J. H. Connell, R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634,

2001. DOI: 10.1147/sj.403.0614.

[16] A. T. B. Jin, D. N. C. Ling, A. Goh. BioHashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004. DOI: 10.1016/j.patcog.2004.04.011.

[17] R. Ang, R. Safavi-Naini, L. McAven. Cancelable key-based fingerprint templates. In *Proceedings of the 10th Australasian Conference on Information Security and Privacy*, Springer, Brisbane, Australia, pp. 242–252, 2005. DOI: 10.1007/11506157_21.

[18] C. Lee, J. Y. Choi, K. A. Toh, S. Lee, J. Kim. Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics – Part B (Cybernetics)*, vol. 37, no. 4, pp. 980–992, 2007. DOI: 10.1109/TSMCB.2007.896999.

[19] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007. DOI: 10.1109/TPAMI.2007.1004.

[20] F. Quan, S. Fei, C. Anni, Z. Feifei. Cracking cancelable fingerprint template of Ratha. In *Proceedings of International Symposium on Computer Science and Computational Technology*, IEEE, Shanghai, China, pp. 572–575, 2008. DOI: 10.1109/ISCSCT.2008.226.

[21] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, A. Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, vol. 40, no. 3, pp. 525–538, 2010. DOI: 10.1109/TSMCA.2010.2041653.

[22] O. Ouda, N. Tsumura, T. Nakaguchi. Tokenless cancelable biometrics scheme for protecting iris codes. In *Proceedings of the 20th International Conference on Pattern Recognition*, IEEE, Istanbul, Turkey, pp. 882–885, 2010. DOI: 10.1109/ICPR.2010.222.

[23] J. K. Pillai, V. M. Patel, R. Chellappa, N. K. Ratha. Sectored random projections for cancelable iris biometrics. In *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, Dallas, USA, pp. 1838–1841, 2010. DOI: 10.1109/ICASSP.2010.5495383.

[24] M. Ferrara, D. Maltoni, R. Cappelli. Noninvertible minutia cylinder-code representation. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1727–1737, 2012. DOI: 10.1109/TIFS.2012.2215326.

[25] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, J. Fierrez. Unlinkable and irreversible biometric template protection based on Bloom filters. *Information Sciences*, vol. 370–371, pp. 18–32, 2016. DOI: 10.1016/j.ins.2016.06.046.

[26] M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez, C. Busch. Protected facial biometric templates based on local Gabor patterns and adaptive bloom filters. In *Proceedings of the 22nd International Conference on Pattern Recognition*, IEEE, Stockholm, Sweden, pp. 4483–4488, 2014. DOI: 10.1109/ICPR.2014.767.

[27] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, J. Fierrez. Towards cancelable multi-biometrics based on bloom filters: A case study on feature level fusion of face and iris. In *Proceedings of the 3rd International Workshop on Biometrics and Forensics*, IEEE, Gjovik, Norway, 2015. DOI: 10.1109/IWBF.2015.7110225.

[28] Y. J. Chin, T. S. Ong, A. B. J. Teoh, K. O. M. Goh. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion*, vol. 18, pp. 161–174, 2014. DOI: 10.1016/j.inffus.2013.09.001.

[29] Y. L. Lai, Z. Jin, A. B. J. Teoh, B. M. Goi, W. S. Yap, T. Y. Chai, C. Rathgeb. Cancellable iris template generation based on indexing-first-one hashing. *Pattern Recognition*, vol. 64, pp. 105–117, 2017. DOI: 10.1016/j.patcog.2016.10.035.

[30] D. Sadhya, B. Raman. Generation of cancelable iris templates via randomized bit sampling. *IEEE Transactions on Information Forensics and*, vol. 14, no. 11, pp. 2972–2986, 2019. DOI: 10.1109/TIFS.2019.2907014.

[31] S. Kirchgasser, C. Kauba, A. Uhl. Cancellable biometrics for finger vein recognition-application in the feature domain. *Handbook of Vascular Biometrics*, A. Uhl, C. Busch, S. Marcel, R. Veldhuis, Eds., Cham, Germany: Springer, pp. 481–506, 2020. DOI: 10.1007/978-3-030-27731-4_16.

[32] S. Kirchgasser, A. Uhl, Y. Martinez-Diaz, H. Mendez-Vazquez. Is warping-based cancellable biometrics (still) sensible for face recognition? In *Proceedings of IEEE International Joint Conference on Biometrics*, Houston, USA, pp. 1–9, 2020. DOI: 10.1109/IJCB48548.2020.9304870.

[33] I. S. Badr, A. G. Radwan, E. S. M. El-Rabaie, L. A. Said, G. M. El Banby, W. El-Shafai, F. E. A. El-Samie. Cancellable face recognition based on fractional-order Lorenz chaotic system and HAAR wavelet fusion. *Digital Signal Processing*, vol. 116, Article number 103103, 2021. DOI: 10.1016/J.DSP.2021.103103.

[34] X. B. Dong, S. Cho, Y. Kim, S. Kim, A. B. J. Teoh. Deep rank hashing network for cancellable face identification. *Pattern Recognition*, vol. 131, Article number 108886, 2022. DOI: 10.1016/J.PATCOG.2022.108886.

[35] D. Chang, S. Garg, M. Hasan, S. Mishra. Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption. *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3152–3167, 2020. DOI: 10.1109/TIFS.2020.2983250.

[36] J. Galbally. A new Foe in biometrics: A narrative review of side-channel attacks. *Computers & Security*, vol. 96, Article number 101902, 2020. DOI: 10.1016/j.cose.2020.101902.

[37] J. Galbally, S. Carballo, J. Fierrez, J. Ortega-Garcia. Vulnerability assessment of fingerprint matching based on time analysis. In *Proceedings of the European Workshop on Biometrics and Identity Management*, Springer, Madrid, Spain, pp. 285–292, 2009. DOI: 10.1007/978-3-642-04391-8_37.

[38] L. G. Zhu, S. Han. Deep leakage from gradients. In *Federated Learning*, Q. Yang, L. X. Fan, H. Yu, Eds., Cham, Germany: Springer, pp. 17–31, 2020. DOI: 10.1007/978-3-

030-63076-8_2.

[39] J. Galbally, C. McCool, J. Fierrez, S. Marcel, J. Ortega-Garcia. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition*, vol. 43, no. 3, pp. 1027–1038, 2010. DOI: 10.1016/j.patcog.2009.08.022.

[40] M. Gomez-Barrero, J. Galbally, J. Fierrez. Efficient software attack to multimodal biometric systems and its application to face and iris fusion. *Pattern Recognition Letters*, vol. 36, pp. 243–253, 2014. DOI: 10.1016/j.patrec.2013.04.029.

[41] M. Gomez-Barrero, J. Galbally, J. Fierrez, J. Ortega-Garcia. Face verification put to test: A hill-climbing attack based on the uphill-simplex algorithm. In *Proceedings of the 5th IAPR International Conference on Biometrics*, IEEE, New Delhi, India, pp. 40–45, 2012. DOI: 10.1109/ICB.2012.6199756.

[42] M. Ghafoorian, D. Abbasinezhad-Mood, H. Shakeri. A thorough trust and reputation based RBAC model for secure data storage in the cloud. *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 4, pp. 778–788, 2019. DOI: 10.1109/TPDS.2018.2870652.

[43] M. Ghafoorian, M. Nikooghadam. An anonymous and secure key agreement protocol for NFC applications using pseudonym. *Wireless Networks*, vol. 26, no. 6, pp. 4269–4285, 2020. DOI: 10.1007/s11276-020-02319-x.

[44] R. Tolosana, P. Delgado-Santos, A. Perez-Uribe, R. Vera-Rodriguez, J. Fierrez, A. Morales. DeepWriteSYN: Online handwriting synthesis via deep short-term representations. In *Proceedings of the 35th AAAI Conference on Artificial Intelligence*, Palo Alto, USA, pp. 600–608, 2021. DOI: 10.1609/aaai.v35i1.16139.

[45] Q. Cao, L. Shen, W. D. Xie, O. M. Parkhi, A. Zisserman. VGGFace2: A dataset for recognising faces across pose and age. In *Proceedings of the 13th IEEE International Conference on Automatic Face & Gesture Recognition*, Xi'an, China, pp. 67–74, 2018. DOI: 10.1109/FG.2018.00020.

[46] D. Yi, Z. Lei, S. C. Liao, S. Z. Li. Learning face representation from scratch, [Online], Available: https://arxiv.org/abs/1411.7923, 2014.

[47] E. Gonzalez-Sosa, J. Fierrez, R. Vera-Rodriguez, F. Alonso-Fernandez. Facial soft biometrics for recognition in the wild: Recent works, annotation, and COTS evaluation. *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2001–2014, 2018. DOI: 10.1109/TIFS.2018.2807791.

[48] G. B. Huang, M. Mattar, T. Berg, E. Learned-Miller. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. In *Proceedings of Workshop on Faces in "Real-Life" Images: Detection, Alignment, and Recognition*, Marseille, France, 2008.

[49] K. M. He, X. Y. Zhang, S. Q. Ren, J. Sun. Deep residual learning for image recognition. In *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*, Las Vegas, USA, pp. 770–778, 2016. DOI: 10.1109/CVPR.2016.90.

[50] J. K. Deng, J. Guo, N. N. Xue, S. Zafeiriou. ArcFace: Additive angular margin loss for deep face recognition. In *Proceedings of IEEE/CVF Conference on Computer Vision and Pattern Recognition*, IEEE, Long Beach, USA, pp. 4685–4694, 2019. DOI: 10.1109/CVPR.2019.00482.

[51] M. Kim, A. K. Jain, X. M. Liu. AdaFace: Quality adaptive margin for face recognition. In *Proceedings of IEEE/CVF Conference on Computer Vision and Pattern Recognition*, IEEE, New Orleans, USA, pp. 18729–18738, 2022. DOI: 10.1109/CVPR52688.2022.01819.

[52] H. W. Zhang, Q. Li, Z. N. Sun, Y. F. Liu. Combining data-driven and model-driven methods for robust facial landmark detection. *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2409–2422, 2018. DOI: 10.1109/TIFS.2018.2800901.

[53] U. Scherhag, D. Fischer, S. Isadskiy, J. Otte, C. Busch. Morphing attack detection using laplace operator based features. *Norsk IKT-Konferanse for Forskning Og Utdanning*, no. 3, 2020.

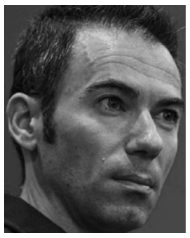
[54] S. Venkatesh, R. Ramachandra, K. Raja, C. Busch. Face morphing attack generation and detection: A comprehensive survey. *IEEE Transactions on Technology and Society*, vol. 2, no. 3, pp. 128–145, 2021. DOI: 10.1109/TTS.2021.3066254.

[55] M. Ghafourian, J. Fierrez, L. F. Gomez, R. Vera-Rodriguez, A. Morales, Z. Rezgui, R. Veldhuis. Toward face biometric de-identification using adversarial examples, [Online], Available: https://arxiv.org/abs/2302.03657, 2023.

Mahdi Ghafourian received the B. Sc. degree in computer science from the Islamic Azad University of Mashhad, Iran in 2011, and the M. Sc. degree in information security and assurance from the Imam Reza University, Iran in 2016. He achieved the second position among top Master's degree graduates. In 2021, he started the Ph.D. with Marie Curie scholarship within the EU ITN project PriMa (Privacy Matters) in the Biometrics and Data Pattern Analytics Laboratory – BiDA-Lab, at the Universidad Autonoma de Madrid, Spain.

His research interests include information security, biometrics protection, face recognition, adversarial examples and federated learning.

E-mail: mahdi.ghafourian@uam.es (Corresponding author)
ORCID iD: 0000-0003-4206-4873



Julian Fierrez received the M. Sc. and the Ph. D. degrees in telecommunications engineering from Universidad Politecnica de Madrid, Spain in 2001 and 2006, respectively. Since 2004, he is at Universidad Autonoma de Madrid, Spain where he is associate professor since 2010. He is Associate Editor for *Information Fusion*, *IEEE Transactions on Information Forensics and Security*, and *IEEE Transactions on Image Processing*. He has received best papers awards at AVBPA, ICB, IJCB, ICPR, ICPRS, and Pattern Recognition Letters; and several research distinctions, including: EBF European Biometric Industry Award

2006, EURASIP Best Ph. D. Award 2012, Miguel Catalan Award to the Best Researcher under 40 in the Community of Madrid in the general area of Science and Technology, and the IAPR Young Biometrics Investigator Award 2017. Since 2020, he is member of the ELLIS Society.

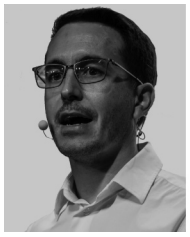
His research interests include signal and image processing, AI fundamentals and applications, HCI, forensics, and biometrics for security and human behavior analysis.

E-mail: julian.fierrez@uam.es

Ruben Vera-Rodriguez received the M. Sc. degree in telecommunications engineering from Universidad de Sevilla Spain, Spain in 2006, and the Ph. D. degree in electrical and electronic engineering from Swansea University, UK in 2010. Since 2010, he has been affiliated with the Biometric Recognition Group, Universidad Autonoma de Madrid, Spain, where he is currently an associate professor since 2018. Ruben has published over 100 scientific articles published in international journals and conferences. He is actively involved in several National and European projects focused on biometrics. He has been Program Chair for the *51st IEEE International Carnahan Conference on Security and Technology* (ICCST) in 2017; *the 23rd Iberoamerican Congress on Pattern Recognition* (CIARP 2018) in 2018; *and the International Conference on Biometric Engineering and Applications* (ICBEA 2019) in 2019.

His research interests include signal and image processing, pattern recognition, HCI, and biometrics, with emphasis on signature, face, gait verification and forensic applications of biometrics.

E-mail: ruben.vera@uam.es



Aythami Morales received the M. Sc. degree in electrical engineering from Universidad de Las Palmas de Gran Canaria, Spain in 2006, the Ph. D. degree in artificial intelligence from La Universidad de Las Palmas de Gran Canaria, Spain in 2011. Since 2017, he is an associate professor with the Universidad Autonoma de Madrid, Spain.

His interests include machine learning, biometric processing, security and privacy.

E-mail: aythami.morales@uam.es

Ignacio Serna received the B. Sc. degree in mathematics and the B. Sc. degree in computer science from the Autonomous University of Madrid, Spain in 2018, and the M. Sc. degree in artificial intelligence from the Autonomous University of Madrid, Spain in 2020. He is currently a Ph. D. degree candidate in computer science at the BiDA-Lab, Spain.

His research interests include computer vision, pattern recognition and explainable AI, with applications to biometric.

E-mail: ignacio.serna@uam.es