Residual Colour Scale-Space Gradients for Reference-based Face Morphing Attack Detection

Raghavendra Ramachandra[1] Guoqiang Li[2]
[1]Norwegian University of Science and Technology (NTNU), Norway
[2]MOBAI AS, Norway

***Abstract*—Face biometrics has become an integral part of the various security and law enforcement applications, including border control scenarios. However, the face recognition systems are vulnerable to the morphing attacks, and thus, it is essential to develop a reliable and robust face Morphing Attack Detection (MAD) techniques. This paper presents a novel approach based on the residual gradients computed from the face image's colour scale-space representation in the reference-based or differential set-up. Thus, the proposed method will take two facial images (one from the passport and another from the trusted device) to compute the residual gradients, which is then classified using Spectral Regression Kernel Discriminant Analysis (SRKDA) to reliable detect the face morphing attacks. Extensive experiments are carried out on two different datasets to benchmark the performance of the proposed method, especially to different morph generation methods, morphing data mediums (digital, print-scan and print-scan compression) and ageing variations. Experimental results demonstrate the improved performance of the proposed method over the state-of-the-art reference-based face MAD in all evaluation protocols.**

I. Introduction

Direct attacks on Face Recognition Systems (FRS) has raised security concerns as these systems are increasingly deployed in law enforcement applications. Among the several types of attacks on FRS, the face morphing attacks have created a severe security problem because of their vulnerability to border control applications. The face morphing process will accept more than one facial image and perform the operation of wrapping and blending to generate the morphing image seamlessly. The generated face morphing image can get verified to all the contributory data subjects when it is enroled to the commercial-off-the-shelves FRS [1]. The extensive vulnerability study reported in NIST FRVT MORPH [2] indicates that the higher the accuracy of the FRS, the higher is the vulnerability. Therefore, it is essential to reliably detect face morphing attacks to achieve trustworthy face recognition in the law enforcement applications.

Face Morphing Attack Detection (MAD) is widely addressed in the biometric community, resulting in a vast number of MAD techniques. The State-Of-The-Art (SOTA) MAD methods can be widely divided into two types [1]: (a) no-reference (or single image) based MAD where the morphing is detected based on the single image. The MAD algorithms that fall under this category are termed S-MAD. (b) reference (or differential) based MAD where the morphing is detected by comparing two facial images (one from a trusted device and another from a passport). The MAD algorithms that fall under this category are termed as D-MAD. Among these two approaches, the D-MAD techniques were reported to show a good detection accuracy [2] as they exhibit more information extracted from two facial images. Figure 1 illustrates the reference-based morph attack detection framework.

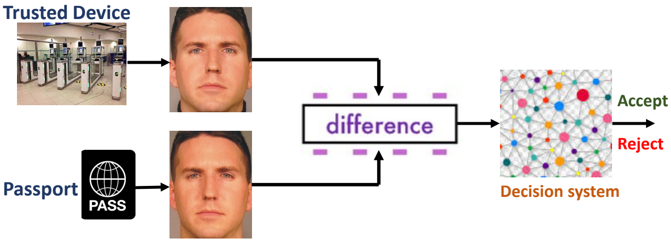


Fig. 1: Illustrating the reference-based (or differential) MAD framework

Existing D-MAD techniques are classified as two main types [1]: (1) Feature difference (2) De-morphing. The idea of the feature difference method is to subtract the features (texture, quality, etc.) that are independently computed on the facial image captured from both trusted device and passport. The difference feature is then processed using machine learning techniques to decide on the facial image from the passport as bona fide/morph. The feature extraction includes texture features [3], [4], landmarks difference [5], [6], 3D information [7] and deep features [3] [8], Siamese Networks [9] and Double Siamese Networks [10]. The facial de-morphing techniques can be categorised into (a) Landmark based [11], (b) Deep learning-based [12], [13], [8]. The landmark-based demorphing approaches will inverse the morphing operation to regenerate the hidden face image. However, these techniques require a highly constrained data capture environment and need prior parameters used for morphing. The deep learning-based face de-morphing approaches are based on the Generative Adversarial Network (GAN) [13] and Auto-Encoders [8] are also proposed. Table I summarises the SOTA on D-MAD techniques.

Even though several D-MAD techniques are presented, the detection performance of these techniques is limited to the quality of the face images used. The quality of both bona fide and morphed images are influenced by various factors

TABLE I: State-of-the-art reference based MAD techniques

Reference	Detection Type	Approach	Algorithm	Database
M Ferrara et al. [11]	D-MAD	Demorphing	Demorphing by image subtraction	Print-scan
M Ferrara et al. [11]	D-MAD	Demorphing approach	Face verification	Digital
U Scherhag et al. [5]	D-MAD	Landmark-based approach	Distance-based and angle-based feature extraction with Random Forest, SVM without kernel and SVM with radial basis function classifier	Digital
U Scherhag et al. [14]	S-MAD + D-MAD	Feature difference-based approach	Pre-processing and feature extraction using texture descriptors, keypoint extractors, gradient estimators and deep learning-based method	Digital
N Damer et al. [4]	D-MAD	Multi-detector fusion	LBPH, Transferable deep-CNN	Digital
J M Singh [7]	D-MAD	Deep learning	SfS Net, AlexNet	Digital + Print-scan
N Damer et al. [6]	D-MAD	Landmark shift	Landmark detection, shift representation	Digital
F Peng et al. [13]	D-MAD	Face restoration by demorphing GAN	Symmetric dual-network architecture	Digital
U Scherhag et al. [3]	D-MAD	Deep Face Representation	ArcFace Network, FaceNet algorithm	Digital + Print-scan
C Seibold et al. [15]	D-MAD	Deep Learning	Layer-wise Relevance Propagation (LRP)	Digital
D Ortego et al. [12]	D-MAD	Demorphing, Deep CNN-based	Auto-encoders	Digital + Print-scan
S Soleymani et al. [16]	D-MAD	Deep learning	Siamese network	Digital
S Soleymani et al. [17]	D-MAD	Deep learning	Appearance and landmark disentanglement	Digital
S Autherith et al. [18]	D-MAD	Analysis of geometric facial features	Facial anthropometry-based facial feature comparison	Digital
Sudipta et al. [19]	D-MAD	Implicitly disentangle identities	Information theoretic framework using Conditional GAN	Digital
Guido et al. [10]	D-MAD	Double Siamese network	Two Siamese network representing different types of face detection	Digital

such as (a) data medium (e.g. digital, print-scan and print-scan compression) (b) morphing generation type (landmark-based or GAN based) (c) influence of ageing. We proposed a new framework based on the residual colour scale-space gradients features to detect the face morphing attack in this work. The proposed method is designed to extract the residuals from the gradient features computed on six different colour channels that are independently represented using three-level scale-space features using a Laplacian pyramid. Finally, the gradient residuals are compared independently using SRKDA classifier to obtain the comparison scores that are fused using the sum rule to make the final decision. Following are the main contributions of this work:

- We presented a novel framework for the reference-based morph attack detection by introducing the residuals of colour scale-space gradients.
- Extensive experiments are carried out to benchmark the performance of the proposed method with existing methods. Evaluation protocols are designed to benchmark the performance of the proposed method to data mediums, morphing generation tools and age variation.
- Extensive experiments are presented with both cross-morph generation and different data medium to quantify the robustness of the proposed method to the unseen attack data.

The rest of the paper is organised as follows: Section II presents the proposed method, Section III presents the experimental results and Section IV draws the conclusion.

II. Proposed Approach

In this section, we discuss the proposed method for the D-MAD. Figure 2 shows the block diagram of the proposed reference-based morph attack detection using residuals of gradients computed from colour scale-space representation. We assert that the residuals gradients computed from the colour scale-space representation can extract the discriminant features that can reveal variations (due to morphing noise, change in geometry, etc.) due to the morphing process. The proposed method consists of six different functional blocks that includes (1) colour space representation, (2) scale-space representation, (3) gradient feature extraction, (4) computing difference, (5) computing comparison scores and (6) fusion.

In the following, we discuss each of these functional blocks in detail.

Given the facial image I (e.g. from the passport), the colour space representation is computed using both HSV and YC_bC_r as they can provide complementary information. This will result in six different color-space images $Ic = \{Ic_1, Ic_2, \ldots, Ic_6\}$. In the next step, we take each color-space images and compute the scale-space representation using a Laplacian pyramid [20] with three level decomposition resulting in three sub-images. In this work, we have selected the Laplacian pyramid over similar approaches by considering their effectiveness in the application of face morphing attack detection [1]. Thus, the scale-space representation will result in a total of 6 color channels $\times$ 3 level decomposition = 18 sub-images. We then extract the gradient features using Histogram of Gradients (HoG) on each sub-images. In this work, we select the HoG descriptors by considering the advantages of their in-variance to geometric and photometric transformations. Hence when computed, the residual between two facial images will result in the discriminant information useful to detect morphing attacks. Let the gradient features corresponding to the facial image I be $G_I = \{G_{I1}, G_{I2}, \ldots, G_{I18}\}$.

The above mentioned steps are repeated on the second facial image J captured using a trusted device. Let the color scale-space gradient features extracted be $G_J = \{G_{IJ}, G_{J2}, \ldots, G_{J18}\}$. We then compute the residual gradients using difference operation $D_x = \{G_{Ix} - G_{Jx}\}$, where $\forall_x = \{1, 2, \ldots, 18\}$. The difference features D_x are used to compute the morphing scores using SRKDA classifiers independently. This will results in 18 different morphing scores that are combined using the sum rule to obtained a single morphing score that is compared with the pre-set threshold to make the final decision on morphing/bona fide.

III. Experiments and Results

This section presents the quantitative performance of the proposed method and the SOTA D-MAD techniques on the two different datasets. The performance of the proposed method is compared with the existing method based on Deep features [3]. We exceptionally choose the deep features by considering its robustness to morphing sources and the medium as reported in [3]. Further, the Deep features [3] method also indicates the best performance on the NIST FRVT MORPH [21] benchmark. To maintain fairness in comparison, we followed the same evaluation protocols by using the same data for training and testing on both the proposed method and the SOTA (Deep features [3]). The quantitative performance of the D-MAD techniques is quantified using the ISO/IEC metrics [22] namely the ´´Attack Presentation Classification Error Rate (APCER (%)) which defines the proportion of attack images (morph images) incorrectly classified as bona fide images and the Bona fide Presentation Classification Error Rate (BPCER (%)) in which bona fide images incorrectly classified as attack images are counted [22] along with the Detection Equal Error Rate (D-EER (%))´´ [23]. In the following, we first briefly discuss the characteristics of the two different datasets followed by the quantitative results.

A. Morphing dataset and evaluation protocol

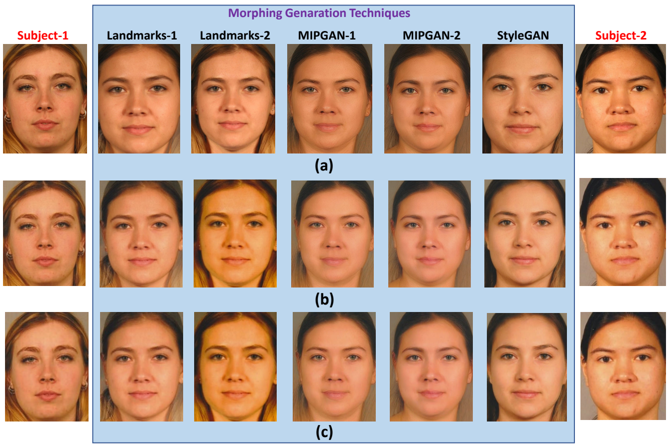


Fig. 3: Illustration of the example images from Database-I

In this work, we have employed two different datasets to benchmark the performance of the proposed method with various sources of morphing noises.

Database-I: This database was first introduced in [23] and consist of morph images generated using five different morph generation techniques. The morph generation techniques employed in Database-I has both landmarks and deep learning-based. landmark-based morph face generation are of two different types: Landmark-I: the morph generation

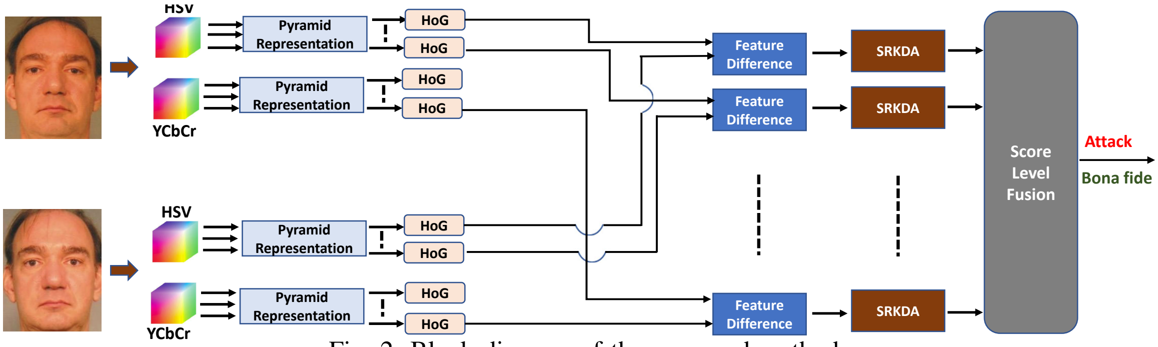


Fig. 2: Block diagram of the proposed method

TABLE II: Quantitative performance of MAD - Training- Landmarks-I [24]

Morph Generation Type: Training	Morph Generation Type: Testing	MAD Algorithms	Digital			Print-scan			Print-scan with compression		
			D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =	
				5%	10%		5%	10%		5%	10%
Landmarks-I [24]	Landmarks-I [24]	Deep features [3]	12.97	52.45	24.55	22.78	80.15	60.11	21.41	78.19	52.16
		Proposed Method	**0.98**	**0.78**	**0.19**	**10.41**	**22**	**10.80**	**11.42**	**23.96**	**14.14**
	Landmarks-II [25]	Deep features [3]	41.30	99.21	96.66	35.56	96.17	89.19	35.94	95.87	87.62
		Proposed Method	**39.40**	**90.56**	**86.76**	**45.93**	**95.28**	**87.62**	**44.14**	**93.90**	**88.80**
	MIPGAN-I [23]	Deep features [3]	36.49	88.80	79.17	28.14	84.47	67.19	18.89	74.65	44.79
		Proposed Method	**41.65**	**90.76**	**83.69**	**32.21**	**75.44**	**64.14**	**30.66**	**71.70**	**58.54**
	MIPGAN-II [23]	Deep features [3]	38.29	94.69	85.26	38.50	96.46	88.40	26.55	87.42	70.92
		Proposed Method	**43.21**	**87.62**	**79.37**	**19.14**	**45.57**	**31.82**	**18.25**	**1.84**	**27.89**
	StyleGAN [26]	Deep features [3]	15.13	44.59	27.30	23.72	70.53	52.25	20.63	76.13	54.51
		Proposed Method	**1.19**	**0**	**0**	**21.03**	**54.22**	**40.47**	**23.18**	**59.13**	**44.79**

TABLE III: Quantitative performance of MAD - Training- Landmarks-II [25]

Morph Generation Type: Training	Morph Generation Type: Testing	MAD Algorithms	Digital			Print-scan			Print-scan with compression		
			D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =	
				5%	10%		5%	10%		5%	10%
Landmarks-II [25]	Landmarks-I [24]	Deep features [3]	19.30	71.11	49.31	24.76	80.55	57.76	20.87	74.65	50.29
		Proposed Method	**36.53**	**78.38**	**68.76**	**23.11**	**59.72**	**46.56**	**11.42**	**23.96**	**14.14**
	Landmarks-II [25]	Deep features [3]	26.13	84.67	66.20	25.52	86.15	67.58	23.16	82.12	62.47
		Proposed Methods	**17.18**	**37.91**	**25.93**	**21.82**	**56.97**	**42.23**	**44.16**	**93.90**	**88.80**
	MIPGAN-I [23]	Deep features [3]	37.71	85.16	72.12	39.39	93.90	85.65	29.85	89.98	81.53
		Proposed Method	**31.40**	**72.88**	**58.74**	**44.99**	**91.15**	**84.28**	**30.66**	**71.70**	**58.54**
	MIPGAN-II [23]	Deep features [3]	43.21	93.90	89.39	43.14	98.15	92.53	28.50	89.19	79.17
		Proposed Method	**29.64**	**78.58**	**64.24**	**36.96**	**83.30**	**71.90**	**18.25**	**41.84**	**27.89**
	StyleGAN [26]	Deep features [3]	29.14	76.81	60.15	20.15	66.14	46.56	21.21	75.63	50.68
		Proposed Method	**32.80**	**72.88**	**61.29**	**31.14**	**76.14**	**65.61**	**23.18**	**59.13**	**44.79**

TABLE IV: Quantitative performance of MAD - Training- MIPGAN-I [23]

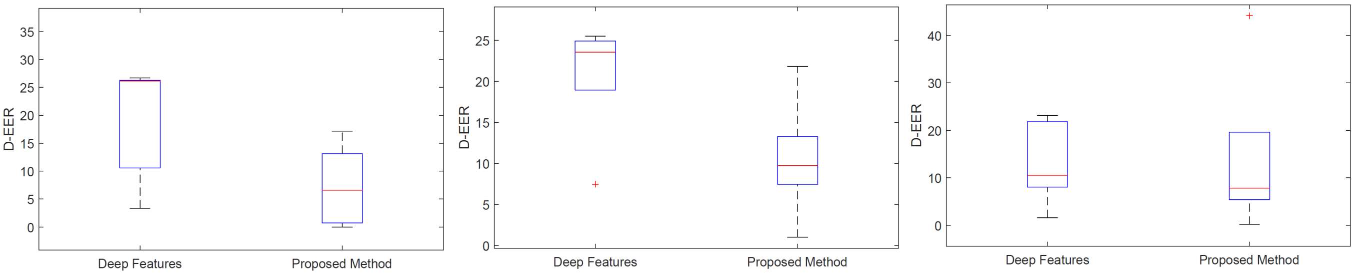
Morph Generation Type: Training	Morph Generation Type: Testing	MAD Algorithms	Digital			Print-scan			Print-scan with compression		
			D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =	
				5%	10%		5%	10%		5%	10%
MIPGAN-I [23]	Landmarks-I [24]	Deep features [3]	33.74	94.49	88.15	33.61	96.26	85.85	26.91	84.28	67.97
		Proposed Method	**23.91**	**62.67**	**41.45**	**20.58**	**51.66**	**35.75**	**21.14**	**47.54**	**34.57**
	Landmarks-II [25]	Deep features [3]	43.37	98.23	94.69	42.64	99.14	96.26	47.34	96.66	87.22
		Proposed Method	**40.80**	**87.81**	**79.37**	**41.95**	**96.17**	**86.24**	**46.37**	**94.13**	**86.55**
	MIPGAN-I [23]	Deep features [3]	26.13	75.14	57.17	24.76	74.85	61.49	10.21	23.34	10.21
		Proposed Method	**11.81**	**23.57**	**13.35**	**9.74**	**17.45**	**9.45**	**7.16**	**9.23**	**4.51**
	MIPGAN-II [23]	Deep features [3]	27.11	80.15	62.86	26.96	82.12	62.27	18.64	68.56	41.25
		Proposed Method	**12.33**	**24.55**	**13.94**	**13.20**	**22.39**	**15.71**	**9.82**	**17.58**	**9.82**
	StyleGAN [26]	Deep features [3]	44.39	95.87	90.56	33.77	89.98	80.15	17.24	57.76	33.79
		Proposed Method	**16.72**	**36.34**	**24.36**	**24.36**	**60.11**	**45.57**	**24.94**	**62.18**	**51.18**

TABLE V: Quantitative performance of MAD - Training- MIPGAN-II [23]

Morph Generation Type: Training	Morph Generation Type: Testing	MAD Algorithms	Digital			Print-scan			Print-scan with compression		
			D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =	
				5%	10%		5%	10%		5%	10%
MIPGAN-II [23]	Landmarks-I [24]	Deep features [3]	33.14	95.18	87.81	31.28	92.73	79.96	30.45	91.55	78.97
		Proposed Method	**27.14**	**64.14**	**50.49**	**18.66**	**47.74**	**35.36**	**21.23**	**50.68**	**35.75**
	Landmarks-II [25]	Deep features [3]	42.13	99.15	97.64	38.55	97.44	92.73	36.91	97.64	91.15
		Proposed Method	**39.29**	**87.42**	**77.21**	**43.98**	**96.85**	**91.94**	**44.62**	**96.66**	**87.22**
	MIPGAN-I [23]	Deep features [3]	30.14	82.52	67.97	28.14	79.17	62.67	18.27	61.49	36.54
		Proposed Method	**11.59**	**22.00**	**13.55**	**22.98**	**47.74**	**36.14**	**20.13**	**39.29**	**29.46**
	MIPGAN-II [23]	Deep features [3]	26.73	88.60	72.69	23.56	74.45	55.59	10.61	24.36	11.19
		Proposed Method	**6.67**	⁀extbf8.25	**4.32**	**9.63**	**16.89**	**9.43**	**7.85**	**12.18**	**6.19**
	StyleGAN [26]	Deep features [3]	34.58	92.14	83.12	30.19	85.46	69.74	22.58	79.17	55.59
		Proposed Method	**22.83**	**46.56**	**36.14**	**28.68**	**69.54**	**56.97**	**27.52**	**66.42**	**51.86**

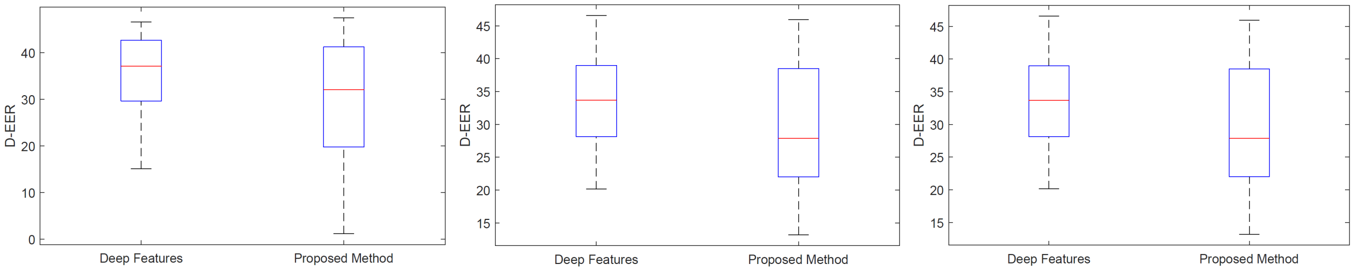
TABLE VI: Quantitative performance of MAD - Training- StyleGAN [26]

Morph Generation Type: Training	Morph Generation Type: Testing	MAD Algorithms	Digital			Print-scan			Print-scan with compression		
			D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =		D-EER(%)	BPCER @ APCER =	
				5%	10%		5%	10%		5%	10%
StyleGAN [26]	Landmarks-I [24]	Deep features [3]	18.31	57.17	35.95	33.18	87.81	77.99	31.65	89.78	77.01
		Proposed Method	**2.36**	**0.58**	**0.19**	**26.96**	**62.86**	**50.68**	**24.16**	**60.70**	**45.38**
	Landmarks-II [25]	Deep features [3]	38.18	96.46	88.80	35.91	92.92	83.30	36.14	92.33	81.72
		Proposed Method	**47.42**	**94.89**	**90.39**	**39.67**	**87.81**	**76.42**	**34.66**	**86.44**	**76.22**
	MIPGAN-I [23]	Deep features [3]	46.55	96.26	92.14	40.64	96.46	88.60	24.30	78.97	61.88
		Proposed Method	**45.95**	**90.17**	**83.14**	**37.30**	**81.53**	**70.72**	**32.98**	**75.24**	**63.17**
	MIPGAN-II [23]	Deep features [3]	44.79	96.66	89.19	46.55	97.24	91.74	27.50	87.62	71.70
		Proposed Method	**44.76**	**90.96**	**85.16**	**27.11**	**67.78**	**53.24**	**23.37**	**60.11**	**47.54**
	StyleGAN [26]	Deep features [3]	3.36	1.96	0.39	7.43	14.73	5.89	3.32	1.57	0.19
		Proposed Method	**0**	**0**	**0**	**1**	**0.19**	**0.19**	**1.37**	**0.19**	**0.19**



(a) Data type: Digital (b) Data type: Print-Scan (c) Data type: Print-Scan Compression

Fig. 4: Box plot summarising the detection performance of the proposed method when trained and tested with same morphing generation technique (Intra evaluation protocol).



(a) Data type: Digital (b) Data type: Print-Scan (c) Data type: Print-Scan Compression

Fig. 5: Box plot summarising the detection performance of the proposed method when trained and tested with different morphing generation technique (Inter evaluation protocol.)

is carried out using a publicly available tool from Open CV [27]. Landmark-II: The morph generation is carried out using the UBO morphing tool [25]. Database-I has three different deep learning-based morph generation techniques include MIPGAN-I, MIPGAN-II and StyleGAN [23]. This database has both bona fide and morphs images generated using three different data mediums such as: digital, print-scan and print-scan with compression. The print images are generated using a DNP printer which is a sublimation printer that can deliver professional-quality photo prints that are challenging to detect. Database-I consists of 2500 $\times$ 3 (types of morph data) $\times$ 4 types of morph generation technique = $30,000$ morph samples and 1270 $\times$ 3 (types of morph data) $\times$ 4 types of morph generation technique = $15,240$ bona fide samples [23]. Figure 3 shows the example images from the DB-I for the digital medium. In this work, we have used the evaluation protocol proposed for this database [23] that includes both Intra (same source of morph generation is used for training and testing) and Inter (different morph generation source is used for training and testing). The inter protocol is designed to evaluate the performance of the MAD techniques for the unseen morph generation techniques to evaluate the generalisability.

Database-II: Database-II used in this work was first introduced in [28] and constructed using MORPH II non-commercial dataset [29]. The main characteristic of this dataset is the variation in age and has two different age bins, including MorphAge-I: This dataset consists of 1002 unique data subjects with an age variation of 1-2 years. This dataset has 10538 face images. (2) MorphAge-2: This dataset consists of 516 unique data subjects with an age variation of 2 to 5 years. This dataset has in total of 3767 face images. Both of these

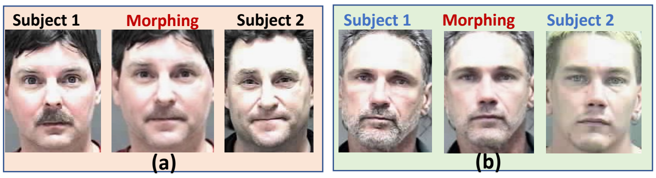


Fig. 6: Illustration of the example images from Database-II (a) MorphAge-I (b)MorphAge-2

datasets have used UBO face Morpher [25] to generate the morphed face images with an alpha factor of 0.5. . This dataset has only digital medium data. Figure 6 illustrates the example face image from MorphAge-I and MorphAge-II datasets. We have followed the evaluation protocol as described in [28].

B. Results

Table II, III, IV, V and VI indicates the quantitative performance of the proposed method with the state-of-the-art techniques. Figure 5 and 4 shows the box plots of the D-EER (%) corresponding to the proposed method and the deep features [3] on three different data mediums. Based on the obtained results, the following are the main observations:

- Figure 4 shows the box plot of the D-MAD techniques on the intra evaluation protocol. In general, the detection error rate is less for the proposed method irrespective of the morph generation type and the data medium. Thus, the proposed method illustrates the best performance when compared to the best performing SOTA.
- Among three different data medium, the proposed method shows the best performance on the digital data. However, the SOTA shows the best performance on the print-scan with compression data medium.
- The detection performance of the proposed method and the SOTA varies across different morph generation methods. The best performance of the proposed method is noted with the StyleGAN and Landmarks-I based morph generation techniques with D-EER = 0% and 0.98% respectively. The degraded performance of the proposed method is noted with the Landmark-II with D-EER = 17.18%.
- it is interesting to note that, both quality of the data medium and morphing generation type will influence the detection performance of both proposed and SOTA algorithms. However, the proposed method consistently indicated the best performance compared to SOTA.
- Figure 5 shows the box plot of the D-MAD techniques on the inter evaluation protocol. In general, the performance of both the proposed method and SOTA is degraded when compared the performance in the intra evaluation protocol.
- In general, the detection performance of both the proposed method and SOTA is superior on the print-scan with compression data medium.
- When trained with landmark-based morph generation data, both the proposed method and SOTA will indicate the degraded detection accuracy when trained on landmark-based morphing data and tested on the deep learning-based morph data (except for the StyleGAN based morphing data). A similar observation in degraded detection performance is noted when the proposed and SOTA methods are trained using deep learning-based morphing data and testing using landmark-based morphing data.
- Based on the results from the inter evaluation protocol, the proposed method has emerged as the best performing D-MAD technique on the Database-I.

TABLE VII: Quantitative performance of the proposed method on ageing database

Database types	Algorithms	Detection Performance		
		D-EER (%)	BPCER@APCER =	
			5%	10%
Age Group - I	Deep features [3]	35.36	89.64	80.17
	Proposed Method	18.34	53.78	34.26
Age Group - II	Deep features [3]	40.34	96.13	86.82
	Proposed Method	17.73	45.13	34.51
Age Group-I Versus Age Group-II	Deep features [3]	42.52	92.24	85.27
	Proposed Method	19.45	46.13	47.14
Age Group-II Versus Age Group-I	Deep features [3]	35.43	86.15	76.19
	Proposed Method	25.91	56.97	47.14

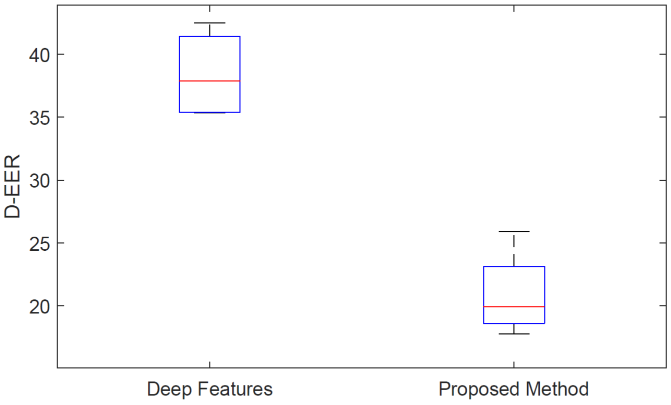


Fig. 7: Box plot showing D-EER (%) on the Database-II

Table VII indicates the quantitative results of the proposed method and the SOTA on the database-II. We have carried out four different experiments that includes training and testing on the same Age Group and the cross Age group. Based on the obtained results, following are the main observations:

- When trained and tested on the same Age group dataset, the performance of the proposed method indicated a lower error rate than the existing methods. The performance of the deep feature [3] method deteriorates, especially on the Age group-II where the age difference is up to 5 years. The deep features-based D-MAD technique is built on the Arcface features, and we assert that robustness to an age difference is limited. This fact is further justified as the deep features D-MAD technique show the D-EER = 35.56% on AgeGroup-I with 1-2 year variation while D-EER = 40.34% on Agegroup-II. However, the performance of the proposed method is independent of the age variation as the performance variation between AgeGroup-I and II is relatively negligible.

- With cross AgeGroup experiments in which one AgeGroup is used for training and another group for testing, the performance of both the proposed method and the existing D-MAD techniques indicates the degraded performance. The proposed method suggests the best performance in this experiment compared to the existing methods.
- Figure 7 shows the box plot of the D-EER corresponding to both the proposed method and the deep feature method on all four experiments. As noticed from the Figure 7, the proposed method has indicated the best performance over existing methods on the Database-II and thereby demonstrating the efficacy in detecting the face morphing attacks.

IV. Conclusion

The reliable face morphing detection is a challenging problem due to the significant variation in the morphing process that will result in various face image qualities that will limit the generalisability of the MAD. This work proposes a novel reference-based morphing attack detection method based on the residuals of colour scale-space gradients computed on the two facial images. The proposed method employs two different colour spaces such as HSV and YC_bC_r. In the next step, each colour channel image is represented in the scale-space domain using a Laplacian pyramid with a three-level decomposition that will result in a total of × 3 level decomposition = 18 sub-images. We then compute the gradient features corresponding to each sub-image using Histogram of Gradients (HoG). The colour scale-space gradients are extracted on both facial images under consideration and then we compute the residual by taking the difference. This process is followed on all 18 sub-images independently. Finally, the residual features from sub-images are used separately to compute the comparison scores that are combined using the sum rule to make the final decision. Extensive experiments are carried out on the two different datasets to benchmark the detection performance of the proposed method compared with the existing method based on the deep features. Obtained results demonstrate the improved detection performance over existing methods.

Acknowledgment

The project leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 883356.

References

[1] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Face morphing attack generation detection: A comprehensive survey," *IEEE Transactions on Technology and Society*, pp. 1–23, 2021.

[2] N. Mei, P. Grother, K. Hanaoka, and J. Kuo, "Face Recognition Vendor Test (FRVT) Part 4: Performance of Automated Face Morph Detection," National Institute of Standards and Technology, Tech. Rep., July 2021.

[3] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, "Deep face representations for differential morphing attack detection," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3625–3639, 2020.

[4] N. Damer, S. Zienert, Y. Wainakh, A. M. Saladié, F. Kirchbuchner, and A. Kuijper, "A multi-detector solution towards an accurate and generalized detection of face morphing attacks," in *22th International Conference on Information Fusion (FUSION)*, 2019, pp. 1–8.

[5] U. Scherhag, D. Budhrani, M. Gomez-Barrero, and C. Busch, "Detecting morphed face images using facial landmarks," in *Image and Signal Processing*. Springer International Publishing, 2018, pp. 444–452.

[6] N. Damer, V. Boller, Y. Wainakh, F. Boutros, P. Terhörst, A. Braun, and A. Kuijper, "Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts," in *Pattern Recognition*, T. Brox, A. Bruhn, and M. Fritz, Eds. Cham: Springer International Publishing, 2019, pp. 518–534.

[7] J. M. Singh, R. Raghavendra, K. B. Raja, and C. Busch, "Robust morph-detection at automated border control gate using deep decomposed 3d shape diffuse reflectance," in *2019 15th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)*, 2019, pp. 106–112.

[8] B. Chaudhary, P. Aghdaie, S. Soleymani, J. Dawson, and N. M. Nasrabadi, "Differential morph face detection using discriminative wavelet sub-bands," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, June 2021, pp. 1425–1434.

[9] S. Soleymani, B. Chaudhary, A. Dabouei, J. Dawson, and N. M. Nasrabadi, "Differential morphed face detection using deep siamese networks," 2020.

[10] G. Borghi, E. Pancisi, M. Ferrara, and D. Maltoni, "A double siamese framework for differential morphing attack detection," *Sensors*, vol. 21, no. 10, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/10/3466

[11] M. Ferrara, A. Franco, and D. Maltoni, "Face demorphing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1008–1017, 2018.

[12] D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso, and E. Cabello, "Border control morphing attack detection with a convolutional neural network de-morphing approach," *IEEE Access*, 2020.

[13] F. Peng, L.-B. Zhang, and M. Long, "FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image," *IEEE Access*, vol. 7, pp. 75 122–75 131, 2019. [Online]. Available: https://doi.org/10.1109%2Faccess.2019.2920713

[14] 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)*, 2018, pp. 187–192.

[15] "Accurate and robust neural networks for face morphing attack detection," *Journal of Information Security and Applications*, vol. 53, p. 102526, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212619302029

[16] S. Soleymani, B. Chaudhary, A. Dabouei, J. Dawson, and N. M. Nasrabadi, "Differential morphed face detection using deep siamese networks," *arXiv preprint arXiv:2012.01541*, 2020.

[17] S. Soleymani, A. Dabouei, F. Taherkhani, J. Dawson, and N. M. Nasrabadi, "Mutual information maximization on disentangled representations for differential morph detection," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2021, pp. 1731–1741.

[18] S. Autherith and C. Pasquini, "Detecting morphing attacks through face geometry features," *Journal of Imaging*, vol. 6, p. 115, 2020.

[19] S. Banerjee and A. Ross, "Conditional identity disentanglement for differential face morph detection," in *2021 IEEE International Joint Conference on Biometrics (IJCB)*, 2021, pp. 1–8.

[20] P. J. Burt and E. H. Adelson, "The laplacian pyramid as a compact image code," *Communications, IEEE Transactions on*, vol. 31, no. 4, pp. 532–540, 1983.

[21] M. Ngan, P. Grother, K. Hanaoka, and J. Kuo, "Face recognition vendor test (frvt) part 4: Morph-performance of automated face morph detection," *National Institute of Technology (NIST), Tech. Rep. NISTIR*, vol. 8292, 2021.

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

[23] H. Zhang, S. Venkatesh, R. Ramachandra, K. Raja, N. Damer, and C. Busch, "MIPGAN–generating robust and high quality morph attacks using identity prior driven GAN," *IEEE Transactions on Biometrics, Behavior, and Identity Science (TBIOM)*, vol. 2, 2021.

[24] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch, "Face morphing versus face averaging: Vulnerability and detection," in *IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 555–563.

[25] 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)*. IEEE, 2019, pp. 1–5.

[26] S. Venkatesh, H. Zhang, R. Raghavendra, K. Raja, N. Damer, and C. Busch, "Can gan generated morphs threaten face recognition systems equally as landmark based morphs? - vulnerability and detection," in *2020 International Workshop on Biometrics and Forensics (IWBF)*. IEEE, 2020, pp. 1–6.

[27] "Face morph using opencv," 2017, accessed: 2017-04-10.

[28] S. Venkatesh, K. Raja, R. Raghavendra, and C. Busch, "On the influence of ageing on face morph attacks: Vulnerability and detection," in *International Joint Conference on Biometrics (IJCB)*, September 2020, pp. 1–8.

[29] G. Bingham, K. Kempfert, B. Yip, J. Fabish, M. Ferguson, C. Nansalo, K. Park, R. Towner, T. Kling, Y. Wang *et al.*, "Preliminary studies on a large face database morph-ii."