https://doi.org/10.2352/EI.2022.34.3.MOBMU-361

Improving Detection of Manipulated Passport Photos - Training Course for Border Control Inspectors to Detect Morphed Facial Passport Photos - Part II: Training Course Materials

Franziska Schwarz[1], *Klaus Schwarz*[2,3,4], *Reiner Creutzburg*[1,2]

[1] *Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany*

[2] *SRH Berlin University of Applied Sciences, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany*

[3] *The University of Texas at San Antonio, College of Engineering, 1 UTSA Circle, San Antonio, TX 78249-0669, USA*

[4] *University of Granada, Faculty of Economics and Business, P.° de Cartuja, 7, ES-18011 Granada, Spain*

Email: franziska.schwarz@th-brandenburg.de, klaus.schwarz@srh.de, kschwarz@correo.ugr.es creutzburg@th-brandenburg.de, reiner.creutzburg@srh.de

Abstract

In recent years, ID controllers have observed an increase in the use of fraudulently obtained ID documents [1]. This often involves deception during the application process to get a genuine document with a manipulated passport photo. One of the methods used by fraudsters is the presentation of a morphed facial image. Face morphing is used to assign multiple identities to a biometric passport photo. It is possible to modify the photo so that two or more persons, usually the known applicant and one or more unknown companions, can use the passport to pass through a border control [2]. In this way, persons prohibited from crossing a border can cross it unnoticed using a face morphing attack and thus acquire a different identity. The face morphing attack aims to weaken the application for an identity card and issue a genuine identity document with a morphed facial image. A survey among experts at the Security Printers Conference revealed that a relevant number of at least 1,000 passports with morphed facial images had been detected in the last five years in Germany alone [1]. Furthermore, there are indications of a high number of unreported cases. This high presumed number of unreported cases can also be explained by the lack of morphed photographs' detection capabilities. Such identity cards would be recognized if the controllers could recognize the morphed facial images. Various studies have shown that the human eye has a minimal ability to recognize morphed faces as such [2], [3], [4], [5], [6].

This work consists of two parts. Both parts are based on the complete development of a training course for passport control officers to detect morphed facial images. Part one contains the conception and the first test trials of how the training course has to be structured to achieve the desired goals and thus improve the detection of morphed facial images for passport inspectors [7]. The second part of this thesis includes the training course and the evaluation of its effectiveness.

Introduction and Motivation

The goal of this work was to develop a training course for passport control officers to recognize morphed facial images. The focus was on developing a procedure that will help employees in the citizens' office and passport control officers at border crossings to detect manipulations at suitable points in the image. For this reason, the training course should take into account both the scenario of border control and the scenario of applying for an identity card at the citizens' office. For this purpose, literature research was started on the standard procedure of ID card control and face morphing attacks. Subsequently, points of attack in the morphing procedure were identified and based on this, a concept for a training course was developed. In connection with this training course, suitable images and texts were created to improve morphing facial images' recognizability.

Part two explains the conception of the developed training course and how the training course has to be structured to achieve the desired goals and thus improve the detection of morphed facial images for passport inspectors. It also includes the evaluation of the course.

Keywords

Face Morphing, Border Control, Morphed Facial Images, Passport Control

Basics

Morphing and Morphing Attack

Morphing is a computer-generated modification of digital image files in which intermediate transitions are calculated between two individual images. Through the use of specific distortions, one image is transformed into another. The aim is to create a transition from the source image to a target image that is as realistic as possible. (cf. [6]) Thus, the typical morphing process consists of selecting prominent image elements (facial features such as mouth, eyes, or outer edges of the face) in the source and target images and distorting them so that their contours can be made to match. To achieve the most realistic effects, the source and target images must look as similar as possible. Figure 1 shows the free program FaceMorpher creating a morphed face image.

Biometric facial recognition is widely used for the identification or authentication of persons. If a digital passport photo is modified by morphing, a passport is obtained with two or more persons' identification features. Face morphing thus poses a serious threat to the integrity of facial recognition-based verification. Attackers have several powerful hardware and software tools at their disposal that allow digital images to be easily created and manipulated without creating any perceptible noise on the digital image. This can undermine the authenticity and integrity of digital images. When facial images are used to prove a person's identity, the facial images' authenticity can no longer be taken for granted [9]. In the worst case, unauthorized persons can be granted access to border control systems or even pass through them. This circumstance poses an enormous challenge to digital image forensics. The following figure (see fig. 2) shows the sequence of a morphing attack.

Application Procedure for an Identity Document at the Citizens' Office (Section 6 Passport Act)

Facial biometrics is widely used in secure border control applications where a person's identity is verified against an electronic passport or national identity card. While in a few countries, the passport's facial image is captured under controlled conditions within a trusted authorized entity (e.g., a police station). In most countries, the applicant is required to submit a facial image. This approach is still widely used in Europe and the USA. Therefore, the applicant can provide an image of his face that may be more similar to his own by using processing techniques. [10]

To apply for a passport at the Citizen's Office, the applicant must appear in person. The application for a passport is filled out on the spot with the Citizen's Office employee. The applicant only needs to sign the application. For the application, fingerprints are required by law (flat print of the left and right index finger). The passport producer will send the passport to the applying citizen's office after production. There it can be accepted by the applicant personally.
Required Documents for the Passport Application (in Europe):

- Valid identity card (passport, identity card, child's identity card, child's passport),
- Current photo in passport format (45 x 35 mm), portrait format, frontal photo without a border, without headgear and without covering the eyes (biometric photo),
- If applicable, the previous passport,
- Birth certificate, if applicable.

Required Documents for the Passport Application (in the United States) [9]:

- Complete the Form (DS-11) Application for U.S. Passport on the State Department website,
- Print completed application. The signature is only done in the citizen office,
- Have a passport photo taken,
- Photocopy the proof of identity and U.S. Citizenship documents,
- Calculate fees.

When applying for a child: the identity card of the present custodian, the declaration of consent if necessary, and a copy of the identity card of the absent custodian, the proof of custody in the case of only one custodian. The verification that the biometric photo submitted also shows the person applying for the passport is the sole responsibility of the person employed at the Citizen's Office who will receive it. A check, e.g., a morphine attack, is only performed by the naked eye of the person employed in the citizen's office. For this reason, it is essential that a possible attack can be detected at this stage to prevent the issuing of a real document with a morphing facial image.

Passport Control Procedures at Border Crossings

Border crossings (see fig. 3) are an essential checkpoint for tracking down persons who are wanted for crimes committed or who try to cross a border illegally and could become a threat to the country concerned. With increasing migration worldwide, border control authorities have become a significant challenge to detect anomalies in documents. Countries are continually trying to develop new methods and procedures and use new technologies to bring such documents to light. Different countries worldwide use different or more types of border control systems and numerous biometric capture devices. Some of the types of border control systems are listed below:

- Manual border control, e.g., the manual border control cabin or a mobile control,
- Self-Service System (SSS), e.g., a self-service kiosk,
- E-gate, e.g., a gate that uses the facial image as a token,
- Automated Border Control (ABC): This system can be considered a combination of a self-service system and an e-gate. e.g., a two-stage, separate person trap system,
- Automated Passport Control (APC) as a U.S. Customs and Border Protection (CBP) program that streamlines the entry process for U.S. citizens. [11]

The following types of biometric capture devices are available:

Two-Modality Systems

These systems are very well able to capture both fingerprints and facial images.

One-Modality Systems

Single-modality systems can capture only one feature at a time, either fingerprints or facial images. If such systems require the capture of biometric data from a traveler's features for which the device is not available, the traveler must be redirected to another system type. One-modal systems with facial capture devices are usually found at border crossings, while systems with fingerprint capture devices are usually found at national registry offices. [12]

Regulation of Biometric Border Control Procedures

The legal ownership of the identity documents presented by the traveler must be established and verified using biometric data.

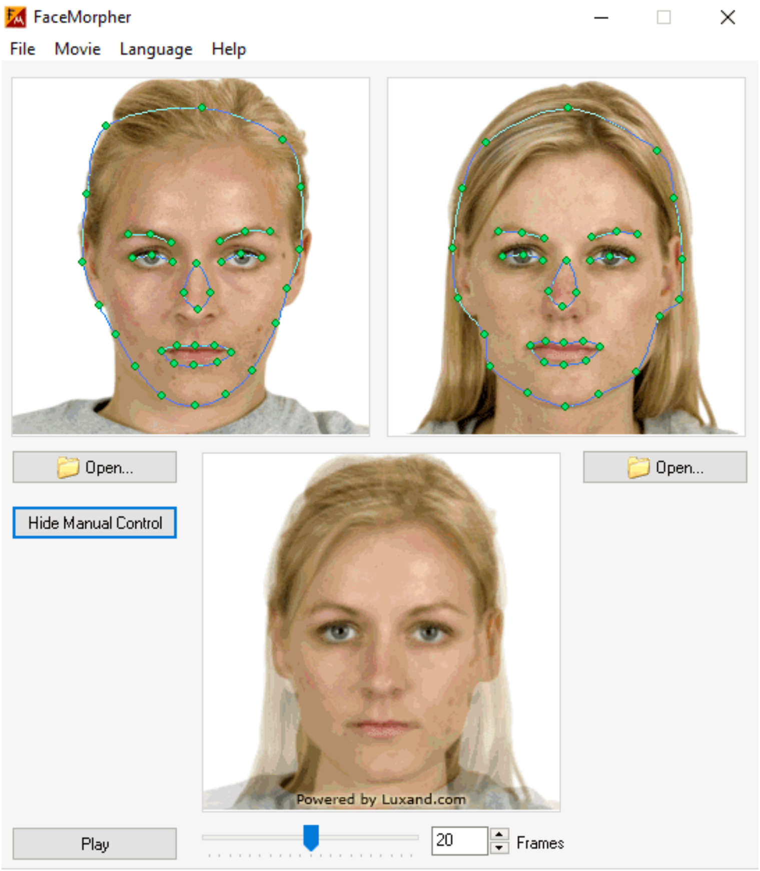

Figure 1. *Morph creation with the software FaceMorpher [8]*

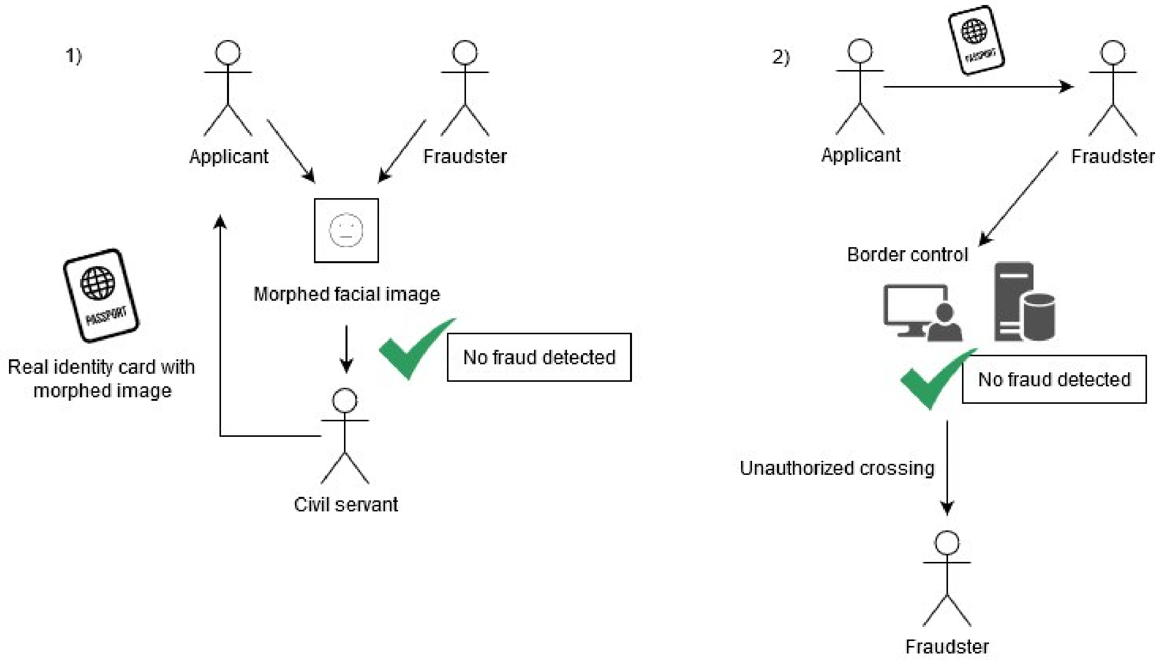

Figure 2. *Face morphing attack in city hall and passport control*

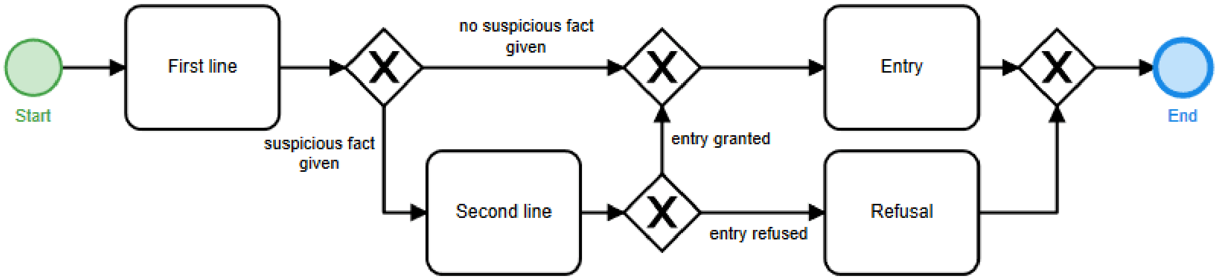

Figure 3. *General passport control procedure [13]*

The border control process described below is the normal process and is generally referred to as the ”first-line process.” In this process, at least one of the described biometric processes is performed for verification purposes. The process includes the following [14]:

- comparison of the printed facial image on the travel document with that of the traveler by the border guard.
- comparison of the traveler’s fingerprints concerned with the biometric data stored by the biometric system on the digital chip of the travel document.
- Comparing the affected traveler’s face with the facial image stored by the biometric system on the travel document’s digital chip.
- Comparing the fingerprints of the traveler concerned with the biometric data stored in the database by the biometric system.
- comparison of the traveler’s face concerned with the image of the traveler’s face stored in the database by the biometric system.

Automated Passport Control (APC) at U.S.-Borders

APC kiosks located at international airports throughout the country make it easier for passengers to enter the United States.

Automated Passport Control (APC) is a U.S. Customs and Border Protection (CBP) program that simplifies the entry process for U.S. citizens, U.S. permanent residents, Canadian citizens, eligible participants in the Visa Waiver Program, certain travelers with a U.S. visa by providing an automated process through CBP’s Primary Inspection Division. Travelers use self-service kiosks to answer CBP inspection questions and provide biographical information. APC is a free service, requires no preregistration or membership, and offers the highest level of protection when handling personal data or information. Travelers who use APC experience shorter waiting times, less congestion, and faster processing. [15]

Instead of filling out a paper form for the customs declaration, authorized passengers can go directly to the APC kiosks in the passport control area. Passengers are asked to scan their passports, take a photo at the kiosk and answer a series of CBP inspection questions to verify biographical and flight data. Once passengers have answered the series of questions, a receipt will be issued. Passengers then take their passports and receipt to a CBP official to complete their inspection for entry into the United States. At the kiosks, people who live at the same address can be processed together. [16]

State of the Art

Ferrara (cf. [2]) introduced the morphing attack as a significant security problem that can bypass all integrity checks (visually by control officers and electronically by automated border control systems, so-called ABC systems). The study illustrates that both automated border control systems and human experts can be deceived when presented with a passport containing a morphed facial image. This observation has been used as a basis for further studies such as that of Robertson et al. (see [3]), which tested humans’ ability to detect morphed facial images with different degrees of morphing in different experiments. Although the test subjects accept 50/50 morphs with alarmingly high rates as real ID (68 % experiment 1), it is relatively easy to significantly reduce this error rate by a few simple instructions (to 21% in experiment 2). This shows that instructions like in a training course can improve the detectability of morphed facial images. In another study, Kramer et al. (cf. [4]) show us, among other things, how people score on the detection of morphed facial images when they can compare them with a live video sequence of the person being tested. In this experiment, subjects scored best when compared with frame-by-frame comparisons. This result shows that live images can contribute to better detectability. The study by Makrushin et al. (cf. [6]) also shows that the manual processing of a passport photo is the greatest weakness in the concept of identity verification with a photo ID. It is based on a border control situation that is as realistic as possible, in which people should compare passport photos with moving faces with the hint that they may be morphed facial images. For this purpose, a video sequence of the person to be checked is shown in each case, showing how this person enters the border control checkpoint. Here too, the human being can recognize face images that have been a little morphed as such. The study concludes that both the personnel checking photo IDs at border crossings and staff at document issuing points need computer-based assistance in detecting morphed facial images. Whether specific training can also support, this is the subject of this work.

Own Contribution

As numerous studies have already prove [2], [3], [4], [5], [6], humans are only conditionally able to evaluate foreign facial photos regarding whether these are morphed or not. Especially with professionally produced morphs that have been carefully cleaned of image artifacts, the results are often only slightly better than those of random guessing [17]. With the help of the weaknesses identified in the morphing process and the training course developed from it, this work is intended to help ID controllers in public offices and at border controls to detect better morphed facial images. It is based fundamentally on statements (cf. [3]) that prove that targeted clues can improve the results of detected morphs. For this purpose, a training course (including solutions) for identity card inspectors will be developed, including ten practical exercises accompanying theoretical questions. With an introductory text, the course will introduce the dangers of a morphing attack and should already motivate and sensitize for this form of attack. It already deals with the substantial dangers of applying for an identity card and passport control. In the introduction, there will be an accompanying theory. Here the term morphing will be explained, and the morphing process will be illustrated in detail using sample images. It will deal with the morphing process's steps (finding control points, alignment through distortion). Also, the artifacts that may arise from this will be explained and illustrated here.

In the context of this work, these artifacts are divided into three categories:

- Artifacts, in case of deviations of the set control points due to algorithmic imprecision or too large biometric deviations between source and target image,
- Artifacts that can be recognized as obvious image defects when superimposed, and
- Artifacts that indicate inconsistencies in identification features.

Setting the control points has a strong influence on the quality of the final face morph. Whether the control points are set automatically or by hand, this is where the most significant subsequent errors occur. Shadows or veils are the results. [18] Therefore, obvious image errors such as shadows and veils on hair, eyes, ears, collar, and hairline will be illustrated in the course. Inconsistencies, which can occur even in carefully edited face morphs, will be pointed out in a detailed text. This section will raise awareness that it is worthwhile to carry out a detailed examination of individual parts of the face. The following section will contain ten tasks in which the participants can answer theoretical questions and solve practical tasks, such as defining control points in given facial morphs. This should help to understand and practically reproduce the process of morphing. For a better understanding, the solutions to the practical tasks will be shown on the following pages. This should help to react to the requirements as early as possible and improve within the course and not only afterward in a possible evaluation. If necessary, the solution can also give first hints and clues for the task. The theoretical questions will refer to the course's theoretical part, which should be read thoroughly in advance. The images used in this course will be based on the Chicago Face Database (CFD) version 2.0.3, which was developed at the University of Chicago (see [19]). Selected facial images will be morphed with free software [8] in a 50/50 ratio and serve as visual material for this course to illustrate the course content.

Course Objectives

The developed course concept and the corresponding exercises are designed for all persons who have to check facial images for authenticity in the citizens' office and at passport control points. A complete course comprises three-course units. The time frame for each unit is, on average, four to six hours.

The aim of this teaching concept and accompanying exercises are designed to give participants a comprehensive overview of the topic of Face Morphing and enable them to work independently with the tools and techniques they learned. Upon successful completion, participants will be able to improve their ability to detect morphed passport photos and contribute significantly to the security of border controls.

The assignments are designed for several exercises to achieve the stated goals. These exercises are primarily intended to impart knowledge about possible modification options for passport photos. Participants will learn which elements of an image are modified and how the process of face morphing works. They will learn about and understand the tools used for this purpose. The course participants create their own morphed face images in practical exercises and thus get an insight into the work of potential attackers. In doing so, the participant will be sensitized especially for the mistakes in this process, so that they can be found successfully after the course completion.

The hands-on exercises will allow participants to become familiar with the tools presented, while an instructor will also supervise the exercises. This allows the participants to memorize and understand the theoretical content of the course on their own. However, they will be addressed directly and individually in case of questions and problems. In this way, the participant's interest in morphed facial passport photos is to be awakened, and thus more specialists in this area are to be trained. The acquired knowledge will be retained over a more extended period of time due to the embedding of practical tasks and independent but accompanied learning. This should motivate participants more and help them achieve a sense of achievement.

The cognitive goals of the course are to gain a basic understanding of the field of morphed facial passport photos and to know what tools are available and how to use this knowledge to detect fraud. The primary practical goal of the course is a case-specific application of the tools taught in the course, to be achieved through hands-on laboratory exercises. The effective goal is trained awareness and sensitivity to the significant problems of the face morphing topic. How can morphed facial passport photos be produced? How can morphed facial passport photos be detected? These are just a few of the many questions that the course participants will ask themselves during the course.

By combining theory and practice in practical scenarios, participants expand their expertise and apply what they have learned directly in a real-world environment. Participants will go through the complete evolution of developing a morphed facial passport photo. This way, participants learn the basics of morphing and its applications.

This is followed by the three main parts of the course, which consist of exercises on various topics related to the face morphing process. In the three main parts, participants will receive a com-

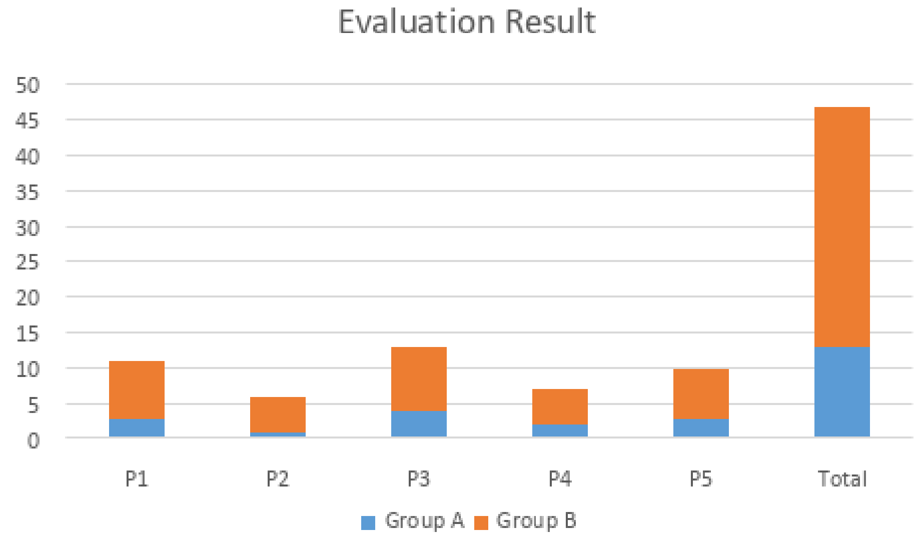

Figure 4. *Evaluation result*

prehensive introduction to the topic of face morphing and will be enabled to work independently with the common tools and techniques. Upon successful completion, participants will be able to produce a morphed facial image that contains the identity features of two or more persons.

The first central part of the course focuses on the theory of the morphing process and understanding this vulnerability in the border control system. For this purpose, groups with a maximum of four participants will be formed at the beginning. These groups will each receive a small database of facial photos to use within the presented tools. These facial photos will be modified step by step during the first central part.

In the second central part of the course, participants will be sensitized to the errors that occur during the morphing process, because it is only on the basis of these that the human eye is able to recognize morphed facial photos. Participants will be sensitized to certain artifacts and control points and learn to pay attention to them in the work situation.

In the third and final part of the course, course participants now practice the knowledge they have learned in a test environment that is as authentic and as close to the truth as possible. For this purpose, the morphed facial images of the other groups are evaluated and examined for their authenticity.

All three parts together provide a comprehensive overview and in-depth knowledge in the field of face morphing and enable the participants to work independently in this area.

Course Description

The course developed in this work consists of a total of three parts and exercises. The first part of the course is dedicated to the following topics:

- Getting familiar with the concept of morphing
- Recognizing the danger posed by morphing on facial images, especially for the passport system
- Getting acquainted with the basics of the processes in the Citizen's Office and at the border control

1. Introduction to the Morphing and Passport Process

The first part of the course focuses on the basics of the concept of morphing and its application. It will be clarified which sub-steps make up the process of morphing and how this process can be exploited for the border crossing of unauthorized persons. Furthermore, the process of passport issuance in the Citizen's Office and the system of border surveillance will be examined and internalized in more detail.

2. Morphing of Facial Photos Using a Practical Approach

In the second part of the course, tools for the creation of morphed facial images will be presented and own morphs will be created in practical exercises. For this purpose, groups of a maximum of 4 persons will be formed. They will receive a photo database with images that can be used for practical applications. The focus will be mainly on the morphing process errors. Artifacts and image errors that result from this process will be examined and highlighted.

3. Recognizing Morphed Facial Images in the Practical Training Exercise

In the third and last part of the course, the acquired knowledge is applied practically. For this purpose, the participants are brought into a realistic situation (passport application office or border control) and are confronted with morphed and unmodified, original passport photos. The participants must now decide and indicate whether or not it is an altered, morphed facial image. For this purpose, they are also shown the persons who are to be seen on the picture life. This is done either by video or in presence.

Evaluation

To evaluate the developed training methods which were designed for the future training course, a group of altogether 10 test persons was available. Members from the family and university environment agreed to clarify whether the course developed for identity card inspectors can better detect morphed facial images. Studies[2] have already proven that (without the training course) there are no differences between trained buttocks (e.g., border control personnel) and untrained subjects (e.g., students or professors) in the detection of morphed facial images. This should lead to a usable result of our evaluation, which only includes untrained subjects.

Methodology

The ten subjects were divided into two groups (Group A and Group B) of 5 participants. Group A completed the designed training course in advance, while Group B only received the information that the facial images to be evaluated could be a morphing attack. Where necessary, a brief explanation was given of what the term morphing means. Further hints, e.g., how to recognize such an attack, were not given. In the process of comparative control, the verification was done by a real live image. Studies such as that conducted by Robin S. S. Kramer (cf. [4]) show that the best results were obtained by comparing a live image and re-enacting a relatively real control situation. The persons to be checked were thus in the same room as the subjects asked to compare a facial image with the person to be checked. Another five persons from the university environment were selected as persons to be examined. High-quality facial images were taken beforehand, and these were morphed in part with facial images from the Chicago Face Database (CFD) that matched as closely as possible. Three high-quality morphs (in a ratio of 50/50) were created, and assigned to the respective persons whose images served as source images here. 2 persons were assigned original passport photos. The test persons were presented with a morphed or non-morphed facial image in the passport photo format (3.5 cm by 4.5 cm) in 5 passes. The only aid was a folding magnifier (manufacturer: Jebester, Amazon for 10.99 $), as it is available to passport inspectors, e.g., at mobile control posts in the transit area, the passport photo, and the relevant facial details sufficiently. After the test, persons could look at the passport photo for one minute, and the person who was to be seen on the passport photo and checked was sent into the room. The person who was to be checked did not know whether the examiner had a morphed facial image or not, in order not to give any clues through a particular behavior. The examiner was allowed to instruct the person to be examined to make certain parts of the face visible, e.g., hairline, by taking back the hair, removing glasses, or similar. The test persons had as much time as they considered necessary to assess whether the passport photo presented was an original or a morph. The participants in both groups evaluated the same picture-person combinations.

Results

Overall, the first experiment's evaluation shows that group B subjects (with training) performed significantly better overall than the subjects from group A (without training). Group A correctly evaluated only 13 of 25 facial images, while group B correctly evaluated 21 of 25 facial images. At the end of the evaluation process, the subjects could indicate whether they accepted or rejected a picture. Fig. 4 shows a graphic representation of the results.

It was also observed that group B subjects gave the persons to be examined more instructions to make certain parts of their faces visible than the subjects from group A, who hardly gave any instructions. This indicates that the training course sensitized the subjects to look closer and compare facial details.

Conclusion and Future Work

The first part of this work shows that a training course for identity card inspectors can improve morphed facial image detectability. Care was taken to ensure that the test environment was as realistic as possible, as it would be in the citizens' office or at the border crossing. It must be noted that this small number of test persons does not provide a reliable result and only a rough outlook on what the created training course in part two of this work can achieve.

The second part of this work shows the detailed course concept for passport control officers in the citizens' office and at border controls. It also includes its evaluation and effectiveness.

Future work could also, for example, take up this procedure, modify it appropriately, and evaluate it with more participants. The training course could also be extended quantitatively (repetition) by further theoretical questions and practical exercises. The special requirements for morphed facial images of children, which usually change faster than those of adults due to natural growth, also remain investigated. Here, unique teaching methods would be necessary to train ID controllers and protect children from abuse and abduction. The main problem here is that there is no compulsory attendance for children under ten years of age when applying for an ID card.

All in all, it can be concluded that in the event of discrepancies or error messages in the system, it is ultimately human personnel who decide whether the person in the passport photo is also the person who is to acquire an ID document or pass through a border crossing. This is why it is so important to have trained operators here.

References

[1] P. Heller, "One passport for two." `https://www.faz.net/aktuell/wissen/computer-mathematik/morphing-ein-pass-fuer-zwei-16588552.html`, Jan. 2020.

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

[3] 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, Jun 2018.

[4] R. S. S. Kramer, M. O. Mireku, T. R. Flack, and K. L. Ritchie, "Face morphing attacks: Investigating detection with humans and computers," *Cognitive Research: Principles and Implications*, vol. 4, Jul 2019.

[5] A. Makrushin, T. Neubert, and J. Dittmann, "Automatic generation and detection of visually faultless facial morphs," in *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, SCITEPRESS - Science and Technology Publications, 2017.

[6] A. Makrushin, T. Neubert, and J. Dittmann, "Humans vs. algorithms: Assessment of security risks posed by facial morphing to identity verification at border control," in *Proceed-*

ings of the 14th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, SCITEPRESS - Science and Technology Publications, 2019.

[7] F. Schwarz, K. Schwarz, and R. Creutzburg, “Improving detection of manipulated passport photos-training course for border control inspectors to detect morphed facial passport photos-part i: Introduction, state-of-the-art and preparatory tests and experiments,” *Electronic Imaging*, vol. 2021, no. 3, pp. 136–1, 2021.

[8] Luxand Inc., “Face Morpher.” `http://www.facemorpher.com`, 2004–2007.

[9] R. Raghavendra, K. B. Raja, and C. Busch, “Detecting morphed face images,” in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–7, 2016.

[10] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, “Single image face morphing attack detection using ensemble of features,” in *2020 IEEE 23rd International Conference on Information Fusion (FUSION)*, pp. 1–6, 2020.

[11] U. Scherhag, C. Rathgeb, and C. Busch, “Towards Detection of Morphed Face Images in Electronic Travel Documents,” in *2018 13th IAPR International Workshop on Document Analysis Systems (DAS)*, pp. 187–192, 2018.

[12] M. Ferrara, A. Franco, and D. Maltoni, “Decoupling texture blending and shape warping in face morphing,” in *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–5, 2019.

[13] BSI, “Biometrics for public sector applications,” tech. rep., Bundesamt für Sicherheit in der Informationstechnik, 2019.

[14] wikiwand, “Automated border control systems.” `https://www.wikiwand.com/en/Automated_border_control_system`, 2020.

[15] usa.gov, “Getting or Renewing a U.S. Passport..” `https://www.usa.gov/passport`, 2020.

[16] D. Gorodnichy, S. Yanushkevich, and V. Shmerko, “Automated border control: Problem formalization,” in *2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM)*, pp. 118–125, 2014.

[17] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch, and A. Uhl, “Detection of Face Morphing Attacks Based on PRNU Analysis,” *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 4, pp. 302–317, 2019.

[18] T. Bourlai, *Face Recognition Across the Imaging Spectrum*. Springer-Verlag GmbH, 2016.

[19] M. Correll and B. Wittenbrink, “The Chicago Face Database: A Free Stimulus Set of Faces and Norming Data..” `https://chicagofaces.org`, 2016.

Author Biography

Franziska Schwarz received her M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2022. Since 2021 she is working at the Department for Cybersecurity and Data Protection of Technische Hochschule Brandenburg. Her research work is focused on Cybersecurity and Management, Data Protection, IoT, and Smart Home Security.

Klaus Schwarz received his B. Sc. and M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017 and 2020, respectively. His research interests include Open Source Intelligence (OSINT) and Cybersecurity, Artificial Intelligence, and Mechatronics related topics such as Autonomous Driving and Multimodal Image Exploitation and Learning. As a faculty member, he is developing a graduate program in Applied Mechatronic Systems with a focus on Artificial Intelligence at SRH Berlin University of Applied Sciences.

Reiner Creutzburg is a retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019 he is a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.