Makeup Presentation Attack Potential Revisited: Skills Pay the Bills

P. Drozdowski, S. Grobarek, J. Schurse, C. Rathgeb, F. Stockhardt, C. Busch
da/sec – Biometrics and Internet Security Research Group
Hochschule Darmstadt, Germany
{pawel.drozdowski,christian.rathgeb,fabian.stockhardt,christoph.busch}@h-da.de

***Abstract*—Facial appearance can be substantially altered through the application of facial cosmetics. In addition to the widespread, socially acceptable, and in some cases even expected use for the purpose of beautification, facial cosmetics can be abused to launch so-called makeup presentation attacks. Thus far, the potential of such attack instruments has generally been claimed to be relatively low based on experimental evaluations on available datasets.**

This paper presents a new dataset of such attacks with the purpose of impersonation and identity concealment. The images have been collected from online sources, concentrating on seemingly highly skilled makeup artists. A vulnerability assessment of face recognition with respect to probe images contained in the collected dataset is conducted on state-of-the-art open source and commercial off-the-shelf facial recognition systems with a standardised methodology and metrics. The obtained results are especially striking for the impersonation attacks: the obtained attack success chance of almost 70% at a fixed decision threshold corresponding to 0.1% false match rate is significantly higher than results previously reported in the scientific literature.

***Index Terms*—Biometrics, face recognition, makeup presentation attacks, concealment, impersonation**

I. Introduction

Presentation attacks (PAs), frequently referred to as "spoofing", pose a serious threat to face recognition systems [1], [2]. To launch a PA, the attacker presents a so-called presentation attack instrument (PAI), *e.g.* a face printout or a 3D face mask, to a biometric capture device or attempts to disrupt the biometric system through their behaviour, *e.g.* movement of the head. That is, the goal of the attacker is either to be recognised as a (certain) target subject registered in the biometric system, *i.e.* *impersonation*, or to prevent being recognised, *i.e.* *concealment* [3]. In the past years, various researchers have confirmed the vulnerability of face recognition systems to PAs, in particular state-of-the-art systems utilising deep convolutional neural networks [4].

Besides the aforementioned common PAIs, facial cosmetics may also be used to perform so-called makeup PAs (M-PAs) [5]. Makeup can be applied in a way that it substantially alters the perceived facial texture and shape which poses a challenge to automated face recognition [6], [7]. In 2010, the Computer Vision Dazzle Camouflage campaign [8] showed how makeup designs can be applied for identity concealment, *i.e.* to camouflage from face detection. When applied by skilled users or professional makeup artists, M-PAs may also be performed with the aim of impersonation [9]. In this case, makeup is applied such that an attacker's face looks similar to that of a target subject, while concealing the facial appearance of the attacker, see figure 1. In 2013, a female researcher successfully impersonated a male target subject by putting on makeup in the TABULA RASA Spoofing Challenge [10]. Moreover, on social media various makeup artists have showcased the feasibility of transforming their facial appearance to that of a target subject through the mere application of makeup.

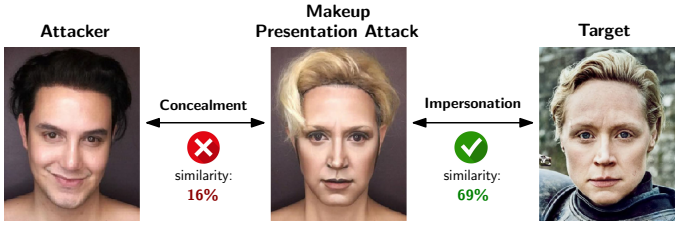


Fig. 1: Makeup presentation attack based on web-collected examples of facial images of a makeup artist: before (left) and after the application of makeup (middle) with the intention of obtaining the facial appearance of a target subject (right). Similarity scores were obtained using a COTS face recognition system.

Recently, different researchers have studied the vulnerability of face recognition systems to M-PAs for impersonation and concealment. For a comprehensive survey on M-PAs and detection approaches the interested reader is referred to [5]. Additionally, some face datasets containing M-PAs have been made available by different research laboratories. Evaluations on these datasets have revealed a moderate attack potential, *i.e.* success chance, of M-PAs which diminishes with rather restrictive decision thresholds [11]. However, it was also found that the chances of success for M-PAs can be arbitrarily high depending on the skill of the attacker and the degree of similarity between the attacker and the target subject in case of impersonation [5].

In this work, a new facial image dataset containing M-PAs for concealment and impersonation is introduced. In contrast to existing datasets, the collected dataset comprises M-PAs involving highly skilled makeup artists. The dataset is

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.

made available to the research community[1]. A vulnerability analysis using state-of-the-art open source and commercial-of-the-shelf (COTS) face recognition systems reveals that the attack potential of M-PAs has been clearly underestimated in previous works.

The remainder of this paper is organised as follows: section II briefly revisits related works on M-PAs. The data collection is described in section III and the vulnerability assessment is presented in section IV. Finally, conclusions are drawn in section V.

II. Related Work

Dantcheva *et al*. [6] first investigated the impact of daily makeup applied by bona fide subjects, *i.e*. bona fide makeup, on face recognition performance. It was found that the changes in facial texture and shape induced by makeup can negatively affect face recognition. Motivated by these findings, makeup-resilient face recognition schemes have been proposed by different research groups, see [7] for a survey on the effects of facial beautification on face recognition.

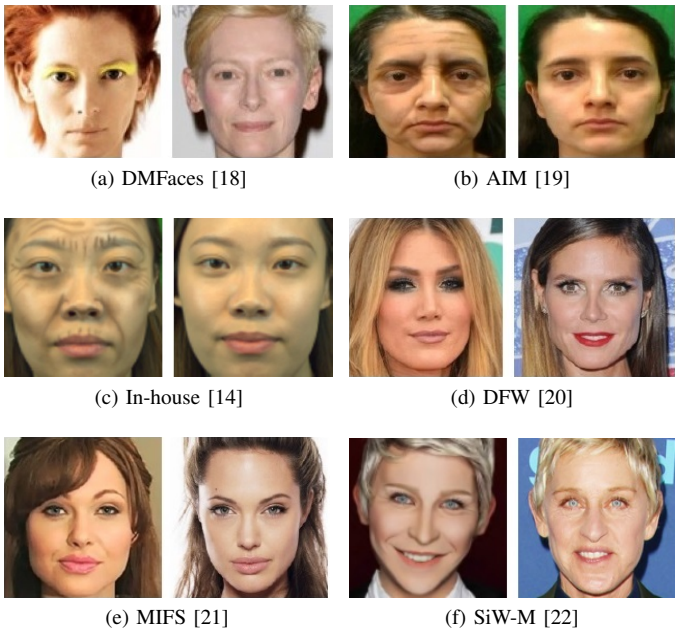
More recent works introduced datasets containing images of faces with heavy makeup (un)intentionally applied for concealment or impersonation. Properties of existing face datasets containing M-PAs are listed in table I. Example images of said datasets are shown in figure 2. Most available datasets contain web-collected facial images while some have been created with the help of professional makeup artists.

Different datasets contain various types of concealment M-PAs. Kumar and Wang [12] introduced the Disguise and Makeup Faces (DMFaces) dataset which comprises face images with heavy makeup. The application of heavy makeup contained in the probe sample of the image pair can be seen as concealment M-PAs for which the authors observed a decrease in genuine comparison scores various face recognition systems. Kotwal *et al*. [13] investigated age-induced concealment M-PAs and published the Age Induced Makeup (AIM) dataset. For this dataset, makeup was applied by professional artists to make the attacker look significantly older. Using an open source face recognition system, the authors observed a large drop in mated comparison scores ($\sim$15%), which confirms the feasibility of this type of M-PA. A similar in-house dataset was used by Arab *et al*. [14]. Singh *et al*. [15] presented the first competition on Disguised Faces in the Wild (DFW) dataset. This web-collected dataset partially contains images with heavy makeup for the purpose of concealment. Several submitted face recognition algorithms have been benchmarked and obtained results confirm the findings of previous works [16]. Finally, a small number of M-PAs are contained in the Spoof in the Wild dataset with Multiple Attack Types (SiW-M) introduced by Liu *et al*. [17].

Focusing on impersonation M-PAs, Chen *et al*. [9] introduced the Makeup Induced Face Spoofing (MIFS) dataset, which was collected from YouTube makeup video tutorials containing face images of subjects before and after the application of makeup, as well as images of target subjects. It was reported that COTS and open source face recognition systems are vulnerable to impersonation M-PAs. Recently, Rathgeb *et al*. [11], [23] confirmed these results for different state-of-the-art face recognition systems reporting success rates of approximately 8% and 30% for decision thresholds corresponding to false match rates (FMRs) of 0.1% and 1%, respectively. Additionally, on the DFW dataset introduced by Singh *et al*. [16], which contains impersonation M-PAs, Rathgeb *et al*. [5] obtained significantly higher success chances for impersonation M-PAs, *i.e*. up to 20% at a FMR of 0.1% and 50% for a FMR of 1%. It was found that the chances of success for impersonation M-PAs increase if there is a certain degree of similarity in terms of soft biometric characteristics between the attacker and the target subject, *e.g*. sex or age, as well as facial geometry, *e.g*. eye distance or forehead height. In summary, the evaluation of the effectiveness of impersonation M-PAs is generally conceded as difficult, since the attack potential depends on various factors such that consistency in the quality of M-PAs can not be guaranteed, especially if the makeup is applied by different makeup artists [5].

TABLE I: Overview of M-PA datasets which are available for research purposes

Dataset	M-PA Type(s)	Subjects	Samples
DMFaces [18]	Concealment	410	2,460
AIM [19]	Concealment	72	456
In-house [14]	Concealment	73	193
DFW [20]	Concealment, Impersonation	1,000	11,157
MIFS [21]	Impersonation	107	642
SiW-M [22]	Concealment, Impersonation	84	84



(a) DMFaces [18] (b) AIM [19] (c) In-house [14] (d) DFW [20] (e) MIFS [21] (f) SiW-M [22]

Fig. 2: Example image pairs of datasets containing M-PAs. Left images in each pair show concealment (a)-(c) and impersonation M-PAs (d)-(f).

[1]https://dasec.h-da.de/research/biometrics/hda-facial-makeup-presentation-attack-database/

III. Data Collection

Images in the presented dataset were found through manual Internet search. The collected dataset consists of two parts:

Bona fide makeup In recent years, many videos of makeup application were posted on popular public video sharing platforms. Among them are videos where a model is shown applying and wearing makeup[2]. From such videos, a reference image without makeup along with multiple (up to 20) images with different makeup styles were extracted.

Concealment and impersonation makeup Recently, instructions on how to imitate the facial appearance of another individual, as shown in figure 1, have gained popularity on video platforms. Several makeup artists have posted images and/or videos[3], where they demonstrate their skills. From such sources triplets of images (artist without makeup, artist with makeup, and target reference) were extracted. Images of artists without and with makeup represent concealment M-PAs and artists with makeup and the corresponding target reference are used as impersonation M-PAs.

The key aim of the data collection was that the collected images be of high quality (which is in contrast to many previously published datasets, recall section II). This was ensured in several ways: only high definition (1080p) videos were considered; from each of the found videos, frames corresponding to different makeup styles were extracted and subsequently manually selected based on general image quality (*e.g.* considering blur and sharpness). Furthermore, extreme facial expressions, partially covered faces, and strongly non-frontal poses were avoided. Table II provides a numerical overview of the collected dataset, while example images are shown in figure 3.

TABLE II: Overview of the collected dataset

Makeup type	Average resolution	Images		
		Neutral	Makeup	Target
Bona fide	552×575	33	366	—
Concealment	493×542	41	88	—
Impersonation	500×547	7	54	54

To facilitate reproducible research and further experiments in this field, the collected dataset along with the links to all the used source videos and websites are made available upon request.

IV. Vulnerability Assessment

Subsection IV-A describes the details of the experimental setup for the conducted vulnerability assessment, while subsection IV-B presents and discusses the obtained results.

[2]Example video: https://www.youtube.com/watch?v=DixJDVT17Ks

[3]Example video: https://www.youtube.com/watch?v=thukennSyGc

A. Experimental Setup

The vulnerability analysis on the collected datasets was conducted using a strong open source system (ArcFace [24]) with a pre-trained model provided by its authors. ArcFace produces feature vectors of 512 elements, whose dissimilarity can be computed using Euclidean distance. For the purposes of visualisation of the results, those dissimilarity scores were mapped into the range $[0, 1]$ using min-max normalisation and converted into similarity scores. While the use of this publicly available and well-known tool ensures the reproducibility of the experiments, an evaluation with a state-of-the-art commercial off-the-shelf (COTS) system was additionally conducted to increase the practical relevance of the obtained results.

To establish a large reference set of mated and non-mated comparison scores, as well as decision thresholds for several fixed, operationally relevant security levels, a subset of FRGCv2 dataset [25] yielding around 9,000 mated and 5,000,000 non-mated comparisons was used.

The results of the vulnerability analysis are reported using metrics standardised by ISO/IEC [26], [27]. Specifically, biometric recognition performance is reported using false match rate (FMR) and false non-match rate (FNMR); the efficacy of concealment attacks is reported using concealer attack presentation non-match rate (CAPNMR), while that of impersonation attacks using impostor attack presentation match rate (IAPMR). Additionally, to establish a relationship between the attack efficacy and biometric recognition performance, the relative impostor attack presentation accept rate (RIAPAR), is reported using the formula $=1+(\text{IAPMR}-(1-\text{FNMR}))$ as originally proposed by Scherhag *et al.* [28].

B. Results

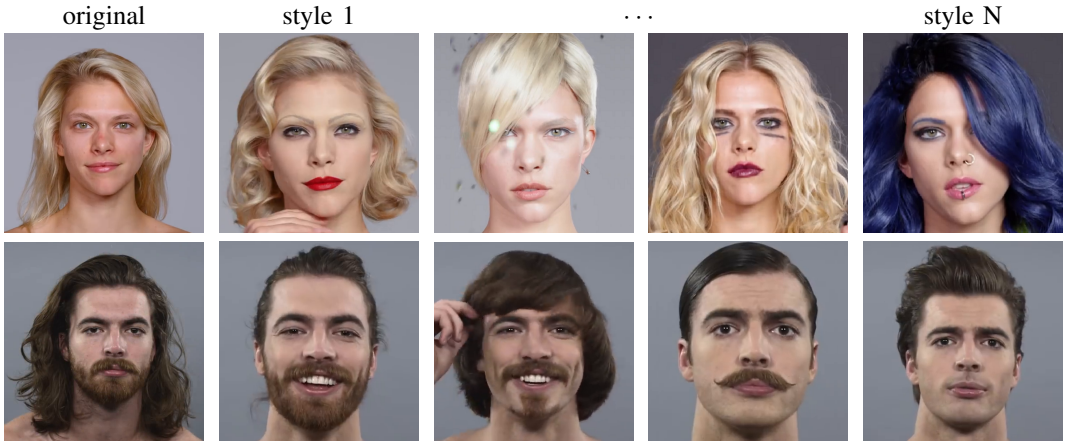
Figure 4 shows boxplots of the obtained comparison scores, while table III presents the corresponding descriptive statistics of the comparison scores. The figures also visualise decision thresholds for several security levels based on a fixed FMR value between 0.001% and 1.0%.

TABLE III: Descriptive statistics of the comparison scores

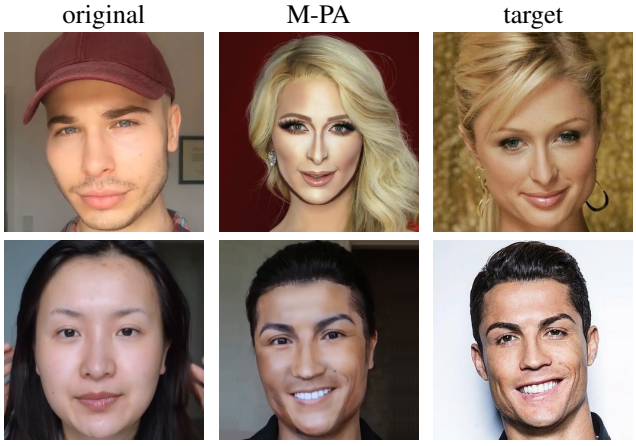
System	Attempt type	Mean	St. Dev.	Skew.	Ex. Kurt.	Min.	Max.
ArcFace	Non-mated	0.171	0.042	0.359	0.463	0.000	0.638
	Mated	0.667	0.091	0.363	-0.229	0.416	0.998
	Bona fide	0.585	0.085	-0.037	1.873	0.249	1.000
	Concealment	0.303	0.078	0.909	2.065	0.127	0.573
	Impersonation	0.364	0.080	-0.224	0.116	0.150	0.534
COTS	Non-mated	0.053	0.062	2.518	9.731	0.000	0.933
	Mated	0.961	0.028	-1.266	2.884	0.730	1.000
	Bona fide	0.900	0.086	-2.987	11.702	0.407	1.000
	Concealment	0.214	0.262	1.057	-0.281	0.000	0.947
	Impersonation	0.596	0.216	-0.454	-0.849	0.127	0.928

Based on the figures and the table above, several interesting observations can be made:

Bona fide makeup This type of makeup certainly leads to a degradation and wider spread of mated comparison scores. Nevertheless, given a fixed FMR value of 0.1%, which is recommended as a security level by FRONTEX in several operationally relevant scenarios [29], the vast majority of verification transactions would be successful.



(a) Bona fide makeup



(b) Concealment and impersonation makeup

Fig. 3: Example images from the collected dataset

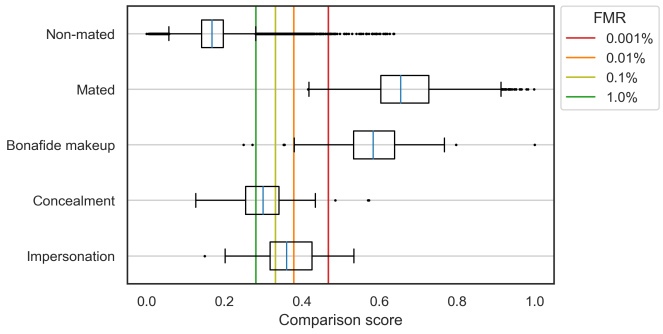
This type of makeup may, however, lead to problems when much more stringent security levels are applied, *cf*. CAPNR at FMR value of 0.001%.

Concealment makeup In this scenario, the applied makeup vastly degrades the mated comparison scores, although the resulting distributions do not fully overlap with the non-mated score distributions, *i.e*. the concealment is not perfect. This notwithstanding, the attacks would prove successful in a large proportion of verification cases for all but the most strict security level depicted in the figures.

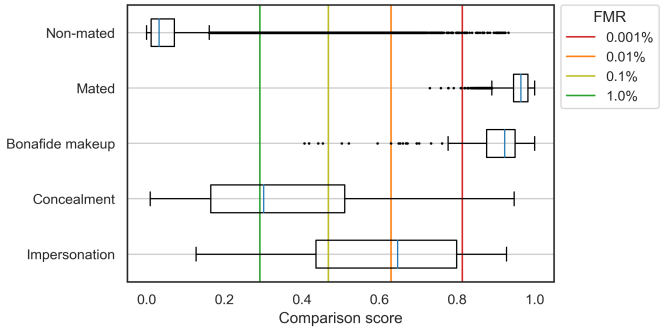
Impersonation makeup This type of makeup produces score distributions which lie between the mated and non-mated ones. In other words, for the most part, the artists manage to alter their appearance such that it mimics that of the target subject at least in some ways. A large proportion of the attacks would prove successful, even at the most stringent of the depicted security levels. It should be noted, that the initial appearance of the artists and possible similarity to the target does not seem to play a major role – the score distributions of comparisons between the artist without makeup and the target did not exhibit deviations from the non-mated score distributions. Furthermore, some artists actually manage successful impersonation despite a large age difference between the artist and the target or even when the artist and target are not of the same sex. This suggests that the skill of the artist is a much more important factor than their initial appearance.

Table IV shows the biometric recognition and presentation attack error rates for the three types of makeup at the aforementioned security (fixed FMR) levels.

It can be seen that the tested systems exhibit a near-optimal biometric performance for normal samples – a very low FNMR even at the most strict of the reported security levels. However, when quantifying the observations made on the score distributions above, significant error rates expressing the vulnerability of the face recognition systems are observed for samples with makeup. The bona fide makeup causes only small to moderately high CAPNMR values, which suggests that current face recognition systems are strongly capable of dealing with data subjects wearing daily makeup. The results are much more dramatic for the concealment and impersonation attacks. Concealment attacks reach a CAPNMR of around 40% and 70% for the open source and COTS systems, respectively



(a) ArcFace



(b) COTS

Fig. 4: Boxplots of the comparison scores

TABLE IV: Error rates (in %)

System	Makeup type	FMR	FNMR	CAPNMR	IAPMR	RIAPAR
ArcFace	Bona fide	0.001	0.540	7.104	—	—
		0.010	0.000	1.093	—	—
		0.100	0.000	0.546	—	—
		1.000	0.000	0.546	—	—
	Concealment	0.001	0.540	96.386	—	—
		0.010	0.000	87.952	—	—
		0.100	0.000	67.470	—	—
		1.000	0.000	40.964	—	—
	Impersonation	0.001	0.540	—	9.804	10.344
		0.010	0.000	—	37.255	37.255
		0.100	0.000	—	68.627	68.627
		1.000	0.000	—	90.196	90.196
COTS	Bona fide	0.001	0.079	7.479	—	—
		0.010	0.000	2.216	—	—
		0.100	0.000	1.108	—	—
		1.000	0.000	0.000	—	—
	Concealment	0.001	0.079	97.674	—	—
		0.010	0.000	89.535	—	—
		0.100	0.000	76.744	—	—
		1.000	0.000	70.930	—	—
	Impersonation	0.001	0.079	—	20.370	20.449
		0.010	0.000	—	53.704	53.704
		0.100	0.000	—	68.519	68.519
		1.000	0.000	—	88.889	88.889

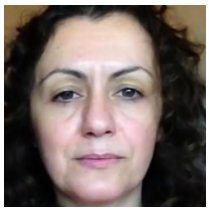
already at the lowest reported security level (fixed FMR of 1%); this quickly increases to beyond 70 and even 90% for higher security levels (*i.e.* lower FMR values). Alarmingly, a decent proportion (10-20%) of the impersonation attacks are successful even at the most stringent of the tested security levels. For less strict security levels, this proportion increases to well above 50% IAPMR: around 70% and 90% at fixed FMRs of 0.1% and 1%, respectively.

Figure 5 shows example image pairs of successful and failed

(a) Successful concealment

(b) Failed concealment

(c) Successful impersonation



(d) Failed impersonation

Fig. 5: Examples of attacks which succeeded or failed against both tested face recognition systems at a fixed FMR of 0.1%

attacks. The subfigure (b) shows the remarkable strength of facial recognition systems – despite extremely strong makeup covering the whole face, a seemingly different shape of the upper lip, as well as a changed hair colour and hair style, both tested systems correctly recognise the depicted data subject. The successful M-PA in subfigure (c) is particularly impressive, as the makeup artist and the attack target are actually of a different sex. This emphasises that sufficiently skilled attackers can successfully impersonate targets to which they bear no immediate resemblance. This anecdotal observation is confirmed by the quantitative evaluation shown in figure 6, which shows that the initial resemblance of the artist and the target does not seem to be a prerequisite for a successful impersonation attack.

The results obtained in the vulnerability analysis of the collected dataset indicate that, provided a sufficiently skilled artist, makeup presentation attacks pose a *much more severe* threat to biometric face recognition systems than previously reported in the literature and summarised in section II.

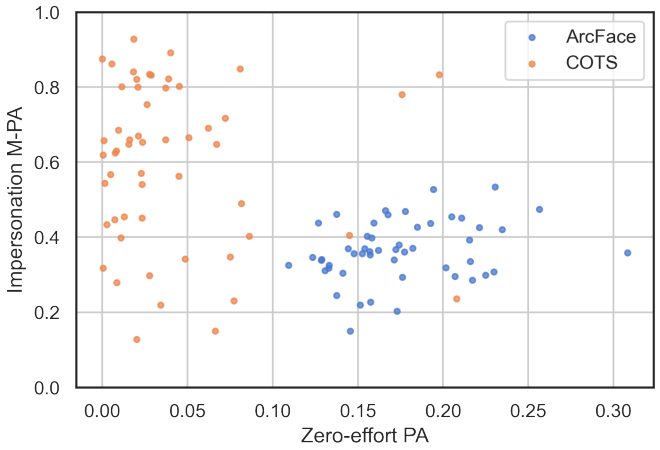


Fig. 6: Scatter plot showing the relation between initial similarity between the attacker and the target prior (x-axis) and after (y-axis) the application of the makeup PAI

V. Conclusion

This paper presents a new dataset of high-quality presentation attacks utilising makeup for the purposes of identity concealment or impersonation. Using the collected dataset, a biometric performance benchmark of state-of-the-art open-source and commercial biometric facial recognition systems has been conducted with ISO/IEC standardised evaluation protocols and metrics.

The obtained results are especially striking for the makeup attacks with the purpose of impersonation. While the IAPRs achieved on previously available datasets (*e.g.* MIFS and DFW) indicated impersonation M-PAs to only be a minor or moderate risk for current facial recognition systems [5], the conducted benchmark shows that the collected high-quality impersonation M-PAs exhibit an very high efficacy (see table IV) for practically relevant security levels in operational biometric verification systems.

To facilitate reproducible research and future experiments in this field, the dataset is made available upon request.

References

[1] 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.

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

[3] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 30107-1. Information Technology - Biometric presentation attack detection - Part 1: Framework*, International Organization for Standardization and International Electrotechnical Committee, 2016.

[4] A. Mohammadi, S. Bhattacharjee, and S. Marcel, "Deeply vulnerable: A study of the robustness of face recognition to presentation attacks," *IET Biometrics*, vol. 7, no. 1, pp. 15–26, January 2018.

[5] C. Rathgeb, P. Drozdowski, and C. Busch, "Makeup presentation attacks: Review and detection performance benchmark," *IEEE Access*, vol. 8, pp. 224 958–224 973, December 2020.

[6] A. Dantcheva, C. Chen, and A. Ross, "Can facial cosmetics affect the matching accuracy of face recognition systems?" in *International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, September 2012, pp. 391–398.

[7] C. Rathgeb, A. Dantcheva, and C. Busch, "Impact and detection of facial beautification in face recognition: An overview," *IEEE Access*, vol. 7, pp. 152 667–152 678, October 2019.

[8] A. Harvey, "Computer Vision Dazzle Camouflage," https://cvdazzle.com/, 2010, last accessed: May 12, 2021.

[9] C. Chen, A. Dantcheva, T. Swearingen, and A. Ross, "Spoofing faces using makeup: An investigative study," in *International Conference on Identity, Security and Behavior Analysis (ISBA)*. IEEE, February 2017, pp. 1–8.

[10] TABULA RASA Spoofing Challenge in conjunction with the 6th International Conference of Biometrics (ICB 2013), http://www.tabularasa-euproject.org/events/tabula-rasa-spoofing-challenge, 2013, last accessed: May 12, 2021.

[11] C. Rathgeb, P. Drozdowski, D. Fischer, and C. Busch, "Vulnerability assessment and detection of makeup presentation attacks," in *International Workshop on Biometrics and Forensics (IWBF)*. IEEE, April 2020, pp. 1–6.

[12] T. Y. Wang and A. Kumar, "Recognizing human faces under disguise and makeup," in *International Conference on Identity, Security and Behavior Analysis (ISBA)*. IEEE, February 2016, pp. 1–7.

[13] K. Kotwal, Z. Mostaani, and S. Marcel, "Detection of age-induced makeup attacks on face recognition systems using multi-layer deep features," *Transactions on Biometrics, Behavior, and Identity Science (TBIOM)*, pp. 1–11, October 2019.

[14] M. A. Arab, P. Azadi Moghadam, M. Hussein, W. Abd-Almageed, and M. Hefeeda, "Revealing true identity: Detecting makeup attacks in face-based biometric systems," in *Proceedings of the 28th ACM International Conference on Multimedia*. Association for Computing Machinery, 2020, p. 35683576.

[15] M. Singh, M. Chawla, R. Singh, M. Vatsa, and R. Chellappa, "Disguised faces in the wild 2019," in *International Conference on Computer Vision Workshop (ICCVW)*. IEEE, October 2019, pp. 542–550.

[16] M. Singh, R. Singh, M. Vatsa, N. K. Ratha, and R. Chellappa, "Recognizing disguised faces in the wild," *Transactions on Biometrics, Behavior, and Identity Science (TBIOM)*, vol. 1, no. 2, pp. 97–108, March 2019.

[17] Y. Liu, J. Stehouwer, A. Jourabloo, and X. Liu, "Deep tree learning for zero-shot face anti-spoofing," in *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4675–4684.

[18] The Hong Kong Polytechnic University Disguise and Makeup Faces Database (DMFaces), https://www4.comp.polyu.edu.hk/~csajaykr/DMFaces.htm, 2016, last accessed: May 12, 2021.

[19] Age Induced Makeup (AIM), https://www.idiap.ch/dataset/aim, 2016, last accessed: May 12, 2021.

[20] Disguised Faces in the Wild (DFW), http://iab-rubric.org/DFW/2019Competition.html, 2019, last accessed: May 12, 2021.

[21] Makeup Induced Face Spoofing (MIFS), http://antitza.com/makeup-datasets.html, 2017, last accessed: May 12, 2021.

[22] Spoofing in the Wild with Multiple Attacks Database (SiW-M), http://cvlab.cse.msu.edu/siw-m-spoof-in-the-wild-with-multiple-attacks-database.html, 2019, last accessed: May 12, 2021.

[23] C. Rathgeb, P. Drozdowski, and C. Busch, "Detection of makeup presentation attacks based on deep face representations," 2020, arXiv 2006.05074.

[24] 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.

[25] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the face recognition grand challenge," in *Conference on Computer Vision and Pattern Recognition (CVPR)*, vol. 1. IEEE, June 2005, pp. 947–954.

[26] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*, International Organization for Standardization and International Electrotechnical Committee, April 2006.

[27] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 30107-3. Information Technology – Biometric presentation attack detection – Part 3: Testing and Reporting*, International Organization for Standardization and International Electrotechnical Committee, September 2017.

[28] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. J. Veldhuis *et al.*, "Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting," in *International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, September 2017, pp. 1–7.

[29] eu-LISA, "Best practice technical guidelines for automated border control ABC systems," Tech. Rep. TT-02-16-152-EN-N, September 2015.