A. Brömme, C. Busch, A. Dantcheva, K. Raja, C. Rathgeb and A. Uhl (Eds.): BIOSIG 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 1

Biometric System for Mobile Validation of ID And Travel Documents

Iurii Medvedev[1], Nuno Gonçalves[2], Leandro Cruz[3]

Abstract: Current trends in security of ID and travel documents require portable and efficient validation applications that rely on biometric recognition. Such tools can allow any authority and citizen to validate documents and authenticate citizens with no need of expensive and sometimes unavailable proprietary devices. In this work, we present a novel, compact and efficient approach of validating ID and travel documents for offline mobile applications. The approach employs the in-house biometric template that is extracted from the original portrait photo (either full frontal or token frontal), and then stored on the ID document with use of a machine readable code (MRC). The ID document can then be validated with a developed application on a mobile device with digital camera. The similarity score is estimated with use of an artificial neural network (ANN). Results show that we achieve validation accuracy up to 99.5% with corresponding false match rate = 0.0047 and false non-match rate = 0.00034.

Keywords: Document security, biometric template, active appearance model, artificial neural network.

1 Introduction

Nowadays, protecting portrait photos on ID and travel documents is of key importance for issuing and legal authorities as face is one of the most largely deployed biometric source [IB08]. That is why the face spoofing attacks widely affect high security field in the companies, government sectors [KSK17]. These attacks usually can be hardly detected by humans as even well trained officers usually perform poorly in matching unfamiliar faces on photos of ID documents, that is why automated systems for efficient document validation are required [SJ19]. Despite all the recent evolution in the facial biometric verification and recognition technologies, when designing security documents and systems, some aspects are relevant. On the one hand, the trend is to allow the validation of documents in totally offline systems, which are designed for scenarios where connectivity may be compromised in terms of availability and security (thus avoiding hacking attacks - such as man-in-the-middle). On the other hand, because of the use of mobile non-proprietary devices, such as smartphones, which are nowadays almost ubiquitous in the hand of authority agents and citizens.

[1] University of Coimbra, Institute of Systems and Robotics - Coimbra, Portugal, iurii.medvedev@isr.uc.pt
[2] University of Coimbra, Institute of Systems and Robotics - Coimbra, Portugal; Portuguese Mint and Official Printing Office (INCM), Lisbon, Portugal, nunogon@deec.uc.pt, Nuno.MiguelGoncalves@incm.pt
[3] University of Coimbra, Institute of Systems and Robotics - Coimbra, Portugal; Portuguese Mint and Official Printing Office (INCM), Lisbon, Portugal, Leandro.Cruz@incm.pt

Consequently, many use cases that rely on facial verification or facial recognition using physical documents are now being designed to allow a fully offline validation with a minutia information extracted from sources of biometric data (such as faces, fingerprints, iris, among others), without storing or accessing databases of face images.

In this paper we present a novel, efficient and compact method for offline mobile applications to secure ID and travel documents with the use of in-house designed facial biometric template and machine readable codes. We are interested in the face photo of documents, either full frontal or token frontal, according to the ISO specifications ISO/IEC 19794-5 [IS11]. Although focused on the face photo, it is worth noting that any source of biometric data (like fingerprint pattern or iris) that can be acquired to perform validation may be employed instead.

The presented approach then solves the document verification task, and does not demand that the biometric samples and features to be stored in any database. This type of validation is sometimes called a match-on-card process.

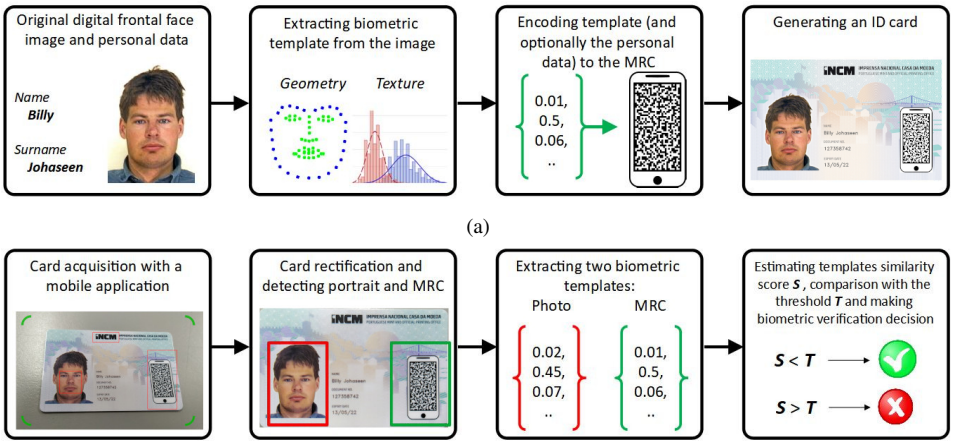


Fig. 1: Pipeline for ID generating(a) and validating(b) in the proposed system.

In our document validation system, we encode the biometric template, that is extracted from a digital frontal face image, within a MRC, and print the resulting code image on the document of an individual (Fig. 1). The approach assumes that the valid MRC for arbitrary biometric sample cannot be recreated by impostors, thus preventing them from issuing the fake identification document that matches different identity. In order to validate the document, the two biometric templates, one from the frontal face photo on its surface and the other from the machine-readable code, are extracted from the testing document to finally be compared to determine if they belong to the same individual. As stated before, this validation shall be performed totally offline. It is important to notice that the biographic data (name, date of birth, etc.) can also be included into the MRC in order to prevent any document ID with original photo and valid MRC to match the data of another individual.

The presented method is related with face recognition problem, however we do not attempt to solve it in its usual formulation. The main goal is to secure a document sample at the moment of its personalization. That is why the problem being solved is the protection of the single document face image itself from biometric impostor attacks like replacing or changing it, into a different identity.

2 Related Work

Recent achievements in different types of face manipulation have made the topic of face forensic recognition to become important for research and investigations [ADB19]. Consequently, document security issues thus encounter new challenges and require efficient methods for face photo security purposes. In [Am19] authors consider a number of different face recognition methods (also including facial landmark-based) in forensics purposes. The paper [DC15] was focused on developing a framework for facial forensics application also related with ID cards fraud. Worth noting that most of the current solutions for document validation are proprietary commercial systems that rely on unpublished algorithms and methods, thus making them difficult to compare with. Consequently, existing benchmarks [GN14] have some submission restrictions.

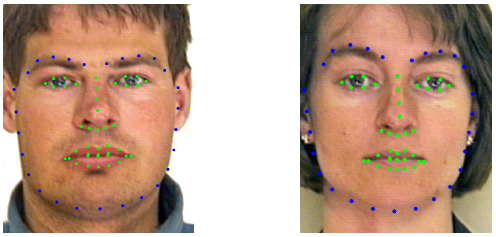
In relation to industry solutions for ID and travel documents, some products have been developed recently. Two approaches are the Digital IPI from Jura [KA04] and both Lasink and DocSeal from IDEMIA [JE19]. They are focused on validation solutions for ubiquitous devices not only to make widely available the access to the authenticity of documents and products, but also to reduce the considerable equipment costs. The main idea of these approaches is to conceal a personalized data within the printed photo that can be further decoded with use of mobile application. Our solution is comparable to these two products, however as they are non-publicly available (both solution and validation dataset), this does not allow one to perform a proper benchmark.

In purposes of face recognition and validation the approaches based on active appearance model (AAM) has been widely used [CET01]. In [ASAAO13], authors use features extracted from AAM of a face and SVM for making a comparison decision. The approach presented in [Ou14] is focused on analysing geometric face distances. The face recognition method in [JP17] is based on face geometric invariances. Modern face recognition approaches usually rely on employing CNN based deep neural networks and use facial landmarks only in alignment [SKP15] or frontalization processes [Ha14]. However, these methods are still computationally heavy especially for application in mobile devices.

3 Facial Biometric Template

Due to limitations of computing power on target platforms, the choice of facial biometic template implementation was made aiming to achieve a trade-off between the calculating complexity and efficiency of its application. We consider the fact that ID and travel documents generally contain frontal face image, where a well-known active appearance model

can be applied (Fig. 2). The model we use contains 68 facial landmarks and denotes the external contour of the face, mouth, eyes, nose, and eyebrows [Re14]. This character of the markup allows one to further determine the various parameters of the face from its image, which can be used for processing by other algorithms.



(a) (b)

Fig. 2: Face image with detected facial landmarks of a man(a) and a woman(b) [Ps].

From the detected set of facial landmarks, we extract values of their coordinates. Nonetheless, those raw data require some normalisation due to the arbitrariness of face location, size and pose on the source image. We solve that problem by performing the following procedure. Firstly, we introduce some predefined set of face feature points. The goal of introducing that supporting set of landmarks is to be the base for aligning other sets of face feature points. If coordinates of two different sets of points are aligned to this supporting set, they will be aligned to each other. As a supporting set in this paper, we choose landmarks detected on artificially generated average face image depicted in Fig. 3a.

In order to align input set of points $\{x_i, y_i\}$ with the supporting set of points, we transform its coordinates to $\{x'_i, y'_i\}$ by rotating, scaling, and shifting it (eq. (1)). The rotation angle α is obtained in order to align input face contour with the horizon (supporting set is already aligned). Although this is a standard procedure, the novelty presented by our work is the scaling, which is performed by the values of face contour perimeter (P_{sup} for supporting set and P for the input set), which is defined by the subset of points with indices 0-26 (blue points on Fig. 2). The shifting vector $S(s_x, s_y)$ is an offset between the average points of supporting and already scaled input sets.

$$\begin{bmatrix} x'_i \\ y'_i \end{bmatrix} = \frac{P_{sup}}{P} * \begin{bmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{bmatrix} * \begin{bmatrix} x_i \\ y_i \end{bmatrix} + \begin{bmatrix} s_x \\ s_y \end{bmatrix} \tag{1}$$

The set of values that will be a included into a facial biometric template is a result of element-wise subtraction of input and supporting facial landmark coordinates. To avoid depending upon characteristics of images, we divide all the elements of this set to the supporting face contour perimeter P_{sup}. This set of values to be included into the template contains 136 values.

To make the template more robust against biometric distortion attacks (eg. the face image of an impostor can be warped in order to be more geometrically similar to the original identity), texture features are also included into it. In order to extract them, the input face image is aligned with the supporting image, and further segmented in ten characteristic re-

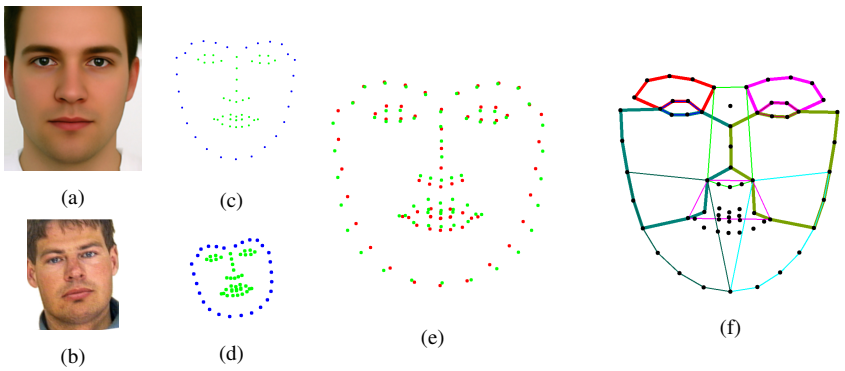


Fig. 3: The process of coordinate recalculating a) supporting face image; b) input face image to be aligned; c) supporting facial landmarks (FL); d) input image FL; e) set of input FL (green) that is aligned with supporting set of FL(red); e) face region contours for extracting HOG features.

gions which are chosen to distinguish face semantic areas (Fig. 3f).Finally for each region features based on histograms of oriented gradients (HOG) are extracted [De11]. This results in 80 features that are concatenated into the resulting biometric template which then contains $D\_size = 216$ elements $\{d_i\}$.

3.1 Template verification

From the ID document that is claimed to be validated, two facial biometric templates are extracted. First $\{d\_test_i\}$ is from the physical face photo that might be forged, and the second $\{d\_orig_i\}$ that is stored on the document, which is assumed to be original. In order to recognize the tested document as genuine, extracted biometric templates are compared between each other. Such straightforward validation can be realised by applying Euclidean distance (eq. (2)). The value of the resulting E in fact indicates the distance score between the templates and can be compared with some threshold in order to trigger the validation decision. Nonetheless, this trivial linear approach does not consider impact weights of different landmarks and seems to be naive and simplistic.

$$E = \sum_{i=1}^{D\_size} |(d\_test_i - d\_orig_i)| = \sum_{i=1}^{D\_size} |d\_sub_i| \tag{2}$$

In order to perform a more robust verification, we solved a binary true-false classification task by designing a multilayer perceptron, where the first layer receives the result of element-wise subtraction of templates. For training that classifier, we employ a classical random sequential back-propagation algorithm [YM98]. The final layer contains one node and returns a response scalar S in the range [0,1].

The input layer of this network receives an element-wise absolute difference of two biometric templates d_sub_i normalised by the coefficient N (see eq. (3)). The purpose of in-

troducing N and limiting the input values to 1 is to fit them within the range of the first layer activation function. In our experiment, the best results are obtained with $N = 0.015$ for geometry based elements and $N = 0.1$ for texture based ones.

$$d\_inp_i = max(1, \frac{|d\_sub_i|}{N}) \tag{3}$$

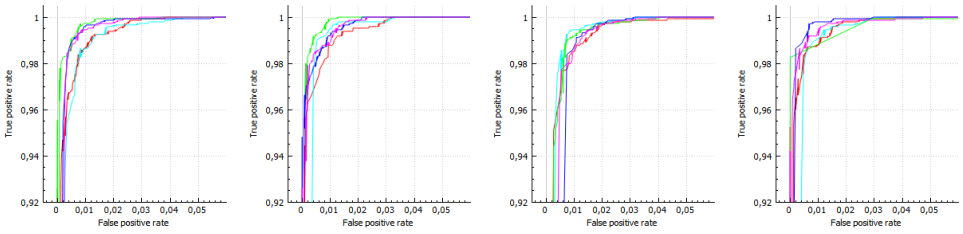
3.2 Classifier Training and Tests

Due to specificity of the verification task, we have prepared an in-house dataset for training, testing and estimating the efficiency of the presented approach. [4] First, a set of frontal face images of 89 individuals was prepared and printed with a size chosen in accordance with [IS19]. In a process of a real document validation with a mobile device, we assume to perform document acquisition with conventional digital camera. In order to follow these conditions properly in training and tests the printing of the dataset is required. These images were used to perform acquisitions similar to Fig. 1a with use of conventional smartphone digital camera (Huawei P20 Pro was used in our tests) and further a perspective transformation based on the structure of the ID document (see Fig. 1b). As a source of frontal face images a dataset from [Ps] was chosen. We have acquired around 4.5 thousand face image samples and in a combination with 89 original digital images, combined around 9 thousand pairs in order to extract a balanced set of $\{d\_sub_i\}$. Each pair of samples contains an original digital image and a rectified capture of the printed image for validating. Pairs with both images belonging to the same identity correspond to the true comparison decision, while the opposite situation imitates a biometric impostor attack of face image replacing. This data was divided into train (70%) and test (30%) parts with different (disjoint) identities in both parts. On this dataset the network learns not only the proper weights for the particular template elements but also learns to avoid noise related with printing, acquisition and rectification inaccuracies.

3.3 Results

For the purpose of choosing a better architecture of the classifier, we have tested a number of different ones. Here we aim to achieve the trade-off between the classifier performance and computing complexity. To evaluate the performance, we build ROC (receiver operating characteristic) curves and estimate their AUC (area under curve) values. (Fig. 4). Architecture with two hidden layers already gives reasonable classification efficiency for our task (Fig. 4d). However the resulting ROC curves are irregular and not smooth, what is not very convenient in practice while tuning to the required optimum between false match and false non-match rates. In our experiments results with less hidden layers were even more impractical. Increasing the number of classifier layers improves results in terms of AUC value (Table 1). At the same time, enlarging the size of the hidden layers does not impact to the performances (Fig. 4c).

[4] https://github.com/visteam-isr-uc/trustfaces-template-verification



(a) (b) (c) (d)

Fig. 4: ROC curves of ANN classifier with different architectures and different numbers of training epochs. Correspondence between labelled sub-figures and architecture is indicated in Table 1. Different colour of curves indicates different numbers of training epochs.

ANN	**AUC**				
Layers Fig. 4	***red 5ep***	***cyan 10ep***	***green 20ep***	***blue 30ep***	***purple 40ep***
216-300-400-100-1 (a)	0.9996	0.9988	0.99994	0.9992	0.9990
216-300-400-200-100-1 (b)	0.9993	0.9987	**0.99995**	0.9998	0.9998
216-300-500-400-200-1 (c)	0.9985	0.9988	0.9989	0.9979	0.9984
216-300-150-1 (d)	0.9997	0.9988	0.9993	0.9996	0.9998

Tab. 1: AUC of classifiers with different architectures.

For the classifier from the Table 1 with the best value of AUC (architecture: 216-300-400-200-100-1; 20 epochs) we estimated the value of maximum accuracy equal to 0.995 (with the minimum of incorrect classifications). It corresponds to false match rate of 0.0047 and false non-match rate of 0.00034 and is achieved for a threshold value of 0.275.

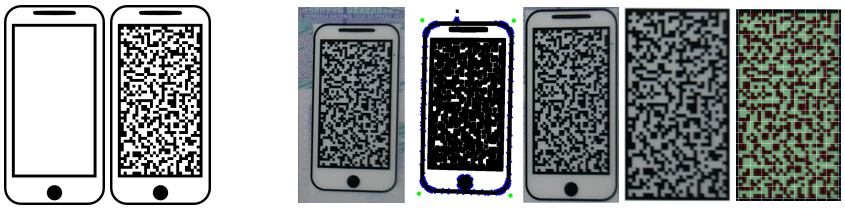
4 Application of MRC

In order to store the biometric template on the document and make it easily extractable by using a digital camera, we employ machine readable code printed on the document Fig. 1b. Namely we employ the Graphic Code from [CPG18] that can be customised for security purposes. At the stage of creating Graphic Code, several layers of security, robustness and data compressing can be added. The algorithm of creating Graphic Code remains open, even though the Graphic code itself can provide enough computational cost of cryptanalysis by specifying the alphabet that was used in the Graphic Code dictionary, the pattern size, the writing order of cells along the image, the writing order of pixels along the cell, and the dictionary itself. Here we follow the approach of symmetrical encryption where the parameters listed above are the key used both for encryption and decryption, and must be private and secured. Finally, one also can use different methods of cryptography over the data itself, when highly security level is needed. As an example, the message containing facial biometric template can be encrypted to ciphered text what can drastically increase computation complexity of cryptanalysis and security.

Another option is to follow an asymmetric encryption approach. In that case during the decoding process one just needs to prove the document issuer's authority to be sure that the document is not presented by impostor. To achieve that the template data is protected with the digital signature. The issuer authority generates the pair of private and public key. The first one is used to generate the digital signature for the created template that is added to that template to be encoded into the graphic code. With the public key the issuer of the document can be correctly validated. To keep the offline mode of the application that public key must be pre loaded on the device.

4.1 Encoding And Decoding

As a base image for the Graphic Code outline, we use the one depicted on Fig. 5a. Based on a variety of possible unit cells composed of 3×3 pixels, we have defined an alphabet that contains $N = 120$ characters. In order to code the biometric template into the Graphic Code, we transform it into the message in the alphabet space by quantisation process. Each character in the message then correspond to the letter from the alphabet and is replaced by the respective pattern in the dictionary. In addition to the biometric template some information about the individual (ID card number, name) can be also encoded for purposes of automatic document processing. The set of check digits is added to the end of the message. Finally, the remaining cells are replaced using non-dictionary patterns.



(a) (b) (c) (d) (e) (f) (g)

Fig. 5: a) - Graphic Code outline image, b) - example of created Graphic Code acquisition. The process of Graphic Code decoding from physical image: c) - detected Graphic Code image, d) - thresholding and corner detection, e) - base image rectifying, f) - code image extracting and g) - Graphic Code reconstruction.

The decoding of MRC is the inverse to the encoding, and receives the same key parameters that are stored on the device. However, the acquired code image is also needed to be prepossessed and rectified, what is performed with common computer vision algorithms. (Fig. 5c - 5g). During the decoding, the rectified image (Fig. 5f) is overlaid with the grid, then scanned, to find patterns from the dictionary and add corresponding characters to the result message. In that process multiple errors can occur due to various reflection, distortion, MRC surface attrition. That is why after having the full message extracted, its content is validated with the use of check digits. In order to prove the robustness of the decoding we performed extensive tests with the various lighting conditions and applied deformations to the MRC. Most of inaccuracies are mitigated by processing the sequence of multiple camera frames. Only the deformations that significantly damage the MRC unit cells (such as hard scratches) lead to the impossibility of valid decoding.

5 Acknowledgment

The authors would like to thank the Portuguese Mint and Official Printing Office (INCM) and the University of Coimbra for the support of the project TrustFaces.

6 Conclusion

In this paper, we present an efficient and compact method for offline mobile applications to secure ID and travel documents using a facial biometric template and machine readable code. The method demonstrates the high level of efficiency against biometric impostor attacks. This approach solves the frontal face verification problem for purposes of securing ID and travel documents with use of smartphones. Additionally, the presented method of document validation can be expanded for usage with other biometric characteristics (such as fingerprints, iris among others). The practical application does not require sophisticated equipment, thus the approach is also quite cheap in production.

References

[ADB19] Akhtar, Zahid; Dasgupta, Dipankar; Banerjee, Bonny: Face Authenticity: An Overview of Face Manipulation Generation, Detection and Recognition. 05 2019.

[Am19] Amato, G.; Falchi, F.; Gennaro, C.; Massoli, F.; Passalis, N.; Tefas, A.; Trivilini, A.; Vairo, C.: Face Verification and Recognition for Digital Forensics and Information Security. pp. 1–6, 06 2019.

[ASAAO13] Abdulameer, M.; Sheikh Abdullah, S.; Ali Othman, Z.: Face recognition technique based on active appearance model. International Review on Computers and Software, 8:2733–2739, 11 2013.

[CET01] Cootes, T.F.; Edwards, G.J.; Taylor, Christopher: Active Appearance Models. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 23:681 – 685, 07 2001.

[CPG18] Cruz, L.; Patrão, B.; Gonçalves, N.: Graphic Code: A New Machine Readable Approach. 2018 IEEE International Conference AIVR, pp. 169–172, 2018.

[DC15] Dessimoz, D.; Champod, C.: A dedicated framework for weak biometrics in forensic science for investigation and intelligence purposes: The case of facial information. Security Journal, 29, 12 2015.

[De11] Deniz, O.; Bueno, G.; Salido, J.; De la Torre, F.: Face recognition using Histograms of Oriented Gradients. Pattern Recognition Letters, 32:1598–1603, 09 2011.

[GN14] Grother, Patrick; Ngan, Mei: Face Recognition Vendor Test (FRVT) Performance of Face Identification Algorithms NIST IR 8009. 2014.

[Ha14] Hassner, Tal; Harel, Shai; Paz, Eran; Enbar, Roee: Effective Face Frontalization in Unconstrained Images. 11 2014.

[IB08] IBG: , Biometrics market and industry report 2009-2014. International Biometric Group, Tech.Rep., October 2008.

[IS11] ISO/IEC 19794-5:2011. Information technology — Biometric data interchange formats — Part 5: Face image data. ISO/IEC JTC 1/SC 37 Biometrics, 11 2011.

[IS19] ISO/IEC 39794-5:2019. Information technology — Extensible biometric data interchange formats — Part 5: Face image data. ISO/IEC JTC 1/SC 37 Biometrics, 12 2019.

[JE19] Jones, Robert L.; Eckel, Robert Andrew: , Line segment code for embedding information in an image. U.S. Patent Application No 16/236,068, 2019.

[JP17] Juhong, A.; Pintavirooj, C.: Face Recognition Based on Facial Landmark Detection. 12 2017.

[KA04] Koltai, Ferenc; Adam, Bence: Enhanced optical security by using information carrier digital screening. In (van Renesse, Rudolf L., ed.): Optical Security and Counterfeit Deterrence Techniques V. volume 5310. International Society for Optics and Photonics, SPIE, pp. 160 – 169, 2004.

[KSK17] Kumar, S.; Singh, S.; Kumar, J.: A comparative study on face spoofing attacks. In: 2017 International Conference on Computing, Communication and Automation (ICCCA). pp. 1104–1108, 2017.

[Ou14] Ouarda, W.; Trichili, H.; Alimi, A. M.; Solaiman, B.: Face recognition based on geometric features using Support Vector Machines. In: 2014 6th International Conference SoCPaR. pp. 89–95, 2014.

[Ps] Psychological Image Collection at Stirling (PICS), hhttp://pics.stir.ac.uk/.

[Re14] Ren, S.; Cao, X.; Wei, Y.; Sun, J.: Face Alignment at 3000 FPS via Regressing Local Binary Features. In: 2014 IEEE Conference CVPR. pp. 1685–1692, 2014.

[SJ19] Shi, Yichun; Jain, Anil K.: DocFace+: ID Document to Selfie Matching. IEEE Transactions on Biometrics, Behavior, and Identity Science, 1:56–67, 2019.

[SKP15] Schroff, F.; Kalenichenko, D.; Philbin, J.: FaceNet: A unified embedding for face recognition and clustering. In: 2015 IEEE Conference CVPR. pp. 815–823, 2015.

[YM98] Y.LeCun, L. Bottou, G.B. Orr; Muller, K.-R.: , Efficient backprop, in Neural Networks—Tricks of the Trade. Springer Lecture Notes in Computer Sciences, 1998.