Face Morphing Attacks: A Threat to eLearning?

Christian Rathgeb, Katrin Pöppelmann and Christoph Busch
da/sec – Biometrics and Internet Security Research Group
Hochschule Darmstadt, Germany
{christian.rathgeb,christoph.busch}@h-da.de

2021 IEEE Global Engineering Education Conference (EDUCON) | 978-1-7281-8478-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/EDUCON46332.2021.9454128

***Abstract*—Recently, the use of remote education via electronic media, i.e. eLearning, has increased due to the COVID-19 pandemic. To achieve secure and reliable identity verification in eLearning exams, it has been suggested to employ face recognition technologies for remote student authentication in online examinations. However, novel attacks on face recognition in eLearning systems have rarely been considered in the scientific literature.**

In this work, we investigate the feasibility of so-called face morphing attacks in eLearning systems. Such attacks can be launched in scenarios where students are authenticated via identity documents containing face images that are remotely presented prior to online examinations. In this relevant scenario, students are able to fool human examination and automated face recognition by morphing their face image with that of an accomplice, e.g. fellow student. Resulting morphed face images contain biometric information of both subjects contributing to it. Consequentially, an accomplice could take part in an online examination for a student with high probability of passing an identity verification unnoticed. We assess the vulnerability of a commercial and an open-source face recognition system to said attack. To this end, a realistic dataset of morphing attacks is collected. It is shown that automated face recognition in eLearning systems can be tricked with alarmingly high success chance.

***Index Terms*—eLearning, remote education, online examination, biometrics, face recognition, morphing attack**

I. Introduction

eLearning systems are currently employed for educational purposes in academia and industry [1]. They enable effective online teaching in a wide range of application scenarios, where in many situations an authentication of students is required, *e.g.* in online examinations. In order to avoid misuse of eLearning systems by impersonation attacks and hence strengthen trust in online examination results, it has been suggested to apply biometric technologies for (continuous) identity verification [2]–[4] as well as further tasks such as emotion estimation.

Biometric recognition refers to automated recognition of individuals based on their biological characteristics, *e.g.* face, or behavioural characteristics, *e.g.* keystroke dynamics. In a biometric system, the biometric characteristic of a data subject is presented to the capture device and a biometric sample is acquired. This is done during registration, *i.e.* enrolment, and at the time of authentication. In order to compare a pair of biometric samples, pre-processing is applied, and features are extracted resulting in two biometric templates referred to as reference and probe templates. In some scenarios, reference and probe templates are extracted simultaneously from a provided identity document containing biometric data and a live capture, respectively, *e.g.* face recognition in automated border control. The similarity between two templates is estimated by the biometric comparator which computes a corresponding comparison score. Finally, a comparison score is compared against a decision threshold yielding acceptance or rejection.

Fig. 1. Remote authentication scenario with simultaneous presentation of a probe face and an identity document containing a reference face.

In the scientific literature, the incorporation of biometric technologies into eLearning systems is motivated by various use-cases including user login, user monitoring, attention estimation, emotion estimation, and authorship verification [2]. In this work, we focus on the first use-case in which a one-time face-based biometric verification is conducted to initially authenticate a subject, *e.g.* prior to an online examination. The use of face recognition in eLearning systems has been suggested by various researchers, *e.g.* in [5]–[7]. A main motivation for using the face for biometric authentication is that a subject's face can be captured using inbuilt or external webcams, *i.e.* specific hardware is not required.[1] More precisely, we consider the application of face recognition in a scenario where no (trusted) biometric reference data is available. That is, a user is required to simultaneously present an identity proof containing a face image, *e.g.* identity document, together with her/his face, see figure 1. Subsequently, biometric reference and probe samples are extracted form the identity document and the subject and the resulting templates are compared, similar to the aforementioned automated bor-

[1]Note that the same holds for other biometric characteristics such as voice and keystroke dynamics which can be captured with a microphone or a keyboard, respectively.

der control scenario. Due to the COVID-19 pandemic, the described scenario is of high relevance as students may not meet lecturers throughout courses.

In this work, we investigate the feasibility of attacking face recognition in online examinations considering the above mentioned authentication scenario. Attacks on biometric technologies used in eLearing systems have hardly been considered in related works, see section II. In detail, we focus on so-called morphing attacks [8], in which a manipulated (morphed) face image is incorporated into the identity proof which is presented during authentication. Morphed face images contain biometric information of two or more subjects as shown in figure 2. With high probability, subjects contributing to a morphed face image are successfully verified against it by human examiners as well as automated face recognition [8], [9]. In other words, it would be feasible for students to trick the face-based authentication process such that one student could take part in an online examination for the other student and vice versa, see section III. In order to empirically evaluate the feasibility of this type of attack, a dataset containing realistic face morphing attacks is created, see section IV. Subsequently, the success chance of the attacks is evaluated using standardised metrics, see section V. Finally, conclusions are drawn and mitigation methods are discussed, see section VI.

(a) Subject 1 (b) Morph (c) Subject 2

Fig. 2. Example of a manually created morphed face image (b) based on the face images of subject 1 (a) and subject 2 (c).

II. Related Work

A. Face Recognition in eLearning

First scientific works on the use of biometrics in eLearning have been presented in the early 2000s. So far various concepts on the application of biometric recognition in eLearning systems have been proposed. For a comprehensive overview on this topic, the interested reader is referred to a recent survey of Rathgeb *et al*. [2]. Numerous researchers recommended the use of face recognition technologies (in combination with other biometric systems) in eLearning systems.

González-Agulla *et al*. [5] proposed the use of face and speaker verification with the aim of improving the security in eLearning systems. Building on the approach in [5], a face-based continuous tracking and recognition system which is capable of measuring learning time as well as verifying subjects (and hence preventing from potential cheating) was introduced in [10]. Another continuous biometric verification system based on face recognition was presented in [11].

Rabuzin *et al*. [12] suggested the use of multi-biometric verification and argued that authentication based on a single biometric characteristic could cause security risks. Further approaches for (continuous) multi-biometric verification (including face recognition) in eLearning systems have been presented in [6], [13]–[15]. Many of the mentioned works, *e.g*. [12], restrict to proposing theoretical frameworks, *i.e*. practical implementations as well as experimental evaluations w.r.t. biometric performance are omitted. This certainly reduces the value of these works since practical biometric performance is vital to prevent from verification errors which in turn lower the usability and hence acceptability of biometric verification. It is important to note that the acceptability of biometric technologies in eLearning systems has only been considered by a few works, *e.g*. in [13], [16]. Authors of said works generally reported high user acceptability for the use of biometric recognition in eLearning.

Numerous researchers recommended a combination of biometric technologies analysing face, voice, mouse and keystroke dynamics [7], [17], [18]. Bhattacharjee *et al*. [19] additionally proposed the application of software-based presentation attack detection (also referred to as anti-spoofing) for face and voice which were developed in the EU-H2020 TeSLA project [20]. As mentioned earlier, said biometric characteristics allow for a cost-effective biometric verification since they can be captured with sensors which are likely to be embedded in the subjects' devices, *e.g*. camera, microphone, keyboard and mouse. On the contrary, some biometric characteristics, *e.g*. fingerprint or EEG signal, require special sensors.

In summary, several applications of face recognition in eLearning systems have been proposed in the scientific literature. However, none of these publications considers well-known attacks on face recognition, [19] being a notable exception.

B. Attacks on Face Recognition

Potential attack vectors against biometric systems were first established in [21]. Due to the fact that many biometric characteristics are not secret, in particular the face, so-called presentation attacks or "spoofing" attacks represent one of the most critical attack vectors against biometric systems [22]. In contrast to software-based attacks, no access to the internal modules of a biometric system is necessary to launch presentation attacks. The vulnerability of biometric systems with regard to presentation attacks has been confirmed by experts in the past years and published in international media [23].

Many efforts have been made towards robust and reliable presentation attack detection in the field of face recognition. Various research projects, *e.g*. EU-FP7 TABULA RASA [24] or IARPA Odin [25], have been conducted and numerous face presentation attack detection methods have been published in the scientific literature. For comprehensive surveys the reader is referred to [26], [27].

Image morphing techniques can be used to combine information from two (or more) images into one image. Morphing

techniques can also be used to create a morphed facial image from the biometric face images of two individuals, of which the biometric information is similar to that of both individuals. Morphed face images that look realistic and are of high image quality can be generated by unskilled users applying readily available tools [28]. A face morphing attack can be seen as special enrolment attack. In a morphing attack, two (similar looking) subjects could morph their face images and one of them applies for an identity document or manipulates an identity document with the morphed image. Since many morphed images are similar enough to deceive human examiners as well as automatic face recognition systems [9], [29], both subjects can then use the issued document to pass through face-based identity check. The vulnerability of automated face recognition systems against such morphing attacks was initially showcased in [8]. The potential to launch a face morphing attack in practice was demonstrated by members of the political activist group *Peng! Kollektiv*, who successfully applied for a passport with a morphed face image.[2]

In the recent past, different approaches to face morphing attack detection have been proposed by various research laboratories. The reader is referred to Scherhag *et al*. [28] for a comprehensive survey on this topic. In addition, different benchmarks [30], [31] have been conducted to compare the performance of different morphing detection methods which further underlines the importance of this type of attack.

III. Face Morphing Attack

In order to launch a face morphing attack in an eLearning system, a student has to perform several steps:

1) *Accomplice selection*: firstly, a rather lookalike accomplice, *e.g*. a fellow student, has to be found. The chance of a successful attack increases if both subjects share certain demographic properties including sex, age, and skintone. Subsequently, frontal face images are taken in similar environments which serve as basis for the following step.
2) *Morph creation*: in the second step, a face morph is generated, possibly by using free software available on the internet. Morphs can be created manually and retouching can be applied in order to reduce arefacts resulting from the morphing process. Face morphing usually involves the detection of corresponding facial landmarks, averaging and triangulation, as well as warping and alpha-blending [28]. Since both subjects should be successfully verified against the morph, equal weights should be put to both images during the morph creation. In other words, the morphed face should contain 50% of biometric information of both contributing face images.
3) *Morph infiltration*: in this step, the morphed face image has to be inserted into an identity document. Here, different scenarios could be taken into account:
    a) In case an official identity document, *e.g*. a passport, is required during authentication, a student may temporarily place the morphed face image on top of the original one. This might be done using adhesive foils. Obviously, a student may not want to forge an official document.
    b) If unofficial identity document, *e.g*. a student card, suffice for the authentication process, a student might even apply for such a document by submitting the morphed face image. In case the student is unknown, *i.e*. no trusted reference face image is available, or the two face images contributing to a high qulaity morph are similar enough, it is likely that the morphed image will be accepted [9].
4) *Morphing attack launch*: finally, the morphing attack is launched by showing the identity document containing the morphed face image during the identity verification process. The morphed face image is then compared against the simultaneously presented face of one of the contributing subjects using automated face recognition.

Fig. 3. Face morphing attack with simultaneous presentation of an identity document (containing a face morph) and a face.

An example of the considered face morphing attack is shown in figure 3. We argue that this attack is relevant in the context of identity verification in eLearning systems due to the following reasons:

- Morphing software is easy to obtain and many free mobile applications (apps) are available to create face morphs. Such apps allow for the creation of high quality morphs even by unskilled users.
- Deployments of eLearning systems are not expected to comprise attack detection modules for face recognition. On the contrary, the use of face recognition and face tracking is usually suggested as a means of preventing from cheating in eLearning systems.
- Checking the authenticity of identity documents which are presented to inbuilt cameras or webcams represents a challenging task. Moreover, authenticity checks of identity documents are expected to rarely be implemented in eLearing systems. That is, the forgery of identity documents becomes easier in such a scenario, in contrast

[2]Peng! Kollektiv, MaskID: https://pen.gg/de/campaign/maskid/

to scenarios where identity documents are checked on site.

Considering the described face morphing attack, a substitution of face images in identity documents might seem to be an even more effective way of attacking face recognition. However, focusing on eLearning such an attack would require that the depicted accomplice takes part in all examinations of a student. In other words, the flexibility of "sharing" a single identity document among two subjects is lost.

IV. Database

In order to test the feasibility of the described face morphing attack a number of 9 participants (6 female and 3 male) were asked to provide a face image which largely fulfills the ICAO requirements for electronic travel documents [32]. Additionally, a small subset of the public FERET face database [33] comprising ICAO compliant face images of 7 subjects (4 female and 3 males) was employed in order to increase the number of morphing attacks. Face images from the FERET database were selected in a way that these exhibit demographic attributes similar to at least one participant, *e.g.* sex or skin tone. Example images of both datasets are depicted in figure 4.

(a) FERET (b) collected database

Fig. 4. Example face images of both used datasets.

The proprietary morphing algorithm FaceFusion[3] was used to create morphed face images. Originally being an iOS app, we deployed an adaptation for Windows which uses the 68 facial landmarks and Delaunay triangulation. To avoid the artefacts in the area outside the face, morphing is only applied in the inner facial region and the outer facial region of the first face is maintained. Additionally, colours are adjusted at boundaries. After the morphing process, certain regions (eyes, nostrils, hair) of the first face image were blended over the morph to eliminate potential artefacts. The created morphs exhibit high quality and low to no visible artefacts. A total number of 102 face morphs was created from pairs of male and female subjects. Examples of morphed face images are shown as part of figure 5.

Subsequently, fake student identity cards including morphed and unaltered (bona fide) face images were created using a freely available identity document template, see figure 6. Participants were than asked to present different fake identity cards containing morphed as well as bona fide face images in an online conference platform and simultaneously show their face. Figure 7 depicts example of face images extracted from presented identity cards which are of noticeable lower quality.

[3]www.wearemoment.com/FaceFusion/

Fig. 5. Examples of created face morphs: original subjects contributing to the morph are depicted on the leftmost and rightmost columns; the two middle columns show the resulting morphs where the outer face region of either of the original subjects is used.

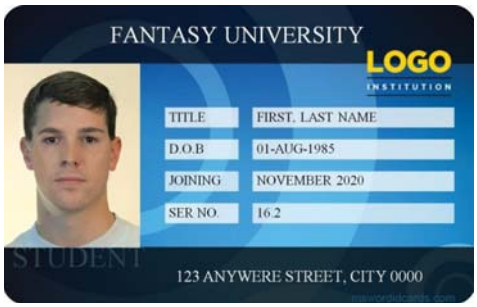


Fig. 6. Example of a created fake student identity card containing a morph.

Fig. 7. Example face images captured from the printed photo of presented student cards (the two leftmost images are bona fide and the two rightmost images are morphs).

V. Experiments

A. Experimental Setup

Mated comparisons, *i.e.* comparisons between same subjects, and non-mated comparisons, *i.e.* comparisons between different subjects, are conducted based on the participants face images and the ones obtained from the FERET face database [33]. Additionally, a morphing attacks is performed. Table I provides an overview of used datasets and the amount of conducted mated and non-mated comparisons as well as morphing attacks.

For face recognition the well-known ArcFace [34] system and a commercial of-the-shelf (COTS) system were employed. The use of the COTS face recognition system raises the

TABLE I
OVERVIEW OF USED DATABASES.

Database	Subjects (f/m)	References bona fide	References morphs	Probes	Comparisons mated	Comparisons non-mated	Morphing attacks
FERET	7 (4/3)	7	102	7	7	375	342
Collected	9 (6/3)	9		18	18		
Total	16 (10/6)	16	102	9	25	375	342

practical relevance of the vulnerability analysis. While the COTS system is closed-source, it is assumed that it is based on deep learning as the vast majority of state-of-the-art face recognition systems. The decision thresholds of the face recognition systems are set to achieve a False Match Rate (FMR) of 0%, *i.e.* no non-mated comparisons result in a false acceptance, and a FMR of 1%, *i.e.* one in onehundred non-mated comparisons results in false acceptance.

The vulnerability of the face recognition systems against morphing attacks is assessed using the metrics described in [35], *i.e.* Mated Morph Presentation Match Rate (MMPMR). The MMPMR describes the proportion of morphed face images accepted by the face recognition system, *i.e.* the success chance of a morphing attack.

B. Results

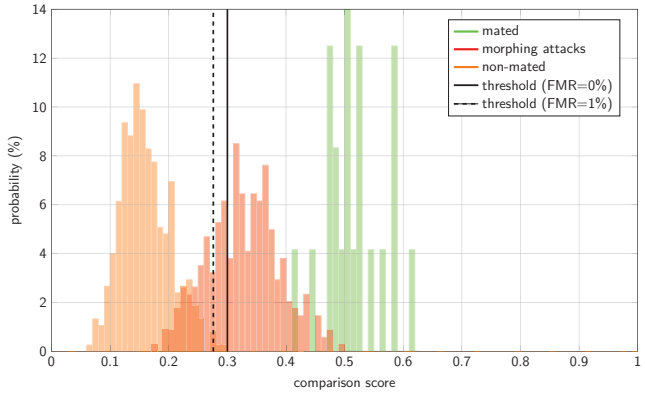
Score distributions of mated, non-mated, and morphing attack scores for both face recognition systems are plotted in figure 8 and summarized in table II. Firstly, it can be seen that both face recognition systems achieve a False Non-Match Rate (FNMR) of 0% for both considered decision thresholds, *i.e.* no mated comparison results in false rejection. It can be further observed that a high percentage of morphing attacks result in comparison scores which lie above the decison thresholds. Precisely, considering a threshold which corresponds to a FMR of 0%, for the ArcFace system a MMPMR of 65.5% is achieved and for the COTS system a MMPMR of 61.1%. For a more liberal decison threshold resulting in a FMR of 1%, MMPMR values of 78.1% and 85.4% are achieved for the ArcFace and the COTS system, respectively. That is, the success chances of morphing attacks significantly increase. It is important to note that more liberal decision thresholds are more suitable in the considered scenario, since face images extracted from identity documents are expected to exhibit lower quality in terms of image resolution, *cf.* figure 7, and therefore more tolerance of the face recognition system is needed.

TABLE II
EXPERIMENTAL RESULTS.

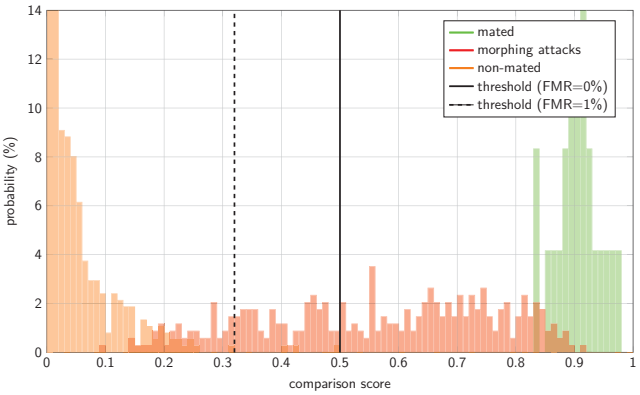
System	FMR (in%)	FNMR (in%)	MMPMR (in%)
ArcFace	0.0	0.0	65.5
	1.0	0.0	78.1
COTS	0.0	0.0	61.1
	1.0	0.0	85.4

VI. SUMMARY

Due to the current COVID-19 pandemic, remote education is predominantly used at schools and universities. Moreover,



(a) Arcface



(b) COTS

Fig. 8. Score distributions of mated/ non-mated comparisons and morphing attacks for both face recognition algorithms.

it is widely assumed that eLearning systems will gain more importance in the foreseeable future going beyond the COVID-19 pandemic. The expected increased use of eLearning systems necessitates a reliable identity verification of students. For this purpose, the application of face recognition has been recommended by numerous researchers.

In this paper, we investigated the feasibility of face morphing attack in eLearning systems considering an authentication scenario in which identity documents are remotely presented, *e.g.* prior to online examinations, and automated face recognition is applied. The attack potential of face morphing attacks has already been confirmed for other application scenarios, in particular for automated border control. It was shown that the success rate of face morphing attacks is rather high in the considered scenario ranging from approximately 60% to more than 85% (depending on the used face recognition system and its decision threshold). Considering the creativity and risk appetite of students when it comes to cheating in examinations, face morphing attacks pose a serious risk for eLearning systems. It is worth noting that similar authentication mechanisms are frequently employed in other security critical use-cases beyond eLearning, *e.g.* remote opening a bank accounts.

To prevent from morphing attacks, appropriate countermeasures would have to be implemented in eLearning systems. Among different proposed morphing attack detection

approaches, those which perform a differential detection appear most promising [30], [31]. Differential morphing attack detection methods analyse differences between a pair of face images to determine whether one of them is a morphed image, *e.g*. demorphing [36] or differential difference in deep face representations [37]. Future eLearning systems will have to incorporate an according attack detection module to prevent from different types of attacks aiming at circumventing biometric authentication including face morphing attacks.

ACKNOWLEDGEMENT

This research work has been partially funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

REFERENCES

[1] V. Chang, "Review and discussion: E-learning for academia and industry," *International Journal of Information Management*, vol. 36, no. 3, pp. 476 – 485, 2016.

[2] C. Rathgeb, K. Pöppelmann, and E. Gonzalez-Sosa, "Biometric technologies for elearning: State-of-the-art, issues and challenges," in *International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2020, pp. 1–6.

[3] P. S. Sanna and G. L. Marcialis, "Remote biometric verification for elearning applications: Where we are," in *International Conference Image Analysis and Processing (ICIAP)*, 2017, pp. 373–383.

[4] M. Messerschmidt and M. Pleva, "Biometric systems utilizing neural networks in the authentication for e-learning platforms," in *17th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2019, pp. 518–523.

[5] E. González-Agulla, E. Argones-Rúa, C. García-Mateo, and Ó. W. Márquez-Flórez, "Development and implementation of a biometric verification system for e-learning platforms," in *EduTech Computer-Aided Design Meets Computer-Aided Learning*, 2004, pp. 155–164.

[6] Y. Sabbah, I. Saroit, and A. Kotb, "A smart approach for bimodal biometric authentication in home-exams (sabbah model)," *CiiT International Journal of Biometrics and Bioinformatics*, vol. 4, pp. 32–45, 2012.

[7] N. Kaur, P. W. C. Prasad, A. Alsadoon, L. Pham, and A. Elchouemi, "An enhanced model of biometric authentication in e-learning: Using a combination of biometric features to access e-learning environments," in *International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES)*, 2016, pp. 138–143.

[8] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *Proceedings of the 2014 International Joint Conference on Biometrics (IJCB)*. IEEE, sep 2014.

[9] D. J. Robertson, A. Mungall, D. G. Watson, K. A. Wade, S. J. Nightingale, and S. Butler, "Detecting morphed passport photos: a training and individual differences approach," *Cognitive Research: Principles and Implications*, vol. 3, no. 1, jun 2018.

[10] E. González-Agulla, L. Anido-Rifón, J. L. Alba-Castro, and C. G. García-Mateo, "Is my student at the other side? applying biometric web authentication to e-learning environments," in *Eighth IEEE International Conference on Advanced Learning Technologies (ICALT)*, 2008, pp. 551–553.

[11] A. Fayyoumi and A. Zarrad, "Novel solution based on face recognition to address identity theft and cheating in online examination systems," *Advances in Internet of Things*, vol. 4, pp. 5–12, 2014.

[12] K. Rabuzin, M. Baca, and M. Sajko, "E-learning: Biometrics as a security factor," in *2006 International Multi-Conference on Computing in the Global Information Technology - (ICCGI)*, 2006, pp. 64–64.

[13] M. Pleva, P. Bours, D. Hladek, and J. Juhar, "Using current biometrics technologies for authentication in e-learning assessment," in *International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2016, pp. 269–274.

[14] J. Curran and K. Curran, "Biometric authentication techniques in online learning environments," in *Biometric Authentication in Online Learning Environments*, 2019, pp. 266 – 278.

[15] E. G. González-Agulla, E. Argones-Rúa, J. L. Alba-Castro, D. González-Jiménez, and L. A. Rifón, "Multimodal biometrics-based student attendance measurement in learning management systems," in *11th IEEE International Symposium on Multimedia (ISM)*, 2009, pp. 699–704.

[16] K. Paullet, D. M. Douglas, and A. Chawdhry, "Verifying user identities in distance learning courses: Do we know who is sitting and submitting behind the screen?" *Issues in Information Systems*, vol. 15, pp. 370 – 379, 2014.

[17] G. Fenu, M. Marras, and L. Boratto, "A multi-biometric system for continuous student authentication in e-learning platforms," *Pattern Recognition Letters*, vol. 113, pp. 83 – 92, 2018.

[18] G. Jagadamba, R. Sheeba, K. N. Brinda, K. C. Rohini, and S. K. Pratik, "Adaptive e-learning authentication and monitoring," in *2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020, pp. 277–283.

[19] S. Bhattacharjee, M. Ivanova, A. Rozeva, M. Durcheva, and S. Marcel, "Enhancing trust in eassessment - the tesla system solution," in *International Technology Enhanced Assessment Conference (TEA2018)*, 2018.

[20] EU-H2020 An Adaptive Trust-based e-assesment System for Learning (TeSLA) , https://tesla-project-eu.azurewebsites.net/, 2016, last accessed: Oct. 2020.

[21] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, March 2001.

[22] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, "Handbook of biometric anti-spoofing: Presentation attack detection," 2019.

[23] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: An evaluation methodology and lessons learned," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 20–30, August 2015.

[24] EU-FP7 Trusted Biometrics under Spoofing Attacks (TABULA RASA) , http://www.tabularasa-euproject.org/, 2016, last accessed: Oct. 2020.

[25] IARPA Odin, https://www.iarpa.gov/index.php/research-programs/odin, 2016, last accessed: Oct. 2020.

[26] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, December 2014.

[27] R. Raghavendra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *Computing Surveys (CSUR)*, vol. 50, no. 1, pp. 1–37, March 2017.

[28] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, "Face recognition systems under morphing attacks: A survey," *IEEE Access*, vol. 7, pp. 23 012–23 026, 2019.

[29] M. Ferrara, A. Franco, and D. Maltoni, "On the effects of image alterations on face recognition accuracy," in *Face Recognition Across the Imaging Spectrum*. Springer, 2016, pp. 195–222.

[30] M. Ngan, P. Grother, K. Hanaoka, and J. Kuo, "Face recognition vendor test (frvt) part 4: Morph-performanceofautomatedfacemorphdetection (nistir 8292)," National Institue of Standards and Technology (NIST), Tech. Rep., 2020.

[31] K. Raja, M. Ferrara, A. Franco *et al.*, "Morphing attack detection – database, evaluation platform and benchmarking," 2020, arXiv 2006.06458.

[32] International Civil Aviation Organization, "ICAO doc 9303, machine readable travel documents – part 9: Deployment of biometric identification and electronic storage of data in MRTDs (7th edition)," ICAO, Tech. Rep., 2015.

[33] P. Phillips, H. Wechsler, J. Huang, and P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image and Vision Computing*, vol. 16, no. 5, pp. 295–306, apr 1998.

[34] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, June 2019, pp. 4690–4699.

[35] U. Scherhag, A. Nautsch, C. Rathgeb *et al.*, "Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting," in *Proceedings of the 2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, sep 2017.

[36] M. Ferrara, A. Franco, and D. Maltoni, "Face demorphing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1008–1017, apr 2018.

[37] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, "Deep face representations for differential morphing attack detection," *Transactions on Information Forensics and Security (TIFS)*, vol. 15, pp. 3625–3639, 2020.