Robust Face Morphing Attack Detection Using Fusion of Multiple Features and Classification Techniques

Jag Mohan Singh[1] Sushma Venkatesh[2] Raghavendra Ramachandra [1]
[1] [1]Norwegian University of Science and Technology (NTNU), Norway. [2]AiBA AS, Norway.
email:jag.m.singh@ntnu.no; sushma@aiba.ai;raghavendra.ramachandra@ntnu.no

***Abstract*—The face morphing process will combine two or more facial images to generate a single morphed facial image demonstrating Face Recognition Systems (FRS) vulnerability. The attack potential of the morphing image directly depends on the perceptual image quality, and when generated with no visible artefacts, it can deceive both human observers and automatic FRS. The current softwares for face morphing generates a morphing image with ghosting artefacts, especially in the eye region, nose and mouth area, which may serve as a potential cue to detect morphing attacks. Hence in this work, we introduce a new dataset comprising 10710 facial images before and after manual post-processing to reduce the visual artefacts and to generate high-quality attacks. Further, we propose a novel single image-based Morph Attack Detection (S-MAD) technique based on the ensemble of features and classifiers using the scale-space domain. The novel concept in the proposed method is the multi-level fusion that combines the comparison scores from different features and classifiers. Extensive experiments are carried out on the newly generated high-quality face images with (i) Morphs before post-processing and (ii) Morphs after post-processing. Further, the experiments are also carried out on two different mediums such as (i) Digital and (ii) Print-scan (or re-digitized) with and without compression. Extensive experimental results are performed to benchmark the detection performance with the existing S-MAD techniques. Obtained results indicate the best performance of the proposed method over existing methods.**

***Index Terms*—Biometrics, Morphing, Morph attack, Attack detection, Morphing attack**

I. Introduction

Biometrics has been widely studied and applied globally for person identification [1]. The trustworthiness of biometric features has gained immense popularity over multi-factor authentication. Among several other physiological modalities like a fingerprint, palmprint, finger vein and iris, face biometrics-based applications have had a wide range of applications for several decades. The face is a unique modality and humans easily identify an individual based on facial features. As identification of a person based on facial features can be achieved through the naked eye, facial biometrics has been well accepted for national ID programs and security-related applications, especially in highly secure places such as border control scenarios.

Although Face Recognition Systems(FRS) are widely installed to provide reliable person identification and recognition, it also encounters threats due to various attacks that highlight the vulnerability of FRS. Presentation attacks, adversarial attacks, and imposter attacks are some example attacks that pose a risk to the reliable performance of FRS [2], [3]. In addition to these attacks, a face-morphing attack is one such attack that can efficiently make the FRS vulnerable, especially in border control applications. Although face morphing was initially performed merely for entertainment, it has gradually transformed into a potential threat in the recent past [4]. As face morphing is achieved by blending the facial features of two or more facial identities to generate a morphing image, this will lead to the vulnerability of FRS to reliably recognize the person.

Based on the International Civil Aviation Organisation (ICAO) recommendation, the face is the prominent modality employed for person recognition and verification in the border control scenario [5], [6]. Hence all passport holders must enroll their facial image in the eMRTD to serve as an identification document for border control authority during travel. Face enrolment procedure varies with the country's passport application procedure. Scandinavian countries have installed a photo booth to perform live capture of the facial image [7]. However, most Asian countries accept printed passport-size facial images during the application process [8]. But New Zealand, Ireland and the UK have a web portal where the applicant has to upload the facial image for the passport renewal process [9], [10]. Even though the facial image undergoes manipulation and makes it easier to identify the existence of morphing, the availability of a variety of high-quality morphing software makes it challenging even for an expert human observer.

Several open-source morphing software yield superior quality morphed facial image that does not require any technical expertise [11]–[15]. Hence a person with malicious intentions can easily generate a morphed facial image with a look-alike accomplice's facial image and successfully submit for the passport enrolment process. As it is challenging to detect unknown facial identities from the morphing image, even a trained border control official finds it difficult to detect the existence of morphing [16], [17]. Eventually, the morphing facial image will be enrolled in the eMRTD that can be claimed by both the identities involved in the morphing process. This disregards the rule of single ownership for the passport/eMRTD

document and eventually creates a loophole in the security. Considering the risk of face morphing and its impact on building a secure society, extensive research has been performed to generate robust techniques for Morph Attack Detection(MAD) [18]–[25]. Based on the MAD techniques developed by several researchers, morph attack detection techniques can be broadly classified into single image-based MAD (without reference image) and differential image-based MAD (with reference image). S-MAD techniques are applicable where single facial image-based person verification is required. In the case of the passport renewal process in Ireland, [26], since it is an online passport service, the applicant's facial image must be uploaded into the web portal. As no supervision exists while uploading the facial image into the web portal, an applicant with malicious intentions may end up uploading the morphed facial image.

Hence several researchers have investigated the problem of face morphing and developed reliable techniques. The first work on the S-MAD technique is investigated by Raghavendra et al. [27] using the texture-based approach. Since then, several S-MAD approaches have been proposed that can be broadly divided into [28] three types (1) Hand-crafted features: These techniques include the different types of features such as: texture-based [29] [30] , time-frequency based [31], color based [19], residual noise [32], image quality based [33]–[35] (2) Deep learning features: These includes the use of pre-trained deep CNN networks [36]–[38], fusion of pre-trained CNNs [31], [39], pixel based DCNN MAD [40] (3) Hybrid Features: These MAD techniques are based on using multiple features and classifiers for face morphing detection. The outcome of the multiple classifiers is combined at either feature or comparison level. Several works proposed in this category includes [41], [42], [31], [43]. Among these techniques, the hybrid approaches have indicated the best performances in detecting face-morphing attacks.

All the available State-Of-The-Art (SOTA) techniques are evaluated on the morphed datasets that are not manually and professionally post-processed. Even though the early work [44] attempts to use the manual post-processing morphs, the dataset size is tiny. In this work, we introduce a new dataset to benchmark the S-MAD techniques' performance systematically. The new dataset is constructed using different mediums such as: digital, print-scan using a DNP printer and print-scan using a Canon printer. We have used standard (Canon) and sublimation (DNP) printers to study the influence of printer noise on face morphing attack detection. The new dataset consists of a total of 10710 facial images before and after post-processing. Further, we have also proposed a new S-MAD technique based on the multi-level fusion of ensemble features and classifiers.

To efficiently evaluate the performance of the proposed MAD technique and its performance over SOTA MAD techniques, we investigate the following research questions that facilitate this study.

- **Q1** Does the performance of the proposed method improves when the morph attack detection is performed on post-processed morphing images compared with the morph images before post-processing?
- **Q2** Is the proposed method generalizable for morphed facial images generated from various mediums and the morphing images before and after post-processing?

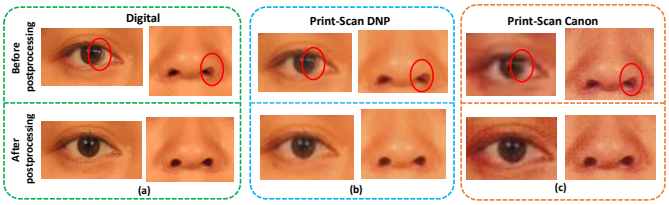

Fig. 1: Illustration of issues of morphing before and after post-processing database from (i) Digital (ii) Print-Scan from DNP (PS-1) (iii) Print-Scan from Canon (PS-2)

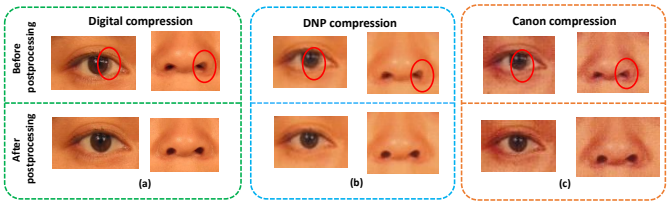

Fig. 2: Illustration of before and after post-processing database from (i) Digital compression (ii) DNP compression (PS-1) (iii) Canon compression (PS-2)

In the course of answering the research questions as mentioned above, the following are the main contributions of this work:

- We present a novel S-MAD approach based on the multi-level fusion of ensemble features and classifiers to detect face-morphing attacks reliably.
- We introduce a new dataset with manual post-processing to achieve high-quality face morphing images free from morphing noise and artefacts. The new dataset is collected using three different mediums that include both digital and two different printers.
- Extensive experiments are carried out to benchmark the detection performance of the proposed method on three different mediums with and without post-processing. Further, the influence of image compression on detection performance is also benchmarked.
- The detection performance of the proposed method is benchmarked with the existing S-MAD techniques in two different experimental protocols.

The rest of the paper is organised as follows: Section II details the newly generated dataset. Section III presents the proposed method using an ensemble of features and classifiers. Section IV details the experimental protocols and corresponding results. Section V provides a discussion on the observation made from the experimental results. Finally, Section V concludes the current work.

II. Face Morphing Dataset

This section presents a new facial morphing dataset constructed using high-quality face images sampled from FRGC V2. The facial images are carefully selected to meet the enrolment guidelines, including zero pose, no shading on the face region, and no occlusion. The new dataset comprises 147 unique data subjects, further divided into two independent groups for training and testing. The training partition consists of 77 unique data subjects and the testing partition consists of 70 unique data subjects. In the next step, we perform the face morphing operation separately on the training and testing set. In this work, we employ the open-source face morphing tools [45], [46] based on landmarks. Further, we have used only two face images with equal weights to perform morphing based on the earlier studies [44], [47] that have indicated high vulnerability on FRS.

In general, the morphing process will result in various types of noises, especially in the eyes and nose region. These noises include double edges in the eye region and the spreading of edges in the nose region. Figure 1 illustrates the noises resulting from the morphing process that can be attributed to the variation in the geometry of the faces used for morphing. Even though these morphing noises are not common but exist in most cases, as shown in Figure 1, the morphing noises can also be predominantly observed even after the print-scan process. However, the quality of the print-scan process can also affect the visibility of edge spreading, as shown in Figure 1(c). Further, as noticed from Figure 2, even after the images are compressed to follow the guidelines of ICAO [48], [49], the morphing noises are still visible in both digital and print-scan versions. Therefore, it is essential to post-process the morphing face image to weed out these noises so that the human observer cannot identify the morphing based on these noises.

Image Type	before post-processing	after post-processing	Total
Digital images	1071	1071	2142
Print & Scan	1071X2 (printers)	1071 X 2 (printers)	4284
Print & Scan compression	1071X2 (printers)	1071X2 (printers)	4284
Total	5355	5355	10710

TABLE I: Total number of morphing images before and after manual post-processing.

TABLE II: Database statistics: training and testing partitions

Data Partition	**Data Type**					
	Digital		**PS-1**		**PS-2**	
	Bona fide	**Morph**	**Bona fide**	**Morph**	**Bona fide**	**Morph**
Training	689	517	689	517	689	517
Testing	583	554	583	554	583	554

Table I tabulates the statistics of the newly developed face morphing dataset with morphing samples before and after manual post-processing. The manual post-processing is carried out using Adobe Photoshop [50] to obtain professional-quality passport face images. Figure 1 and 2 illustrates the manual post-processing images in which the morphing noises are corrected to achieve the highest quality of the morphed face images. In this work, face morphing uses the alpha value (or morphing factor) of 0.5 by considering the highest vulnerability demonstrated in several earlier works [44], [47].

We first generate the face morphing images separately for the training and testing sets. In the next step, we used two different printers, which are DNP and a Canon printer, to digitize the digital images by print & scan. The DNP printer used in this work is the dye-sublimation photo printer that can generate the highest quality passport face images and is widely deployed in photo studios. In contrast, the CANON PIXMA printer is a conventional inkjet printer used for printing passport face images. We term the data generated using the DNP printer as PS-1 and CANON PIXMA printer as PS-2, respectively. Figure 2 illustrates the example images from the newly developed datasets before and after manual post-processing.

A. Dataset partition: Train and Test

To effectively evaluate the Morph Attack Detection (MAD) algorithms, the whole dataset is partitioned into two independent sets: training and testing. The training set consists of 77 unique data subjects and the testing partition consists of 70 unique data subjects. The morphing images are generated by using the data subjects within each partition. Thus, the training set comprises 689 bona fide and 517 morph face images. Table II indicates the statistics of training and testing independently for morphing samples before and after manual post-processing.

III. Proposed Method

Figure 3 shows the block diagram of the proposed method leveraged on the multi-level score level fusion of multiple features. The main objective of the proposed method is to exploit the complementary features of the different feature extractors and classifiers combined at two different levels. We assert that the use of complementary features and classification scores can capture the discriminant information useful for reliable face morph detection. The proposed method is designed using four different functional units, namely: (a) color space, (b) scale-space decomposition, (c) multiple features and classifiers (d) multi-level fusion. We discuss each of the functional units in detail in the following subsections.

A. Color space representation

Given the input image I, the first step is to extract the different color spaces using YC_bC_r and HSV. We have selected these two color spaces by considering their robustness to capture the morphing noises as is demonstrated in earlier works [19]. Thus, for the given image I, we get six different representations such as:$I_{Col} = I_H, I_S, I_V, I_Y, I_{C_b}, I_{C_r}$.

B. Scale-Space decomposition

In the next step, we extract the scale-space features on each color space image using the Laplacian pyramid [51]. The choice of Laplacian pyramid-based scale-space features extraction is made by considering the effectiveness in extracting

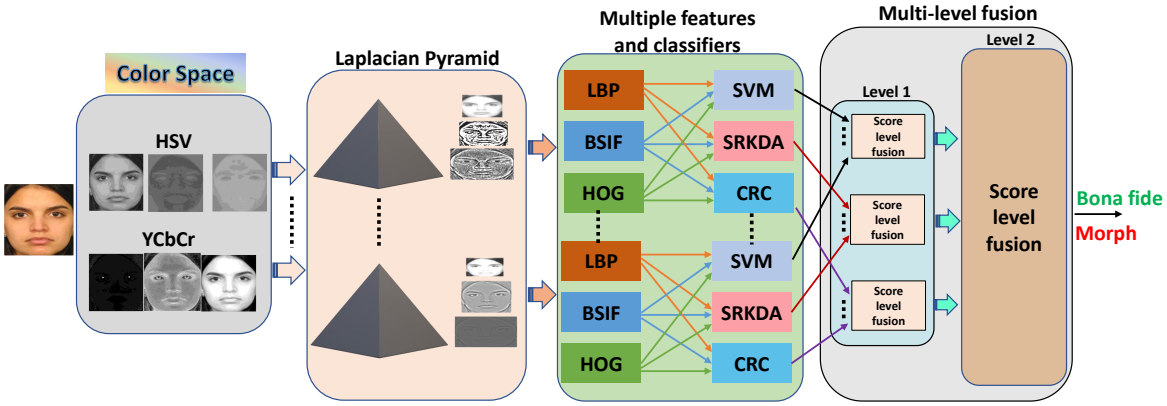

Fig. 3: Block diagram of the proposed method

the discriminant features compared to similar techniques such as steerable pyramids [43]. We use three-level decomposition on each color image based on their empirical evaluation. Thus, given the color image I_H, the corresponding scale-space images can be represented as I_{H1}, I_{H2}, I_{H3}. In this work, we have used six different color channels and thus, the corresponding scale-space representation will result in $6 \times 3 = 18$ sub-images that are independently processed to extract the multiple features. Let the sub-images be represented as: $SI_k = SI_1, SI_2, \ldots, SI_{18}, \forall k = 1, 2, \ldots, 18$.

C. Multiple features and classifiers

Multiple features and classification systems used in this work are based on three types of feature extraction and three different classifiers. Three different feature extraction techniques include Local Binary Patterns (LBP), Histogram of Gradients (HoG) and Binary Statistical Image Features (BSIF). These three features are selected by considering the complementary features that include texture features extracted using both hand-crafted and naturally learned in addition to the gradient information. These features represent the image's different characteristics, especially the pixel discontinuities, and thus can provide rich information to detect the morphing processing. Given the sub-image $SI_k, \forall k = 1, 2, \ldots, 18$, three different types of features are extracted independently.

In the next step, we employ three different types of classifiers, including linear Support Vector Machine (SVM) [52], Spectral Regression Kernel Discriminant Analysis (SRKDA) [53] and Probabilistic Collaborative Representation Classifier (P-CRC) [54]. We have considered these three classifiers by considering the high performance and robustness of various data sources [28]. Further, the non-availability of the large-scale morphing database justifies the choice of the ensemble of these three classifiers to achieve reliable morph detection. Given the features independently from the three different feature extraction techniques, we independently obtain the comparison scores from three different classification techniques.

D. Multi-level fusion

This work proposes the two-level fusion of comparison scores obtained using multiple classifiers. The first level of fusion will combine the comparison scores obtained using individual classifiers corresponding to three different feature extraction techniques. Therefore, first-level fusion has three independent fusion units corresponding to three independent classifiers. In the second level, we combine the comparison scores from the first level corresponding to individual classifiers to make the final decision. The multi-level fusion is designed based on empirical experiments that have indicated superior performance compared to serial fusion. At both levels, we have used the weighted sum rule to perform the fusion and weights are computed using the bootstrap method [55] on the development dataset and kept constant through the experiments.

IV. Experiments and Results

TABLE III: Experiment-1: Quantitative results of MAD algorithms on different datasets

Dataset	Post-processing		MAD Algorithms	Detection Performance			Detection Performance		
				D-EER (%)	BPCER @APCER		D-EER (%)	BPCER @APCER	
					=5%	=10%		=5%	=10%
	Training	Testing		without compression			with compression		
Digital	Before	Before	**Proposed Method**	**0**	**0**	**0**	**0**	**0**	**0**
			Ensemble Features [20]	0.18	0	0	0.18	0	0
			Hybrid Features [19]	0	0	0	0.18	0	0
	After	After	**Proposed Method**	**0.18**	**0**	**0**	**0.36**	**0**	**0**
			Ensemble Features [20]	0.18	0	0	0.36	0	0
			Hybrid Features [19]	0.18	0	0	0.18	0	0
PS-1	Before	Before	**Proposed Method**	**0**	**0**	**0**	**3.45**	**2.47**	**1.02**
			Ensemble Features [20]	0	0	0	4.27	3.6	1.71
			Hybrid Features [19]	0	0	0	5	5.14	2.4
	After	After	**Proposed Method**	**0**	**0**	**0**	**3.09**	**2.22**	**1.02**
			Ensemble Features [20]	0	0	0	3.28	2.4	1.54
			Hybrid Features [19]	0	0	0	4.46	4.28	2.74
PS-2	Before	Before	**Proposed Method**	**10.00**	**15.01**	**10.66**	**7.72**	**11.83**	**7.2**
			Ensemble Features [20]	11.00	16.98	11.66	8.72	11.66	8.06
			Hybrid Features [19]	14.09	29.33	19.38	8.54	14.4	6.86
	After	After	**Proposed Method**	**5.74**	**6.34**	**3.75**	**5.19**	**5.14**	**2.91**
			Ensemble Features [20]	6.01	7.03	4.11	5.19	5.14	3.77
			Hybrid Features [19]	8.56	12.34	7.2	5.64	6.17	2.91

TABLE IV: Experiment-2: Quantitative performance of MAD algorithms on before post-processing data generated using different morphing types

Training data	Testing Data	MAD Algorithms	Detection Performance			Detection Performance		
			D-EER (%)	BPCER @APCER		D-EER (%)	BPCER @APCER	
				=5%	=10%		=5%	=10%
			without compression			with compression		
Digital	PS-1	**Proposed Method**	**31.90**	**78.38**	**67.12**	**31.64**	**77.53**	**67.58**
		Ensemble Features [20]	38.27	87.82	80.27	38.09	89.02	81.3
		Hybrid Features [19]	37.72	88.67	78.9	35.73	86.96	76.67
	PS-2	**Proposed Method**	**47.08**	**94.68**	**88.16**	**45.45**	**92.79**	**86.96**
		Ensemble Features [20]	50	97.77	93.31	50	97.42	92.28
		Hybrid Features [19]	50	96.22	93.65	50	94.85	90.73
PS-1	Digital	**Proposed Method**	**3.63**	**2.22**	**0.68**	**5.26**	**5.48**	**3.77**
		Ensemble Features [20]	8.09	14.23	6.51	8.09	15.6	6.51
		Hybrid Features [19]	8.54	13.2	7.54	20.72	43.91	33.1
	PS-2	**Proposed Method**	**20.9**	**55.74**	**41.16**	**12.18**	**23.67**	**15.95**
		Ensemble Features [20]	19.72	45.11	33.44	13.18	21.09	15.26
		Hybrid Features [19]	24.91	57.11	45.45	13.36	22.98	18.01
PS-2	Digital	**Proposed Method**	**9.45**	**16.63**	**8.74**	**9.63**	**16.98**	**9.6**
		Ensemble Features [20]	21.09	46.31	36.02	17.63	40.13	26.92
		Hybrid Features [19]	9.63	20.41	9.26	23.18	43.05	33.1
	PS-1	**Proposed Method**	**12.27**	**30.1**	**18.09**	**0.16**	**0**	**0**
		Ensemble Features [20]	14.27	28.64	19.72	0.16	0	0
		Hybrid Features [19]	19.72	42.19	31.73	0.72	0	0

TABLE V: Experiment-2: Quantitative performance of MAD algorithms on after post-processing data generated using different morphing types

Training data	Testing Data	MAD Algorithms	Detection Performance			Detection Performance		
			D-EER (%)	BPCER @APCER		D-EER (%)	BPCER @APCER	
				=5%	=10%		=5%	=10%
			without compression			with compression		
Digital	PS-1	**Proposed Method**	**31.24**	**78.55**	**65.69**	**31.87**	**78.9**	**68.09**
		Ensemble Features [20]	34.15	83.53	76.67	37.52	87.13	77.53
		Hybrid Features [19]	38.06	89.87	80.78	37.7	88.67	81.3
	PS-2	**Proposed Method**	**35.6**	**87.3**	**71.18**	**36.15**	**87.47**	**74.09**
		Ensemble Features [20]	39.25	93.31	84.21	42.26	94.51	84.56
		Hybrid Features [19]	44.44	91.25	82.16	41.71	91.59	80.61
PS-1	Digital	**Proposed Method**	**4.09**	**3.94**	**2.91**	**6.82**	**9.43**	**5.83**
		Ensemble Features [20]	9.37	15.43	8.06	8.19	12	12.17
		Hybrid Features [19]	20.03	32.76	27.44	28.14	60.2	49.05
	PS-2	**Proposed Method**	**12.12**	**25.27**	**15.32**	**7.47**	**10.69**	**6.83**
		Ensemble Features [20]	13.02	26.75	16.63	8.19	12	6.86
		Hybrid Features [19]	24.86	50.08	42.19	10.47	16.46	10.46
PS-2	Digital	**Proposed Method**	**10.47**	**21.09**	**11.49**	**11.84**	**23.15**	**13.2**
		Ensemble Features [20]	18.48	45.11	31.9	15.93	38.59	25.38
		Hybrid Features [19]	11.1	26.92	13.89	23.13	44.94	36.87
	PS-1	**Proposed Method**	13.93	28.98	19.55	**0**	**0**	**0**
		Ensemble Features [20]	9.92	18.18	9.94	0.16	0	0
		Hybrid Features [19]	18.48	41.16	30.7	0.55	0	0

TABLE VI: Experiment-3: Quantitative performance of MAD algorithms by training after post-processing data and testing before post-processing data generated using different morphing types

Training data	Testing Data	MAD Algorithms	Detection Performance			Detection Performance		
			D-EER (%)	BPCER @APCER		D-EER (%)	BPCER @APCER	
				=5%	=10%		=5%	=10%
			without compression			with compression		
Digital	PS-1	**Proposed Method**	**30.72**	**80.44**	**68.95**	**31.9**	**80.44**	**67.92**
		Ensemble Features [20]	36.18	86.96	79.07	37.72	88.67	79.41
		Hybrid Features [19]	37.54	89.7	81.3	35.99	86.1	78.55
	PS-2	**Proposed Method**	**46.45**	**94.16**	**88.67**	**46.63**	**93.31**	**87.99**
		Ensemble Features [20]	50.27	97.25	93.31	51.27	96.91	92.1
		Hybrid Features [19]	50.9	94.16	90.39	52.09	95.54	91.76
PS-1	Digital	**Proposed Method**	**5.45**	**5.83**	**3.6**	**8.9**	**13.55**	**8.57**
		Ensemble Features [20]	13.1	25.55	18.52	13.18	25.72	16.12
		Hybrid Features [19]	9.82	19.72	9.6	27.09	60.89	51.11
	PS-2	**Proposed Method**	**17.9**	**37.77**	**26.7**	**11.81**	**22.29**	**12.52**
		Ensemble Features [20]	18.54	41.16	29.5	11.99	20.06	12.69
		Hybrid Features [19]	28.08	56.43	45.62	12.36	21.95	15.09
PS-2	Digital	**Proposed Method**	**11.81**	**21.44**	**14.92**	**13.72**	**31.73**	**21.09**
		Ensemble Features [20]	22.08	50.94	39.1	18.81	44.59	28.47
		Hybrid Features [19]	13.36	29.15	17.15	22.63	46.68	34.47
	PS-1	**Proposed Method**	**12.72**	**21.56**	**13.32**	**0.3**	**0**	**0**
		Ensemble Features [20]	13.18	22.81	16.46	0.16	0	0
		Hybrid Features [19]	18.99	40.13	30.7	0.72	0	0

TABLE VII: Experiment-3: Quantitative performance of MAD algorithms by training before post-processing data and testing after post-processing data generated using different morphing types

Training data	Testing Data	MAD Algorithms	Detection Performance			Detection Performance		
			D-EER (%)	BPCER @APCER		D-EER (%)	BPCER @APCER	
				=5%	=10%		=5%	=10%
			without compression			with compression		
Digital	PS-1	**Proposed Method**	**32.05**	**79.93**	**69.12**	**32.6**	**79.07**	**71.01**
		Ensemble Features [20]	36.52	87.82	80.96	38.88	89.36	80.96
		Hybrid Features [19]	39.25	89.87	83.87	37.7	88.5	80.78
	PS-2	**Proposed Method**	**37.25**	**90.05**	**75.64**	**36.15**	**88.67**	**74.95**
		Ensemble Features [20]	40.61	95.54	87.13	42.34	95.71	86.44
		Hybrid Features [19]	45.44	93.13	83.87	41.16	91.93	80.96
PS-1	Digital	**Proposed Method**	**3.46**	**2.57**	**1.02**	**5.64**	**6.68**	**3.94**
		Ensemble Features [20]	8.92	15.6	7.54	9.92	16.63	9.77
		Hybrid Features [19]	17.3	32.76	24.52	22.13	45.45	34.81
	PS-2	**Proposed Method**	**16.4**	**40.96**	**29.81**	**10.29**	**20.92**	**10.97**
		Ensemble Features [20]	17.66	42.02	31.73	10.65	18.01	11.32
		Hybrid Features [19]	24.31	50.08	41.16	11.84	19.03	13.55
PS-2	Digital	**Proposed Method**	**9.74**	**16.46**	**8.91**	**10.47**	**17.32**	**10.97**
		Ensemble Features [20]	22.41	47.51	37.9	17.66	42.53	28.47
		Hybrid Features [19]	9.74	25.9	9.6	24.04	47.68	37.56
	PS-1	**Proposed Method**	**12.48**	**23.04**	**16.26**	**0.16**	**0**	**0**
		Ensemble Features [20]	13.93	26.75	18.01	0.16	0	0
		Hybrid Features [19]	20.94	44.25	34.3	0.55	0	0

In this section, we present and discuss the proposed method's quantitative results and the existing methods such as Hybrid features [19] and Ensemble features [20]. We particularly select these two existing methods as (1) these methods indicate the best performance in several reported studies [28] and one of them is benchmarked on the NIST FRVT morph [56] (2) these methods are based on the hand-crafted features thus are more appropriate to be compared with the proposed method (3) these methods are more appropriate by considering the size of the databases used in this work. The use of deep learning methods may result in overfitting due to the small datasets. The performance of the S-MAD techniques is benchmarked using ISO/IEC 30107-3 [57] metrics such as Attack Presentation Classification Error Rate (APCER (%)), Bona fide Presentation Classification Error Rate (BPCER(%)) and Detection-Equal Error Rate (D-EER(%)).

A. Experimental protocols:

To effectively evaluate the performance of the MAD algorithms using the proposed method, our experiments are categorized into three different protocols discussed as follows:

- **Experiment-1: Intra-dataset evaluation:** is performed within the same dataset type. This evaluation protocol performs training and testing on the same dataset type. As shown in Table III, the three dataset types (digital, PS-I and PS-II) are independently evaluated before and after post-processing. For instance, the digital dataset type before post-processing is trained and the same dataset type is tested. A similar protocol is followed for the digital dataset type after post-processing, followed by the two different print-scan dataset types PS-I (before and after post-processing) and PS-II (before and after post-processing). All experiments are carried out with and without compression.
- **Experiment-2: Inter-medium evaluation**: is performed to analyze the MAD performance of the proposed method

in cross-dataset types. This protocol is designed to investigate the robustness of the proposed method when it is trained and tested on different dataset types (digital, PS-1 and PS-2) generated from different mediums (digital, print-scan with and without compression). Tables IV and V indicates the two different experiments performed for cross-dataset evaluation in the inter-medium scenario. Among the three dataset types employed in this work, we train one dataset type and test it on the other two. For instance, if the digital dataset type is trained, the two different print-scan dataset types, PS-I and PS-II, are tested. The same evaluation protocol is followed for the two print-scan dataset types. To better evaluate the cross-dataset performance of the proposed method, we have performed two different experiments (i) inter-medium evaluation before post-processing and (ii) inter-medium evaluation after post-processing.

- **Experiment-3: Inter-medium varied post-processing**: is performed to evaluate the performance of MAD in cross datasets generated from various mediums (digital, print-scan with and without compression) in both before and after post-processing scenarios. Tables VI and VII indicates the two experiments conducted for inter-medium and varied post-processing scenario. Two different experiments were conducted to evaluate the proposed method's performance. Following the similar experimental protocol as inter-medium evaluation, the first experiment is performed by (i) training the dataset types after post-processing and testing the dataset types before post-processing. The second experiment is performed by training the dataset types before post-processing and testing after post-processing.

B. Experimental results

In this section, we present the quantitative results of the proposed method and the existing methods of the three different evaluation protocols. The quantitative results obtained from the three different protocols designed for intra-dataset evaluation, inter-medium evaluation and inter-medium with varied post-processing evaluation scenarios are tabulated in the Tables III, IV, V, VI, VII.

*1) **Results on Experiment-1: Intra-dataset evaluation**:* Based on the obtained results presented in Table III following are the main observations:

- The proposed method has indicated the best performance on all three data mediums before and after post-processing. Thus, the proposed method has emerged as the best-performing method before and after post-processing.
- The detection performance of the existing methods also indicates the competitive performance, especially with digital and PS-1 data mediums both before and after post-processing.
- The detection performance of the S-MAD techniques indicates the degraded performance, especially with the PS-2 data medium that can be noticed before and after post-processing data. Thus, the morph generation quality will impact the detection accuracy of both the proposed and existing S-MAD techniques.
- Performing the post-processing indicates the impact on the detection performance. In some cases, the detection performance of the proposed method and the existing methods indicates improvement. This can be attributed to the possible variations in the image quality that might have resulted from post-processing operation. However, with data compression, the performance difference is not noticeable.
- The performance of the S-MAD algorithms also varies with and without compression, irrespective of the post-processing.

*2) **Results on Experiment-2: Inter-medium evaluation**:* Table IV and V indicates the quantitative performance of the proposed method together with existing methods in Experiment 2. Based on the obtained results following can be noted:

- The Inter-medium training and testing indicate the drastic degradation of the detection accuracy of both the proposed method and the existing methods. The degradation is noticed both before and after post-processing.
- The S-MAD algorithms degrade more when algorithms are trained with digital and tested against PS-I and PS-II. Less degradation is noted when S-MAD algorithms are trained with PS-I and tested against digital and PS-II. Similar degradation is noticed both before and after post-processing.
- The S-MAD algorithms have indicated a better detection accuracy on the print-scan compression when compared to without compression, especially on the before post-processing data. However, the S-MAD algorithms did not show much difference in the detection performance on the before post-processing data. This indicates that using the post-processing data to train and test the S-MAD algorithms might be key to achieving the generalisation in cross-medium experiments.
- Based on the experimental results in Experiment-2, the proposed method has indicated the best performance compared to existing methods on both before and after post-processing data.

*3) **Experiment-3: Inter-medium varied post-processing**:* In this section, we discuss the quantitative results of the proposed method and the existing S-MAD techniques, especially to study the influence of post-processing operation versus different mediums on detection accuracy. Tables VI and VII indicate the quantitative results of the S-MAD techniques, including the proposed method. Based on the obtained results, the following can be noted:

- The performance of the S-MAD algorithms indicates the degraded detection rate irrespective of the data post-processing type.
- In general, the performance of the S-MAD algorithms, including the proposed method, indicates the marginal im-

provement in the detection performance when trained using post-processed data irrespective of the data medium.
- The performance of the proposed method indicates the best performance compared with the existing methods, irrespective of the data type (before or after post-processing) used for the training. The best performance of the proposed method is when PS-1 is trained and tested on digital data before and after post-processing.

V. Discussion

The research questions formulated in Section I are answered below based on the extensive experiments conducted, obtained results and the observations made above.

- **Q1**. Does the performance of the proposed method improve when the morph attack detection is performed on post-processed morphed images when compared with the morph images before post-processing?
  - As noted by the obtained experimental results reported in Table IV V, the performance of the proposed method shows a marginal improvement when used with the morph images after post-processing in Experiment-1, especially on the PS-2 data medium. However, the proposed method's performance did not significantly influence (even though the proposed method has shown little improvement in some cases) the post-processing in Experiment-2.
- **Q2**.Is the proposed method generalizable for morphed facial images generated from various mediums and also for the morphed images before and after post-processing?
  - Based on the experimental results (see Table III IV, V, VI, VII), the proposed method has indicated the best performance in two different experimental protocols.

Thus, based on the obtained results, one can attribute the improvements to using multiple features with multiple classifiers, which would increase generalization.

VI. Conclusions and Future Work

Reliable face morphing attack detection using a single image is a challenging problem due to the variation in image quality attributed to the various source of the morph generation and digitisation processes. In this work, we proposed a new framework for S-MAD using multiple features and classifiers whose comparison scores are combined at multiple levels to detect face-morphing attacks reliably. We have also introduced a new dataset based on manual post-processing to generate high-quality face morphing images free from morphing artefacts. The dataset constructed has three different mediums: digital, Print-Scan (PS-1 re-digitised using DNP printer and PS-2 re-digitised using CANON printer) and print-scan compression. Extensive experiments are carried out using two different evaluation protocols to benchmark the performance of the proposed method together with the existing methods. The obtained results demonstrated the best performance of the proposed method in two different evaluation protocols compared with the existing methods. In future work, we could evaluate more advanced fusion techniques, benchmarking the proposed method and comparison with more SOTA approaches.

References

[1] A. Jain, P. Flynn, and A. Ross, *Handbook of Biometrics*. Springer, July 2007.

[2] R. Raghavendra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Comput. Surv.*, vol. 50, no. 1, Mar. 2017. [Online]. Available: https://doi.org/10.1145/3038924

[3] F. Vakhshiteh, A. Nickabadi, and R. Ramachandra, "Adversarial attacks against face recognition: A comprehensive study," *IEEE Access*, vol. 9, pp. 92 735–92 756, 2021.

[4] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *2014 IEEE Intl. Joint Conf. on Biometrics (IJCB)*, September 2014, pp. 1–7.

[5] International Civil Aviation Organization, "Machine readable passports – part 12 – public key infrastructure for MRTDs," http://www.icao.int/publications/Documents/9303_p12_cons_en.pdf, International Civil Aviation Organization (ICAO), 2015.

[6] International Civil Aviation Organization, "Machine readable passports – part 9 – deployment of biometric identification and electronic storage of data in eMRTDs," http://www.icao.int/publications/Documents/9303_p9_cons_en.pdf, International Civil Aviation Organization (ICAO), 2021, last accessed: 2021-11-23.

[7] T. Kalvet, H. Karlzén, A. Hunstad, and M. Tiits, "Live enrollment for identity documents in europe: The cases of sweden, norway, kosovo, and estonia," *JeDEM - eJournal of eDemocracy and Open Government*, 2018.

[8] "OCI services, india," https://ociservices.gov.in/Photo-Spec-FINAL.pdf, accessed: May 2020.

[9] "Department of Internal Affairs (DIA), NZ," https://www.passports.govt.nz/passport-photos/passport-photo-requirements/.

[10] "GOV.UK," https://www.gov.uk/photos-for-passports, accessed: May 2020.

[11] "Abrosoft fantamorph," FantaMorph,Abrasoft:http://www.fantamorph.com/, 2021, accessed: September 2021.

[12] "3dthis face morph," https://3dthis.com/morph.htm, 2021, accessed: September 2021.

[13] "Face swap online," https://faceswaponline.com/, 2021, accessed: September 2021.

[14] "Morph thing," https://www.morphthing.com/, 2021, accessed: September 2021.

[15] "Face morpher," http://www.facemorpher.com/, 2021, accessed: September 2021.

[16] R. S. Kramer, M. O. Mireku, T. R. Flack, and K. L. Ritchie, "Face morphing attacks: Investigating detection with humans and computers," *Cognitive research: principles and implications*, vol. 4, no. 1, pp. 1–15, 2019.

[17] D. Robertson, R. Kramer, and A. Burton, "Fraudulent ID using face morphs: Experiments on human and automatic recognition," *Plos One*, March 2017.

[18] 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.

[19] R. Raghavendra, S. Venkatesh, K. Raja, and C. Busch, "Towards making morphing attack detection robust using hybrid scale-space colour texture features," in *IEEE 5th Intl. Conf. on Identity, Security, and Behavior Analysis (ISBA)*. IEEE, January 2019.

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

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

[22] M. Ferrara, A. Franco, and D. Maltoni, "Face demorphing in the presence of facial appearance variations," in *2018 26th European Signal Processing Conference (EUSIPCO)*. IEEE, 2018, pp. 2365–2369.

[23] L. Spreeuwers, M. Schils, and R. Veldhuis, "Towards robust evaluation of face morphing detection," in *Proc. of the 26th European Signal Processing Conf. (EUSIPCO)*, 2018.

[24] J. M. Singh, R. Ramachandra, 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)*. IEEE, 2019, pp. 106–112.

[25] J. M. Singh and R. Ramachandra, "Reliable face morphing attack detection in on-the-fly border control scenario with variation in image resolution and capture distance," in *2022 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2022, pp. 1–10.

[26] "Passport online," https://www.dfa.ie/passportonline/, 2021, accessed: September 2021.

[27] R. Raghavendra, K. Raja, and C. Busch, "Detecting morphed face images," in *2016 IEEE 8th Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 8th IEEE Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS-2016). IEEE, September 2016.

[28] 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.

[29] A. Makrushin, C. Kraetzer, J. Dittmann, C. Seibold, A. Hilsmann, and P. Eisert, "Dempster-shafer theory for fusing face morphing detectors," in *2019 27th European Signal Processing Conf. (EUSIPCO)*. IEEE, September 2019.

[30] A. Makrushin, C. Kraetzer, T. Neubert, and J. Dittmann, "Generalized benford's law for blind detection of morphed face images," in *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, ser. IH&MMSec '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 49–54. [Online]. Available: https://doi.org/10.1145/3206004.3206018

[31] P. Aghdaie, B. Chaudhary, S. Soleymani, J. Dawson, and N. M. Nasrabadi, "Detection of morphed face images using discriminative wavelet sub-bands," 2021.

[32] S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, "Morphed face detection based on deep color residual noise," in *9th Intl. Conf. on Image Processing Theory, Tools and Applications (IPTA)*. IEEE, November 2019.

[33] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann, "Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps," in *2017 5th Intl. Workshop on Biometrics and Forensics (IWBF)*. IEEE, April 2017, pp. 1–6.

[34] C. Seibold, A. Hilsmann, and P. Eisert, "Reflection analysis for face morphing attack detection," in *Proc. of the 26th European Signal Processing Conf. (EUSIPCO)*, 2018.

[35] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch, and A. Uhl, "Detection of face morphing attacks based on PRNU analysis," *Trans. on Biometrics, Behavior, and Identity Science (TBIOM)*, 2019.

[36] C. Seibold, A. Hilsmann, and P. Eisert, "Style your face morph and improve your face morphing attack detector," in *2019 Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*. IEEE, September 2019.

[37] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch, "Transferable deep-cnn features for detecting digital and print-scanned morphed face images," in *IEEE Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1822–1830.

[38] M. Ferrara, A. Franco, and D. Maltoni, "Face morphing detection in the presence of printing/scanning and heterogeneous image sources," *CoRR*, vol. abs/1901.08811, 2019. [Online]. Available: http://arxiv.org/abs/1901.08811

[39] S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, "Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network," in *The IEEE Winter Conference on Applications of Computer Vision (WACV)*, March 2020, pp. 1–8.

[40] N. Damer, N. Spiller, M. Fang, F. Boutros, F. Kirchbuchner, and A. Kuijper, "Pw-mad: Pixel-wise supervision for generalized face morphing attack detection," *arXiv preprint arXiv:2108.10291*, 2021.

[41] P. Aghdaie, B. Chaudhary, S. Soleymani, J. Dawson, and N. M. Nasrabadi, "Morph detection enhanced by structured group sparsity," *arXiv preprint arXiv:2111.14943*, 2021.

[42] K. O'Haire, S. Soleymani, B. Chaudhary, P. Aghdaie, J. Dawson, and N. M. Nasrabadi, "Adversarially perturbed wavelet-based morphed face generation," 2021.

[43] R. Raghavendra, S. Venkatesh, K. Raja, and C. Busch, "Detecting face morphing attacks with collaborative representation of steerable scale-space features," in *Intl. Conf. on Computer Vision and Image Processing (CVIP)*, September 2018.

[44] K. Raja, M. Ferrara, A. Franco, L. Spreeuwers, I. Batskos, *et al.*, "Morphing attack detection - database, evaluation platform and benchmarking," *IEEE Trans. on Information Forensics and Security*, November 2020.

[45] M. Ferrara, A. Franco, and D. Maltoni, *Face Recognition Across the Imaging Spectrum*. Springer, 2016, ch. On the Effects of Image Alterations on Face Recognition Accuracy.

[46] M. Ferrara, A. Franco, and D. Maltoni, "Decoupling texture blending and shape warping in face morphing," in *Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*. IEEE, September 2019.

[47] S. Venkatesh, K. Raja, R. Ramachandra, and C. Busch, "On the influence of ageing on face morph attacks: Vulnerability and detection," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*, 2020, pp. 1–10.

[48] International Civil Aviation Organization, "Machine readable passports – part 1 – introduction," http://www.icao.int/publications/Documents/9303_p1_cons_en.pdf, International Civil Aviation Organization (ICAO), 2015, last accessed: 2015-11-23.

[49] Intl. Civil Aviation Organization, "Machine readable passports – part 9 – deployment of biometric identification and electronic storage of data in emrtds," http://www.icao.int/publications/Documents/9303_p9_cons_en.pdf, International Civil Aviation Organization (ICAO), 2015, last accessed: 2015-11-23.

[50] "Adobe photoshop," https://www.adobe.com/no/products/photoshop.html, 2021, accessed: December 2021.

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

[52] V. Vapnik, "An overview of statistical learning theory," *IEEE Transactions on Neural Networks*, vol. 10, no. 5, pp. 988–999, 1999.

[53] D. Cai, X. He, and J. Han, "Speed up kernel discriminant analysis," *The VLDB Journal—The International Journal on Very Large Data Bases*, vol. 20, no. 1, pp. 21–33, 2011.

[54] L. Zhang, M. Yang, and X. Feng, "Sparse representation or collaborative representation: Which helps face recognition?" in *2011 International Conference on Computer Vision (ICCV)*, 2011, pp. 471–478.

[55] R. Raghavendra and C. Busch, "Novel image fusion scheme based on dependency measure for robust multispectral palmprint recognition," *Pattern Recognition*, vol. 47, no. 6, pp. 2205–2221, 2014.

[56] 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.

[57] 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.