Detecting Face Morphing Attacks with Collaborative Representation of Steerable Features

R.Raghavendra, Sushma Venkatesh, Kiran Raja, Christoph Busch

Norwegian University of Science and Technology (NTNU), Norway
{raghavendra.ramachandra, sushma.venkatesh, kiran.raja, christoph.busch}@ntnu.no

Abstract. Passports have used face reference samples to establish and verify the identity of an individual. Face images provide high accuracy in verification and also present the opportunity of verifying the identity visually against the passport face image if the need arises. Morphed image based identity attacks are recently shown to exploit the vulnerability of the passport issuance process, when two different facial images are morphed into one image, which can match against probe images from both subjects. The challenge is further increased when the properties in the digital domain are lost after the process of print and scan. This work addresses the challenge of detecting the morphing of face images such that the attacks are detected even after the print and scan process. As the first contribution of this work, we extend an existing database with 693 bona-fide and 1202 morphed face images with the newly added of 579 bona-fide and 1315 morphed images. We further propose a new approach based on extracting textural features across scale-space and classifying them using collaborative representation. With a set of extensive experiments and benchmarking against the traditional (non-deep-learning methods) and deep-learning methods, we illustrate the applicability of the proposed approach in detecting the morphing attacks. With the obtained Bona fide Presentation Classification Error (BPCER) of 13.12% at Attack Presentation Classification Error Rate (APCER) of 10%, the use of the proposed method can be envisioned for detecting morph attacks even after print and scan process.

Keywords: Biometrics · Face morphing · spoofing attacks.

1 Introduction

Biometrics-based access to the restricted services is widely deployed in applications that include border control, smartphone unlocking, national identity card management, forensics identification among many others. Amongst several biometric characteristics, face characteristics are widely used due to the non-intrusive nature of the capture process and user convenience. Face biometrics in border control applications has carved a niche in Automatic Border Control

(ABC) gates due to feasibility of having the face biometric data on passport and compare that reference image against the probe image captured in the ABC gate. However this has been exploited recently and biometric systems are vulnerable through the use of seamless morphing attacks [2]. A morphing attack employs the process of combing the face images from two different subjects to generate one composite image, which can match to a probe image from either subjects visually and computationally. This is a pressing problem due to the fact that the passport application process in many countries relies on a printed photo provided by applicant. The process leaves the loop-hole through which the applicant can submit a morphed image such that a person with a criminal background will be able to avail the passport. The process can be scrutinized by the supervision of qualified professionals, but a recent study has established that a morphed image of sufficient quality can challenge also human experts including trained border guards to detect the subtle differences in morphed images [3] [15].

With the backdrop of those studies, the detection of morphed face image has not only gained the interest from both academia but also from the practitioners in industry who face the challenge in deployed systems. A number of techniques have been proposed in the recent years to detect the morphing attacks which can be widely grouped in two main classes: (1) Single image-based: given an image, it is classified either as morph or bona-fide. (2) Differential image-based: given two images, one captured in a controlled environment and the other image from the passport. The former class can be independent of a live for-instance in an ABC gate, while the latter is dependent of a trusted capture environments as it is given Automatic Border Control (ABC) gates, where the captured images can be compared with the image available in a passport to make the final decision.

The techniques further proposed under each of the above-mentioned categories can be of two types: (1) Digital images: The digital version of the morphed and bona-fide images are used. Countries like New-Zealand, Ireland and Estonia use the digital photograph to renew the passport. Therefore morph detection on digital images is pursued in the literature. (2) Print-Scanned: The scanned version of the printed images (either morphed or bona-fide). This represents at large-scale the real-world use-case, as the majority of countries still accepts a printed photo in the passport application process, which is then scanned and incorporated in passport. It has to be further noted that most of the reported works have focused on detecting the attacks with digital images based on (a) Engineered texture features (b) Deep learning features and (3) Image degradation features. Table 1 presents the overview of face morphing attack detection algorithms.

Observing from Table 1, it can be noted that the majority of the reported work is based on digital images and also on the single image-based approach. The popular feature extraction techniques are texture features like LBP, BSIF and LPQ [12], [1], [16]. Further, the image degradation methods based on JPEG compression [10] and DCT features [8] are also explored on the digital images. Further, the methods using pre-training deep CNN's especially using the VGG architecture[19] and fusion of features from VGG and Alex CNN architecture

Table 1: State-of-the-art face morphing attack detection algorithms

Authors	Algorithm(s)	Type of database	Type of Approach
R. Raghavendra et al. [12]	Local Binary Patterns (LBP), Binarised Statistical Image Features (BSIF), Image Gradient magnitude (IG) Local Phase Quantitation (LPQ)	Digital database	Single-image based
Andrey Makrushin et al. [8]	Quantized DCT coefficients	Digital database	Single-image based
Mario Hildebrandt et al. [6]	StirTrace technique	Digital database	Single-image based
Tom Neubert [10]	Image degradations	Digital database	Single-image based
Clemens Seibold et al. [19]	Deep CNN (VGG)	Digital database	Single-image based
Aras Asaad et al. [1]	Topological representation of LBP	Digital database	Single-image based
Ulrich Scherhag et al. [16]	Texture & frequency methods	Digital & print-scanned	Single-image based
R. Raghavendra et al. [13]	Deep learning (VGG and AlexNet)	Digital & print-scanned	Single-image based
R. Raghavendra et al. [14]	Color Textures	print-scanned database	Single-image based
Matteo Ferrara et al. [4]	De-morphing	Digital database	Differential image based
Ulrich Scherhag et al. [18]	facial landmarks	Digital database	Differential image based
Ulrich Scherhag et al. [17]	feature difference	Digital database	Differential image based

[13] are also studied on digital images. Experimental results described in [13] have indicated better performance when compared to that of the texture based methods, especially with the low-quality (or highly compressed) morph images. The color texture features [14] are explored on high-quality morphed face images. Recently, the first method on the differential image based approach using face de-morphing technique was proposed in [4]. Experiments are carried out on digital high-quality face morph show interesting and promising results. The key findings from the set of available works are:

- The majority of the works are focused on detection of a digital version of the face morphed image, especially with the single image-based approach.
- Among the available techniques, the texture based methods are widely employed.
- Deep learning techniques based on a pre-trained network are explored only with VGG and AlexNet architecture.
- The differential morphed face detection technique is explored on high quality facial images. However, the robustness of such methods are to be demonstrated with different resolution data with real-life noise (illumination and shadow) that are commonly encountered with ABC systems. As the electronic passports potentially/likely contains a print and scanned image, the robustness of the de-morphing systems must be carried out on comparing digital face image (from ABC) to print-scanned face images on the passport would be interesting.

In this paper, we present the novel approach to detect morphed face images by exploring the collaborative representation of the steerable features from the luminancecomponentof a face image. To this extent, the proposed method first extracts the luminance component of the given face image. The scale-space features are extracted by employing the Steerable pyramids with different scales and orientation, which is then classified using the Collaborative Representation Classifier (CRC) to make the final decision as either morph or bona-fide. Thus, following are the main contributions of this paper:

- Presents a new method for detecting the morphed face images based on the collaborative representation of the scale-space features from the luminance component of the given face image.
- Face morphing database available in [14] is further extended such that it has 2518 morphed images and 1273 bona fide images. All the images in the database are print-scanned to reflect the real-life passport issuance procedure. Thus, the final database is comprised of 3791 face images that have resulted in the largest morphed face database in the literature.
- Extensive experiments are carried out by comparing the proposed method with 7 different deep learning methods and 5 different hand-crafted feature based methods. The quantitative performance of the proposed method together with 12 different algorithms are presented using the ISO/IEC metrics for Morphing Attack Detetion (MAD).

The rest of the paper is organized as follows: Section 2 describes the proposed method, Section 3 presents the experimental results of the proposed method compared with both deep learning and non deep learning (or hand-crafted feature) methods on the newly extended face morphing database. Section 4 draws the conclusion and lists the key findings.

2 Proposed Method

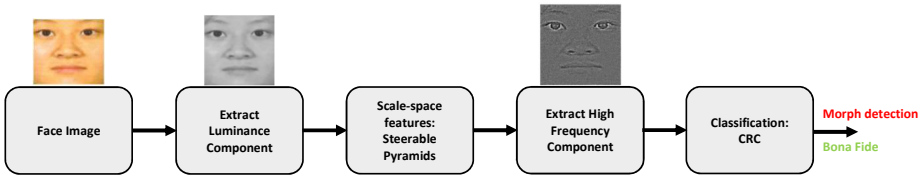

Fig. 1: Block Diagram of the Proposed Method

Figure 1 shows the block diagram of the proposed approach that can be structured into four functional blocks: (1) extract luminance component (2) extract scale-space features (3) extract high frequency components from scale-space

features (4) classification using Collaborative Representation Classifier (CRC). Given the face image, we first extract the face region using Viola-Jones face detector, which is further processed to correct the translation and rotation errors to get the normalised face image I_f of size $250 \times 250 \times 3$ pixels. We then compute the luminance component L_f corresponding to I_f as follows:

$$L_f = K_R.R + K_G.G + K_B.B \tag{1}$$

Where, K_R, K_G and K_B denotes three defined constants that are derived from the definition of corresponding RGB space as mentioned in [11].

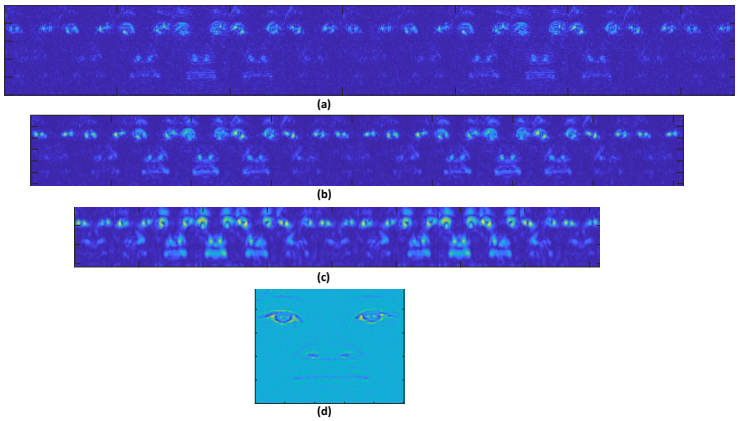

Fig. 2: Qualitative illustration of the scale-spcae features extracted using Steerable Pyramind (a) Level 1 (b) Level 2 (c) Level 3 (d) High pass residual band

In the next step, we obtain the scale-space features using Steerable pyramid [5], which are basically a set of oriented filters that are synthesized as a linear combination of the basis functions. In this work, we use the steerable pyramid based scale-space features by considering it's rotation and translation invariance property, which can effectively capture the texture information. Given the luminance component of the face image L_f, corresponding steerable pyramid representation $P_{m,n}(x, y)$ can be obtained as follows:

$$Pm, n(x, y) = \sum_x \sum_y L_f(x, y) D_{m,n}(x - x1, y - y1) \tag{2}$$

Where, $D_{m,n}$ denotes the directional bandpass filters at stage $m = 0, 1, 2, ..., S1$, and orientation $n = 0, 1, 2, ..., K1$.

Figure 2 illustrates features obtained from a steerable pyramid with three different levels. Each of which indicate the texture features extracted from eight different orientations. In the next step, high-pass residual band components are extracted and they can effectively represent the distortion in the image, which is

useful for detecting a morphed face image. Let the high-pass residual band corresponding to the luminance face image L_f be H_f. Figure 3 shows the qualitative results of the proposed method on both bona fide (see Figure 3 (a)) and morphed face image respectively. It can be observed from Figure 3 that the high-frequency residual features extracted using steerable pyramids from the luminance component of the image can show the visual differences between the bona-fide and morphed face images. This justifies the intuition of the proposed method to effectively capture the useful texture information to aid us in detecting the morphed face image.

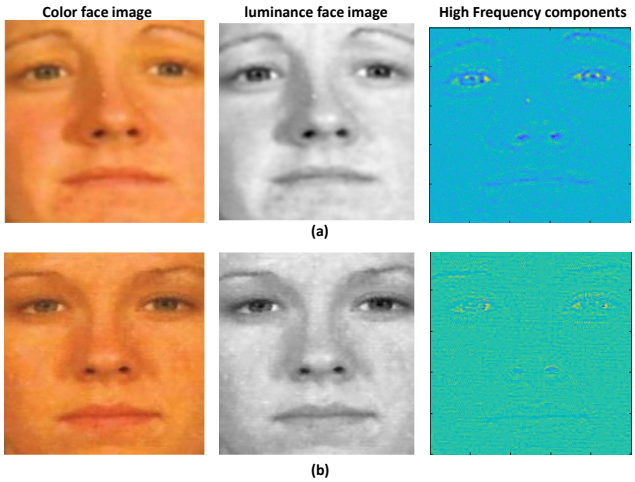

Fig. 3: Qualitative illustration of the Proposed Method (a) Bona fide face image (b) Morphed face image

To effectively classify the features at various scale-space, in this work we have employed the Collaborative Representation Classifier (CRC) [20]. The extracted features from the training set of the database are learned in a collaborative subspace ρ_λ and the final classification scores are obtained using regularised Least Square Regression coefficients on the learned spectral feature vectors against the test sample image, which is explained mathematically as follows:

$$D = argmin_\beta \left\| H_f - \rho_\lambda \beta \right\|_2^2 + \sigma \left\| \beta \right\|_2^2 \tag{3}$$

3 Experiments and results

Experiments presented in this work are carried out on the semi-public database available from [14]. In this work, we have extended this database by strictly following the protocol as described in [14]. To make sure that the quality of bona-fide and morphed face images is the same, so that classier is not biased, we

have evaluated the blind image quality measure BRISQUE [9]. Figure 4 shows the measured quality values of both bona-fide and morphed images, which are completely overlapping and thus indicating no bias in the image quality of bona-fide and morphed images. The extended database comprises of 693 bona-fide and 1202 morphed face images in the training set and 579 bona-fide and 1315 morphed images in the testing set. Thus, the complete database comprises of 3791 samples.

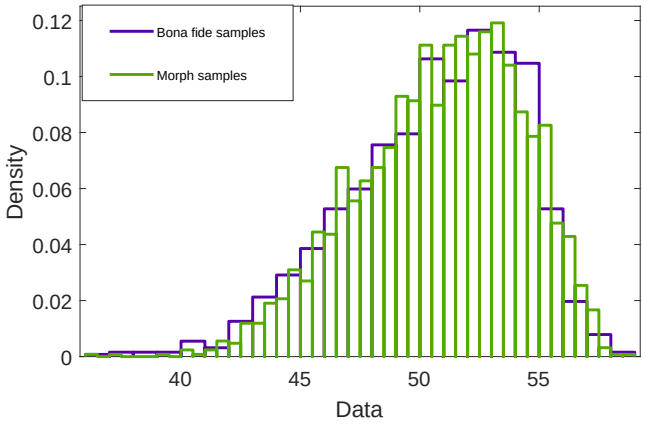

Fig. 4: BRISQUE quality distribution on bona-fide and morphed face images

Experiments are carried out by comparing the performance of the proposed method with 12 different state-of-the-art algorithms that include both deep learning and non deep-learning methods. The results are presented using the metrics: *Bonafide Presentation Classification Error Rate (BPCER) and Attack Presentation Classification Error Rate (APCER)* along with the corresponding DET curves (APCER versus BPCER) as described in IS0/IEC 30107-3 [7]. **BPCER** is defined as proportion of bona-fide presentations incorrectly classified as presentation attacks at the attack detection subsystem in a specific scenario while **APCER** is defined as proportion of attack face images incorrectly classified as bona-fide images at the attack detection subsystem in a specific scenario. Besides, we also report the performance of the system by reporting the value of BPCER by fixing the APCER to 5% and 10% corresponding to realistic operating values of face recognition systems.

Table 2 indicates the qualitative results of the proposed method together with 12 different state-of-the-art methods. The corresponding DET curves are shown in the Figure 5 for deep learning methods. For the simplicity, we have indicated the DET curves only for deep learning methods, however similar observations in DET curves can also be made for non deep learning methods. The deep learning methodology employed in this work is based on fine-tuning the pre-trained deep CNN architecture. While performing the fine-tuning, the data augmentation is

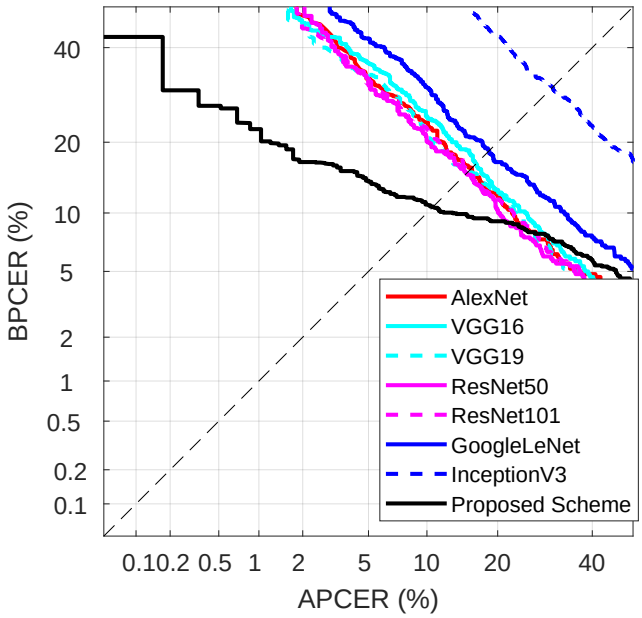

Fig. 5: DET curves indicating the performance of the proposed method with Deep learning methods

Table 2: Quantitative performance of the proposed method

Algorithm Type	Algorithm	BPCER (%) @	
		APCER = 5%	APCER = 10%
Deep Learning Methods	AlexNet	32.76	23.62
	VGG16	36.38	24.83
	VGG19	33.62	21.55
	ResNet50	32.24	20.17
	ResNet101	30.34	22.59
	GoogleLe Net	41.38	30.86
	IceptionV3	73.97	59.83
Non-Deep Learning Methods	LBP-SVM	89.63	75.14
	LPQ-SVM	94.64	82.13
	IG-SVM	68.08	56.47
	BSIF-SVM	96.2	86.87
	Color Textures	80.48	51.64
	Proposed Method	**45.76**	**13.12**

carried out to avoid the overfitting of the deep CNN networks. Based on the obtained results the following can be observed:

- Among the deep CNN architectures, the best performance is noted with the ResNet50 architecture with, $BPCER = 32.24\%@APCER = 5\%$ and $BPCER = 20.17\%@APCER = 10\%$.
- Among non deep learning methods, the state-of-the-art technique based on the color texture shows the best performance with, $BPCER = 80.48\%$ @ $APCER = 5\%$ and $BPCER = 51.64\%@APCER = 10\%$. However, the similar performance is also noted with other techniques such as: BSIF-SVM and LPQ-SVM.
- Deep learning technique shows the improved performance when compared to that of non-deep learning techniques.
- The performance of the proposed method shows the best performance with $BPCER = 45.76\%@APCER = 5\%$ and $BPCER = 13.12\%@APCER = 10\%$.

4 Conclusion

The use of face biometrics in passport document for border crossing is known to provide high accuracy while aiding the border guards to verify the identity visually. The recent works have demonstrated the vulnerability of passport systems where a morphed image can be submitted to avail a valid passport that can match with colluding identities. The challenge therefore is to detect such morphed images before they are used for passport issuance not only in the digital domain, but also the detecting morphed image after the image has been printed and scanned. In this work, we have presented a new approach to detect such morphed image attacks where the images are first morphed, printed and scanned. The approach has been validated with existing database of 693 bona-fide and 1202 morphed face images and with the newly extended database of 579 bona-fide and 1315 morphed images. The approach is based on extracting textural features across scale-space and classifying them using collaborative representation has been experimentally proven effective in detecting the morphing attacks. The proposed approach has provided results with D-EER of 10.71% and a APCER of 12.84% @ BPCER of 5% exemplifying the applicability in detecting the morphed image attacks after the print and scan process.

Acknowledgment

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

References

1. Asaad, A., Jassim, S.: Topological data analysis for image tampering detection. In: International Workshop on Digital Watermarking. pp. 136–146 (2017)

2. Ferrara, M., Franco, A., Maltoni, D.: The magic passport. In: IEEE International Joint Conference on Biometrics. pp. 1–7 (sep 2014)
3. Ferrara, M., Franco, A., Maltoni, D.: Face Recognition Across the Imaging Spectrum, chap. On the Effects of Image Alterations on Face Recognition Accuracy, pp. 195–222. Springer International Publishing (2016)
4. Ferrara, M., Franco, A., Maltoni, D.: Face demorphing. IEEE Transactions on Information Forensics and Security **13**(4), 1008–1017 (2018)
5. Freeman, W.T., Adelson, E.H., et al.: The design and use of steerable filters. IEEE Transactions on Pattern analysis and machine intelligence **13**(9), 891–906 (1991)
6. Hildebrandt, M., Neubert, T., Makrushin, A., Dittmann, J.: Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps. In: International Workshop on Biometrics and Forensics (IWBF 2017). pp. 1–6 (2017)
7. International Organization for Standardization: Information Technology – Biometric presentation attack detection – Part 3: Testing and reporting. ISO/IEC DIS 30107-3:2016, JTC 1/SC 37, Geneva, Switzerland (2016)
8. Makrushin, A., Neubert, T., Dittmann, J.: 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 - Volume 6: VISAPP, (VISIGRAPP 2017). pp. 39–50 (2017)
9. Mittal, A., Moorthy, A.K., Bovik, A.C.: No-reference image quality assessment in the spatial domain. IEEE Transactions on Image Processing **21**(12), 4695–4708 (2012)
10. Neubert, T.: Face morphing detection: An approach based on image degradation analysis. In: International Workshop on Digital Watermarking. pp. 93–106
11. Poynton, C.: Digital video and HD: Algorithms and Interfaces. Elsevier (2012)
12. Raghavendra, R., Raja, K.B., Busch, C.: Detecting Morphed Face Images. In: 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS). pp. 1–8 (2016)
13. Raghavendra, R., Raja, K.B., Venkatesh, S., Busch, C.: Transferable deep-cnn features for detecting digital and print-scanned morphed face images. In: Proc. IEEE Conf. Computer Vision Pattern Recognition Workshops (CVPRW). pp. 1822–1830 (2017)
14. Raghavendra, R., Raja, K., Venkatesh, S., Busch, C.: Face morphing versus face averaging: Vulnerability and detection. In: IEEE International Joint Conference on Biometrics (IJCB). pp. 555–563 (2017)
15. Robertson, D., Kramer, R.S., Burton, A.M.: Fraudulent id using face morphs: Experiments on human and automatic recognition. PLoS ONE **12**(3), 1–12 (2017)
16. Scherhag, U., Raghavendra, R., Raja, K., Gomez-Barrero, M., Rathgeb, C., Busch, C.: On the vulnerability of face recognition systems towards morphed face attack. In: International Workshop on Biometrics and Forensics (IWBF 2017). pp. 1–6 (2017)
17. Scherhag, U., Rathgeb, C., Busch, C.: 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)
18. Scherhag, U., Budhrani, D., Gomez-Barrero, M., Busch, C.: Detecting morphed face images using facial landmarks. In: Image and Signal Processing. pp. 444–452. Springer International Publishing (2018)
19. Seibold, C., Samek, W., Hilsmann, A., Eisert, P.: Detection of face morphing attacks by deep learning. In: International Workshop on Digital Watermarking. pp. 107–120 (2017)

20. Zhang, L., Yang, M., Feng, X.: Sparse representation or collaborative representation: Which helps face recognition? In: IEEE International Conference on Computer Vision (ICCV). pp. 471–478 (2011)