Detecting Morphed Face Images

R. Raghavendra Kiran B. Raja Christoph Busch
Norwegian Biometrics Laboratory, NTNU, 2802 Gjøvik, Norway
Email: {raghavendra.ramachandra; kiran.raja; christoph.busch} @ntnu.no

Abstract

Widespread deployment of Automatic Border Control (ABC) along with the electronic Machine Readable Travel Documents (eMRTD) for person verification has enabled a prominent use case of face biometrics in border control applications. Many countries issue eMRTD passports on the basis of a printed biometric face photo submitted by the applicant. Some countries offer web-portals for passport renewal, where citizens can upload their face photo. These applications allow the possibility of the photo being altered to beautify the appearance of the data subject or being morphed to conceal the applicant identity. Specifically, if an eMRTD passport is issued with a morphed facial image, two or more data subjects ,likely the known applicant and one or more unknown companion(s), can use such passport to pass a border control. In this work we propose a novel scheme to detect morphed face images based on facial micro-textures extracted using statistically independent filters that are trained on natural images. Given a face image, the proposed method will obtain a micro-texture variation using Binarized Statistical Image Features (BSIF), and the decision is made using a linear Support Vector Machine (SVM). This is first work carried out towards detecting the morphed face images. Extensive experiments are carried out on a large-scale database of 450 morphed face images created using 110 unique subjects with different ethnicity, age, and gender that indicates the superior performance.

1. Introduction

Face recognition is a widely used biometric method that has become part of our everyday life. The automatic recognition of individuals observing facial biometric characteristics, especially in constrained conditions yields very high accuracy. This fact elevated face biometrics to have a prominent role in international border control [1]. Face recognition systems are built on knowledge gathered from signal and pattern recognition algorithms over the last 40 years, which has resulted in accurate and reliable face recognition algorithms. This performance increase has permitted the use of face biometrics in diverse applications that range from forensics, surveillance, physical and logical access control to e-Commerce and e-Government applications.

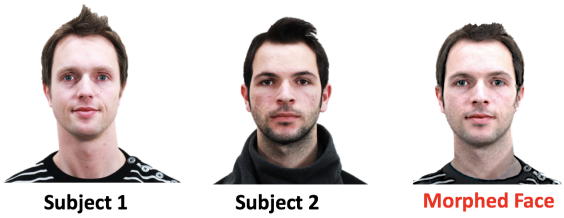

Figure 1: Example of face morphed image

Biometric facial reference images have become an important part of electronic passports [9], which have reached after a ten year introduction period now a deployment of close to 800 million passport instances. Thus face recognition based on these passports has become a prominent application [1] in border control environment. One of the reasons that face recognition was chosen for the border control scenario is that, in case of a false negative system decision, a visual comparison can be conducted by the border control officer, which is a distinct advantage over other biometric modalities (e.g. fingerprint recognition). These factors justify the applicability of face recognition in Automatic Border Control (ABC) e-gates [6]. In a typical ABC system, the link between the electronic Machine Readable Travel Document (eMRTD) and the passport holder (i.e the individual presenting the eMRTD to the border guard) will be automatically verified by comparing the live captured face image with the facial reference image stored in the eMRTD passport. This has boosted the benefits provided by ABC systems, which can be attributed to highly reliable and accurate border control processes.

The International Civil Aviation Organization (ICAO) [9] has decided to require a facial image as the primary identifier for machine readable travel documents (MRTD). Thus, the facial image is the only biometric reference that

is present in all electronic passports globally [1]. With the widespread adoption of ABC systems, the vulnerability of face recognition subsystems as the relevant technological ABC-component, to different kinds of attacks has gained more attention. These attacks can broadly be classified in two types: (1) Attacks on the ABC system: These attacks are typically carried out on the capture device (or camera) by presenting a face artefact. Such attacks are referred to as face spoofing or presentation attacks. However these attacks require a high effort in generating a face artefact (i.e. artificial presentation attack instrument) and also in presenting the same to the ABC e-gate. Furthermore this kind of attack can only be successful, if the attacker can gain access to a lost or stolen eMRTD passport that will allow him to prepare the face artefact that can resemble the face photo present in the eMRTD passport. (2) Attacks on the eMRTD biometric reference: Here attacks could be considered to manipulate the biometric data stored in the logical data structure (LDS) of the (stolen) passport, with the intent to replace the reference image. Such attacks could easily be spotted as the hash computed over the facial image data field would be changed. A more effective approach is to exploit the deficiencies in the passport application and issuing protocol. This attack is simple to conduct, as most of the passport issuing procedures will accept a (printed) face photo during the application process. Furthermore, there are several countries that will accept the digital photo upload to a web-portal for renewal of the passport as well as for a VISA application. This will provide ample opportunity for an attacker to submit altered face photo to the passport issuing agency and in turn receive an authentic eMRTD passport with all physical and electronic security features and containing the altered photo. One can argue that the use of biometric kiosk at the passport enrolment can mitigate this effect, but such live enrolment kiosks are available in only very few passport application offices.

In order to execute an attack on the eMRTD biometric reference image, alterations can be performed easily with freely available software [5]. Among the different kinds of face image alterations (geometric, aspect ratio and beautification), the face morphing is emerging as the most critical attack on ABC border control systems [4] [10]. The objective of face morphing is to generate a new face image using the unique information available from two or more different source face images corresponding to two or more different subjects. Thus the morphed face image will essentially constitute the facial appearance features corresponding to multiple data subjects that have contributed to the morphed face. This will provide an opportunity for any attacker (e.g. a known criminal) to morph his facial image with another (innocent) data subject's facial image and apply for a eMRTD passport that can be used by both subjects. A recent study [4][5] has demonstrated the inability of humans to detect morphed facial images. Since eMRTD passport can now widely be used with ABC systems for border control, any attacker can execute this attack without ever forging a passport document. Thus, these kind of attacks need to be mitigated to assure the security of border control processes.

The vulnerability of the enrolment process for face morphing attacks was first indicated in [10] and recently demonstrated in [4] on commercial face recognition algorithms. Experiments conducted on a relatively small database consisting of ten male and nine female morphed face images have indicated the vulnerability of the commercial-of-the-shelf (COTS) face recognition systems. In [5], the difficulty in detecting a face morphing is emphasized by presenting the image pair to a group of human observers including face recognition experts (44 border guards, 439 biometric experts along with 104 common persons with limited knowledge on biometrics). The study concluded that even face recognition experts fail to detect morphed face images. To date there is no approach reported to detect a morphed face image automatically.

In this work, we present a novel framework to detect morphed face images. The proposed method is based on the observation of micro-textures using Binarised Statistical Image Features (BSIF). Classification is carried out using a linear Support Vector Machine (SVM). To the best of our knowledge, this is the first work that addresses morphed face detection using BSIF features. Extensive experiments are carried out on our newly constructed large-scale morphed face database with 450 different morphed face samples. The database is constructed with 110 subjects from different ethnicity, age and gender. Thus the following are the main contributions of this paper: (1) New large-scale face morphed database with 450 morphed images generated using 110 subjects. (2) Extensive study on the vulnerability of a commercial-off-the-shelf (COTS) face recognition system on our newly created database of morphed face images. (3) Novel scheme to automatically detect morphed face images. (4) Extensive experimental analysis of the proposed morphed face detection system on our newly collected database. In addition, we also compare the performance of the proposed texture descriptor with four different contemporary schemes that are predominately used in the biometric community for face anti-spoofing (or presentation attack detection).

The rest of the paper is organized as follows: Section 2 provides information on our morphed face database, Section 3 presents the details of the proposed morphed face detection scheme, Section 4 discuss the quantitative results and Section 5 draws the conclusion.

[1] Countries of the European Schengen Zone store additionally left and right fingerprint images

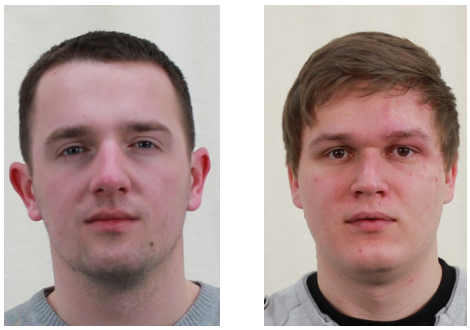

Figure 2: Example of images captured from data subjects that are used to generate a morphed image

2. Database construction

In this work, we constructed a new large-scale morphed face database comprised of 450 morphed images generated using different combination of facial images stemming from 110 data subjects. The first step in the data collection is to capture the face images following the ICAO capture standards [9] as defined in the eMRTD passport specification. To this extent, we first collect the frontal face images in a studio set up with uniform illumination, uniform background, neutral pose and normal facial expression. The images are captured using a Canon EOS 550D DSLR camera mounted on a tripod and placed at a distance of 2 meters. Figure 2 shows examples of captured high-quality face images of two data subjects.

The morphed face images are generated using the freely available GNU Image Manipulation Program v2.8 (GIMP) and GIMP Animation Package (GAP) tools. The two face images that are going to be morphed are manually aligned and provided as an input to the GAP tool. The GAP tool will generate a sequence of image frames showing the translation of one subject to another. The final morphed image is selected manually by confirming its resemblance to the faces of the contributing subjects to the morphing process. The Figure 3 shows the examples of the morphed face image that is obtained using two different subjects. Contrary Figure 4 shows the morphed face image obtained using three different data subjects. Since our database is comprised of the 110 subjects belonging to different ethnicities (Caucasian, European, American, Latin American, Asian and Middle Eastern), we have explored both two subject and three subject combinations between the various ethnicities as well as different genders. Thus, this is the first database with a variety of ethnic origin along with a large number of subjects that are combined to obtain 450 different morphed face images.

Figure 3: Examples of morphed face images generating using two different subjects

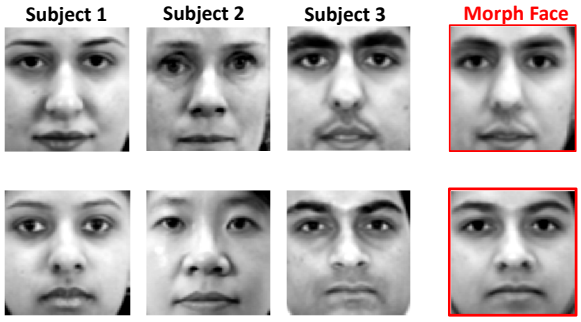

Figure 4: Examples of morphed face images generating using three different subjects

2.1. Performance assessment protocol

In order to adequately evaluate the morphed face database and to benchmark the morphed face detection algorithms, we divided the whole database of 450 morphed images to three independent sub-sets as training set, development set and testing set. The training set comprises 200 morphed images, which are used exclusively for training of the SVM classifier. The development set comprises 50 morphed images, which are used to tune the parameters of the proposed scheme especially in selecting the size and length of the BSIF filter. The testing set is comprised of 200 morphed images, which are solely used to report the results of the morph face detection algorithms.

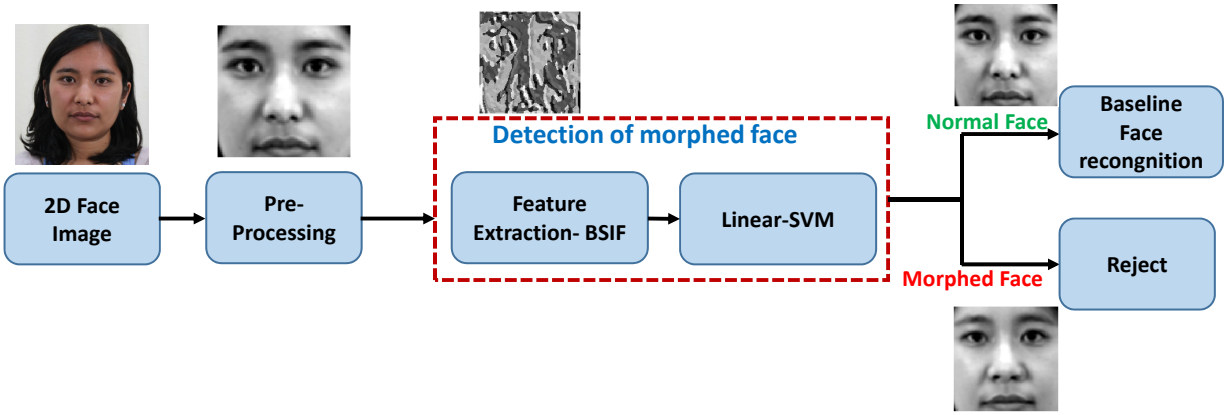

Figure 5: Block diagram of the proposed approach for morphed face image detection

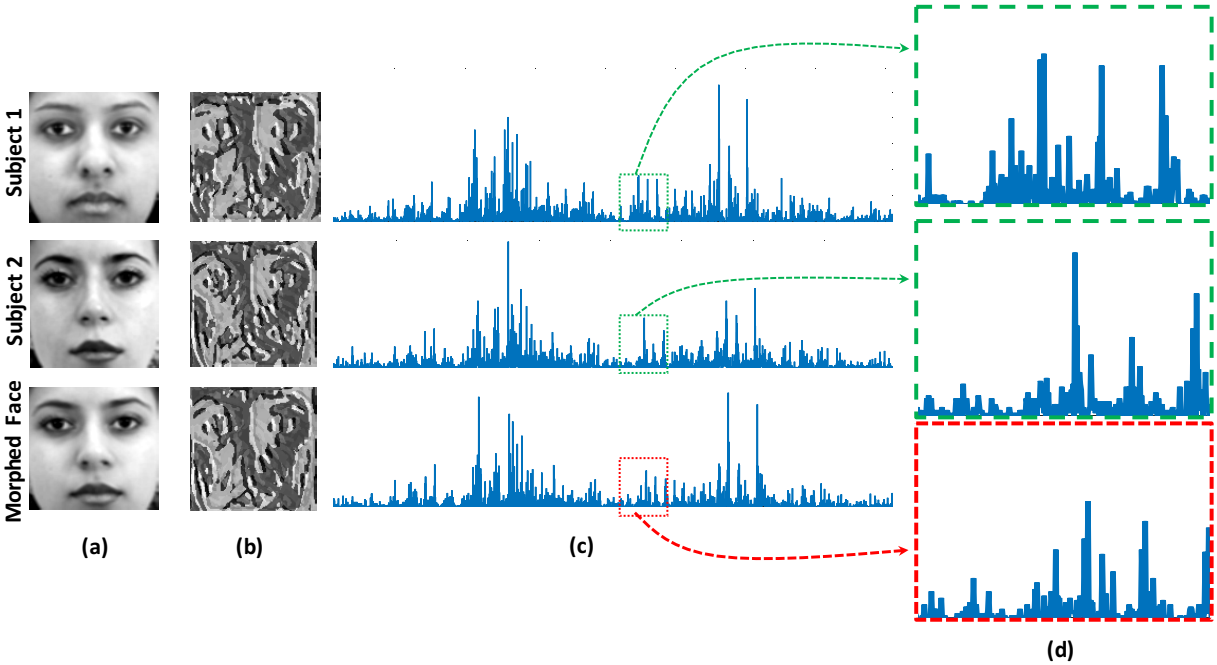

Figure 6: Qualitative Results of BSIF with size 11×11 with 12-bit length on normal and morphed face images: (a) Normalised face images, (b) BSIF features represented as the image, (c) Normalised BSIF feature histogram, (d) Enlarged histogram profile corresponding to some bins.

3. Proposed morphed face detection framework

Figure 5 shows the block diagram of the proposed approach for robust morphed face image detection. The proposed method is structured using two main steps namely: pre-processing and morphed face detection.

3.1. Pre-processing

The idea of the pre-processing is to extract the normalized face region. In this work, the face detection is carried out using the Viola-Jones algorithm [22] by considering its known robustness and performance in a real-world scenario. The face images used in this work are captured in constrained conditions with uniform illumination, neutral pose, and neutral expression. Thus, the employed face

detection method has indicated an accurate face detection. In the next step, the face image is normalized to compensate rotation using the affine transform as introduced in [20]. Finally, the normalized face images are resized to 120×120 pixels.

3.2. Morphed face detection

The proposed morphed face detection is based on the micro-texture features extracted from a normalized face image using BSIF filters [11] that are classified using a linear SVM. The BSIF features are obtained from the image, while representing each pixel as a binary code by computing its response to a filter that is trained on statistical properties of natural images. In this work, we have employed the open-source filters [11] that are trained using 50000 image patches randomly sampled from 13 different natural scenic images [8]. The statistically independent filters are trained based on unsupervised learning using the Independent Component Analysis method [21]. The Binarized Statistical Image Features (BSIF) have already been used in many other biometric applications and have indicated an strong verification performance on various biometric modalities including face [11], iris [12], periocular [13] and palmprint [18]. BSIF features have also been used to detect biometric artefacts (or spoofing or presentation attacks) such as face and iris objects [17]. In addition the BSIF features have also shown a robust performance in detecting contact lenses [19] [14] in the eye. By considering this success, we intend to explore the BSIF [11] features for the morphed face detection.

Given the normalized face image I_f, we extract the BSIF features by performing the convolution of I_f with the BSIF filters. Since the BSIF filters are generated based on unsupervised learning, one can generate any number of filters with different sizes. In this work, we have evaluated 8 different filter sizes such as 3×3, 5×5, 7×7, 9×9, 11×11, 13×13, 15×15 and 17×17 and with 8 different bit lengths such as 5,6,7,8,9,10,11 and 12. Finally, we selected the filter of size 11×11 with 12-bit length by considering its accuracy based on our experiments on the development dataset (see Section 2.1).

Figure 6 shows the qualitative results of BSIF features obtained on both normal and morphed face images using a filter size of 11×11 with 12-bit length. It is interesting to observe that the BSIF histogram features (Figure 6 (c)) indicate the variations in the histogram profile between normal and morphed face image. The difference can be seen further by zooming into the histogram profile in corresponding bins in all three face images as indicated in Figure 6 (d). In this work, we have used the normalized histogram features obtained from 11×11 with a 12-bit filter on the normalized face image I_f that will result in a dimension of 1×4096. We then employ the linear SVM classifier to determine whether the presented face image belongs to the normal or the morphed class. The SVM classifier is first trained using a set of positive (normal faces) and negative (morphed) samples according to the standard protocol described in the Section 2.1.

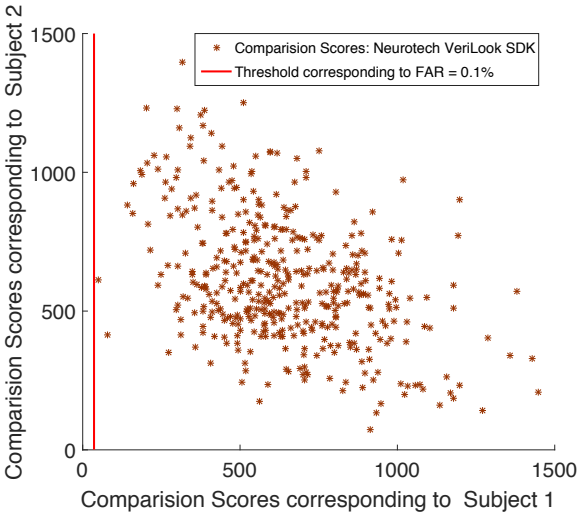

Figure 7: Comparison scores obtained using COTS [3] by comparing a morphed face image (enroled reference image) with normal face image (probe image) corresponding to one of the contributing subjects of morphed face image.

4. Experiments and results

In this section we present quantitative results of the proposed scheme for automated morphed face detection. We first present the results regarding the vulnerability experiments carried out on the COTS, and then we present the quantitative results of the proposed morphed face detection approach.

4.1. Vulnerability of morphed face database

We present a vulnerability analysis results on our morphed face image database constructed in this work. To this extent, we have used Neurotechnology's Verilook face recognition SDK [3] to evaluate its vulnerability regarding morphed face images. The experiments are carried out by enroling a morphed face image to the COTS (Verilook face recognition SDK), and using a probe sample corresponding to one of the data subjects that have contributed to generate the enroled morphed image. Thus, for each enroled morphed face, we will get either two or three different comparison scores depending on the number of subjects used to create an enroled morphed face image.

Figure 7 shows the scattered comparison scores obtained on the whole database comprised of 450 morphed images

using Verilook face SDK. The effectiveness of these obtained comparison scores is assessed by fixing the threshold of the COTS face recognition SDK following the guidelines of FRONTEX (the European Agency for the Management of Operation Cooperation at the External Borders of the Member States of the European Union) [6]. FRONTEX advocates the face verification algorithm in an ABC system operating in the verification mode to provide a performance of False Acceptance Rate (FAR (%)) = 0.1% and False Reject Rate (FRR%) lower than 5%. In our experiments we have used the threshold provided by the SDK, which is 36 for the given FAR = 0.1% [3]. The red line in the Figure 7 indicates this verification threshold value (36) corresponding to the target FAR = 0.1%. Thus, the comparison scores greater than 36 are considered as successful verifications. As noticed from Figure 7 all morphed images are successfully matched for this threshold and thereby indicating the attack potential of our morphed face images for real-world applications.

4.2. Quantitative results of the morphed face detection scheme

In this section, we present the quantitative results of the proposed scheme for automated morphed face detection. In addition to the proposed scheme, we have also evaluated four different contemporary feature extraction schemes such as Image Quality Analysis (IQA), Local Binary Patterns (LBP), Local Phase Quantisation (LPQ) and 2D Fast Fourier Transform (2DFFT). These features are selected by considering their relevance to the problem and also their accuracy in recent Presentation Attack Detection work. The classification of these feature extraction scheme is carried out with linear SVM to be consistent with the proposed scheme.

Since this is the first work on automated morphed face detection, we define two different performance evaluation metrics to quantify the results such as (1) Normal Face image Classified as Morphed face image (NFCM): The ratio of normal face images classified as morphed face image. (2) Morph Face image Classified as a Normal face image (MFCN): The ratio of morphed face images classified as normal face. The overall accuracy can be measured using an Average Classification Error Rate (ACER) defined as: ACER = $\frac{(NFCM+MFCN)}{2}$.

Table 1 indicates the quantitative results of the proposed algorithm along with the four different baseline algorithms employed in this work. Based on the obtained results the following can be observed:

- The best performance is noted for the proposed scheme with an ACER of 1.73%.
- The best MFCN is noted for the image quality analysis features with MFCN of 1.73%, but the NFCM value for this setting is quite high with 73.37%, which is not applicable in a real-world scenario.

Table 1: Quantitative performance of the proposed scheme on the morphed face detection database

Algorithms	MFCN (%)	NFCM (%)	ACER (%)
Image quality [7] - SVM	1.73	73.37	37.55
LBP [16] - SVM	37.66	13.20	25.43
LPQ [2] - SVM	29.00	11,47	20.23
2DFFT [15] - SVM	61.03	37.22	49.12
Proposed Method	**3.46**	**0**	**1.73**

Based on the obtained results, the use of statistical image features based on the BSIF filters has demonstrated the best performance when compared with the conventional feature extraction techniques. The obtained results demonstrate the applicability of the proposed scheme for automated morphed face detection.

5. Conclusion

Recent changes in the electronic Machine Readable Travel Documents (eMRTD) such as passports, which can store biometric reference images (e.g. 2D facial images) for person verification, have now enabled automatic border control operations. Many countries around the globe issue eMRTD passports based on the face photo submitted by the applicant during the initial application. This will give ample opportunity for any individual with e.g. criminal background to generate a manipulated/morphed face image with the help of another subject (companion with clean background, who serves as the eMRTD applicant). The manipulated images is submitted during the eMRTD application process with the intent to get an authentic eMRTD document. Since such morphed face photos can in general not be spotted through visual inspection by a human operator, the criminal has a high chance to receive from his companion the authentic eMRTD that supports both the criminal and the companion in passing through biometric verification at border crossing. In this work we have addressed this important research aspect of automated morphed face detection, which was not explored in any of the earlier work. To this extent, we have proposed a new framework based on studying the statistical image features captured using Binarized Statistical Image Features (BSIF) and a final decision is obtained using linear Support Vector Machine (SVM). Extensive experiments are carried out using morphed face database comprised of 450 morphed face images generated using 110 unique subjects with different age, ethnicity, and gender. We have presented an extensive experiment that indicated intense vulnerability of Neurotechnology Verilook face recognition SDK on morphed face images. The ob-

tained results have shown that all 450 morphed face images are successfully verified, while operating on a threshold (FAR = 0.1%) that is recommended by FRONTEX. We have also presented an extensive experiment on the proposed automated morphed face detection scheme along with four different contemporary baseline algorithms. The obtained results have indicated the best performance with an average classification error (ACER) of 1.73% that shows the applicability of the proposed scheme for a real-world scenario.

Acknowledgment

This work is carried out under the funding of the Research Council of Norway (Grant No. IKTPLUSS 248030/O70).

References

[1] Easypass – grenzkontrolle einfach und schnell. http://www.bundespolizei.de/DE/01Buergerservice/Automatisierte-Grenzkontrolle/EasyPass/_easyPass_anmod.html, 2014. Accessed: 2014-08-19.

[2] A. Benlamoudi, D. Samai, A. Ouafi, S. Bekhouche, A. Taleb-Ahmed, and A. Hadid. Face spoofing detection using multi-level local phase quantization (ml-lpq). 2015.

[3] F. COTS. Verilook cots. http://www.neurotechnology.com/verilook.html, 2015. Accessed: 2015-02-08.

[4] M. Ferrara, A. Franco, and D. Maltoni. The magic passport. In *Biometrics (IJCB), 2014 IEEE International Joint Conference on*, pages 1–7, 2014.

[5] M. Ferrara, A. Franco, and D. Maltoni. *Face Recognition Across the Imaging Spectrum*, chapter On the Effects of Image Alterations on Face Recognition Accuracy, pages 195–222. Springer International Publishing, 2016.

[6] Frontex. Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, 2015.

[7] J. Galbally, S. Marcel, and J. Fierrez. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *Image Processing, IEEE Transactions on*, 23(2):710–724, Feb 2014.

[8] A. Hyvèarinen, J. Hurri, and P. O. Hoyer. *Natural Image Statistics*, volume 39. Springer, 2009.

[9] International Civil Aviation Organization NTWG. Machine Readable Travel Documents – Part 1 Volume 1 – Passports with Machine Readable Data Stored in Optical Character Recognition Format. http://www.icao.int/publications/pages/publication.aspx?docnum=9303, 2006.

[10] International Organization for Standardization. *19792:2009, Security techniques Security evaluation of biometrics*, 2009.

[11] J. Kannala and E. Rahtu. Bsif: Binarized statistical image features. In *Pattern Recognition (ICPR), 2012 21st International Conference on*, pages 1363–1366, 2012.

[12] Kiran B. Raja, R. Raghavendra, and C. Busch. Binarized statistical features for improved iris and periocular recognition in visible spectrum. In *2nd International Workshop on Biometrics and Forensics (IWBF 2014)*, pages 1–4, 2014.

[13] Kiran B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch. Smartphone authentication system using periocular biometrics. In *Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the*, pages 1–8. IEEE, 2014.

[14] J. Komulainen, A. Hadid, and M. Pietikinen. Generalized textured contact lens detection by extracting bsif description from cartesian iris images. In *Biometrics (IJCB), 2014 IEEE International Joint Conference on*, pages 1–7, 2014.

[15] J. Li, Y. Wang, T. Tan, and A. K. Jain. Live face detection based on the analysis of fourier spectra. In *Defense and Security*, pages 296–303. International Society for Optics and Photonics, 2004.

[16] J. Maatta, A. Hadid, and M. Pietikainen. Face spoofing detection from single images using micro-texture analysis. In *Biometrics (IJCB), 2011 International Joint Conference on*, pages 1–7, Oct 2011.

[17] R. Raghavendra and C. Busch. Presentation attack detection algorithm for face and iris biometrics. In *Signal Processing Conference (EUSIPCO), 2014 Proceedings of the 22nd European*, pages 1387–1391, 2014.

[18] R. Raghavendra and C. Busch. Texture based features for robust palmprint recognition: a comparative study. *EURASIP Journal on Information Security*, 2015(1):1–9, 2015.

[19] R. Raghavendra, K. B. Raja, and C. Busch. Ensemble of statistically independent filters for robust contact lens detection in iris images. In *Proceedings of the 2014 Indian Conference on Computer Vision Graphics and Image Processing*, ICVGIP '14, pages 24:1–24:7. ACM, 2014.

[20] V. Struc. *The PhD face recognition toolbox : toolbox description and user manual*. Faculty of Electrical Engineering Ljubljana, 2012.

[21] J. H. van Hateren and A. van der Schaaf. Independent component filters of natural images compared with simple cells in primary visual cortex. *Proceedings of the Royal Society of London. Series B: Biological Sciences*, 265(1394):359–366, 1998.

[22] P. Viola and M. J. Jones. Robust real-time face detection. *International Journal of Computer Vision*, 57(2):137–154.