Towards making Morphing Attack Detection robust using hybrid Scale-Space Colour Texture Features

Raghavendra Ramachandra, Sushma Venkatesh, Kiran Raja, Christoph Busch
Norwegian Biometrics Laboratory, NTNU - Gjøvik, Norway
{raghavendra.ramachandra; sushma.venkatesh; kiran.raja; christoph.busch} @ntnu.no

Abstract

The widespread use of face recognition algorithms, especially in Automatic Border Control (ABC) systems has raised concerns due to potential attacks. Face morphing combines more than one face images to generate a single image that can be used in the passport enrolment procedure. Such morphed passports have proven to be a significant threat to national security, as two or more individuals that contributed to the morphed reference image can use that single travel document. In this work, we present a novel method based on hybrid colour features to automatically detect morphed face images. The proposed method is based on exploring multiple colour spaces and scale-spaces using a Laplacian pyramid to extract robust features. The texture features corresponding to each scale-space in different color spaces are extracted with Local Binary Patterns (LBP) and classified using a Spectral Regression Kernel Discriminant Analysis (SRKDA) classifier. The scores are further fused using sum rule to detect the morphed face images. Experiments are carried out on a large-scale morphed face image database consisting of printed and scanned images to reflect the real-life passport issuance scenario. The evaluation database consists of images comprised of 1270 bona fide face images and 2515 morphed face images. The performance of the proposed method is compared with seven different deep learning and seven different non-deep learning methods, which has indicated the best performance of the proposed scheme with Bona fide Presentation Classification Error (BPCER) = 0.86% *@ Attack Presentation Classification Error Rate (APCER) =* 10% *and BPCER =* 7.59% *@ APCER =* 5%*. The obtained results indicate the robustness in detecting morphing attacks as compared to earlier works.*

2019 IEEE 4^{th} *International Conference on Identity, Security, and Behavior Analysis (ISBA)*
978-1-7281-0532-1/19/$31.00

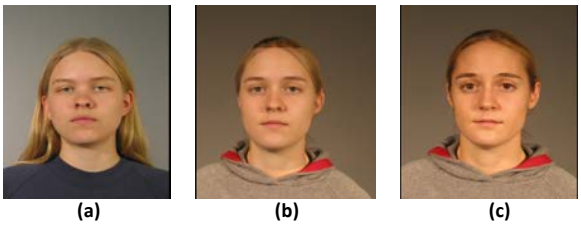


Figure 1: Example of face morphing (a) Subject 1 (b) Morphed face image (c) Subject 2

1. Introduction

Face recognition algorithms are widely deployed in several applications that also include the identity check at the border crossing using Automatic Border Control (ABC) systems. The availability of standardized electronic Machine Readable Travel Documents (eMRTD) storing a face image of the document owner has further boosted the deployment of ABC systems in border control processes. An ABC system verifies the identity of a capture subject by comparing the face image stored in the eMRTD with the live probe image captured from the ABC system. ABC systems are already operational in more than 180 countries in which the biometric verification at border control supports a human expert decision [18].

Enabling wide deployment of ABC systems at border control has raised the awareness towards various attacks that can be broadly classified as [15]: Attacks against the ABC system in the form of presentation attack and attacks on the eMRTD, by modifying the facial data stored in the Logical Data Structure (LDS) of the eMRTD. Attacks against the ABC system itself can be addressed by using Presentation Attack Detection (PAD) methods and attacks on eMRTD LDS can be easily spotted as the hash computed over the facial image (data group 2 in the LDS) would be different, if for instance the face image is replaced. However, it was demonstrated that the submission of a morphed face images in which the facial representation of two individu-

Table 1: Overview of existing face morphing attack detection techniques

Detection type	Morphed Image type	Technique type
No-reference MAD	Digital Morphed Images	**Texture Methods:** LBP [15], LPQ [15], BSIF [15], 2DFFT [15], media forensics [11], Image forensics [1], SIFT [11], SURF [11], FAST [11].
		Deep Learning: Pre-trained deep network models [16], [23] & [17]
		Image Degradation: StirTrace algorithm [9], JPEG compression artefacts [13], PRNU [6], Benfords features [12], Specular reflection [22].
	Print & Scanned Images	**Texture Methods:** LBP [20] [14], LPQ [20] [14], BSIF [20] [14], LPQ [20] [14], Color Textures [14], Steerable features [17].
		Deep Learning: Pre-trained deep network models [16].
		Image Degradation: StirTrace algorithm [9].
Differential MAD	Digital Morphed Images	**Texture Methods:** LBP, HOG, SURF, BSIF with feature difference [21].
		Facial Geometry: 2D landmarks[19].
		Image subtraction: Demorphing [8].
	Print & Scanned Images	**Image subtraction:** Demorphing [8].

als is combined to have a single image, can be used to exploit the passport issuance protocol by deceiving the officer [7]. As the morphed face image generated using two different face images can be used to match both subject's face image, having a morphed face in the eMRTD can then be used by both subjects in various applications that demand the e-passport to be presented. Further, it is also demonstrated that the morphed face images are difficult to be spotted by both commercial face recognition software and also by human experts [18] [14]. These facts have strongly motivated researchers to develop reliable techniques to detect morphed face images.

Figure 1 illustrates an example morphed face image (see Figure1 (b)) generated from two different subjects as illustrated in Figure 1 (a) & (c). It is evident from the Figure 1 that the morphed face image shows the facial characteristics corresponding to both constituent subjects. The critical use-case of such a morphed face image is to obtain an electronic passport by deceiving the passport application officer. Then the submitted photo, printed by the applicant, is further scanned and stored as digital facial reference in the ePassport. Thus, the face morphing attack detection from a print and scanned version of the manipulated face image represents closely the real-life use case to date in most countries.

1.1. Related work

Detection of morphed faces has received a substantial interest from the research community recently resulting in several techniques that can be broadly classified in two main groups: (a) no-reference morphing attack detection techniques and (b) differential morphing attack detection techniques. A no-reference morphing attack detection (MAD) method is analysing a single image and classifying the same as either morphed or bona fide. A differential morphing attack detection technique will use two images at a time to make the decision. The differential MAD method is well suited for the ABC scenario, where the MAD technique can compare the trusted live captured face image (captured in the border gate) with the ePassport reference face image to determine, whether the face image stored in the ePassport is bona fide or morph. Further, the techniques developed in the literature can be divided into two types (a) Digital morph detection: In which both bona fide and morphed face images are and remain in digital form at all times. This represents the use case of visa application or ePassport renewal (e.g. operated New Zealand, Finland and Estonia) in which an applicant can submit a digital photo. (b) Print & scanned morph detection: This will present the typical application of passports in which the applicant will submit his printed photograph to the officer which is then scanned and stored in the ePassport.

Table 1 presents a systematic overview of existing MAD techniques. As noted from the Table 1: (1) the majority of the work in literature is focused on no-reference MAD methods, especially working on the digital image type. To this extent, the first work [15] was focused on exploring the texture based and frequency based features that have indicated a moderate MAD performance. Several morphed face detection techniques based on techniques like JPEG artefact detection, media forensic features (like edge detectors, feature descriptors like SIFT, SURF, BRIEF and FAST) were also introduced which have resulted in very low detection accuracy. A recent work in this direction has explored the features based on Photo Response Non-Uniformity (PRNU) that measures the pixel variation as a result of the camera noise [6]. However, the results reported in [6] have indicated a similar performance to that of BSIF on the same database as indicated in [21]. Further the PRNU-based method suits well, if the camera noise pattern is preserved, which is unfortunately unlikely in the real-life condition with print-scanned morphed face images. We assume that this limits the applicability of the PRNU method for MAD of digital morphed images only. (2) The print-scanned MAD is a challenging problem as the printing and scanning procedure will introduce additional noise and will also mask the pixel discontinuity that might no longer exist due to the morphing process. The existing approaches in this direction are based on texture descriptors and deep learning methods. However, it is demonstrated in [16] that the digital morphed face images are less challenging to detect as compared to print-scanned morphed face images. Recent work in this direction has explored the Steerable texture features that have indicated a better performance to that of transferable deep learning methods. (3) Differential MAD techniques are based on a pair of images (one from the ABC gate and the other from the ePassport) from which properties are observed in order to make a decision. There exist few approaches that are based on texture features, 2D face landmarks and image subtraction (a.k.a. face demorphing). Among these methods, the demorphing technique [8] has indicated a reliable performance. Thus, based on the available literature it is clear that the detection of print-scanned is more challenging but less addressed. This motivated us to address the morphing attack detection in the print-scanned domain.

In this work, we present a novel method for morphed face detection from the print-scanned images. The proposed method is based on extracting the hybrid textures features from multiple colour spaces like HSV and $YCbCr$. It is our assertion that the use of multiple colour spaces will result in the complementary information, which can be further processed to extract vital information that helps to detect morphed faces reliably. Further, the use of the Laplacian pyramid to extract the multi-scale images to quantify the spatial features. Finally, each of the multi-scale images is processed using block-wise Local Binary Patterns (LBP) which is then classified using a Spectral Regression Kernel Discriminant Analysis (SRKDA) classifier to detect the morphed face images. Thus, the following are the main contributions of this work:

- Proposed a new method based on exploring multiple colour spaces to extract multi-scale texture features.
- Extensive experiments are carried out on the largest semi-public database to the best knowledge of authors. The database is comprised of 1270 bona fide face images and 2515 morphed face images.
- Exclusive evaluation of the proposed method is provided with fourteen different state-of-the-art morphing attack detection methods. Among the state-of-the-art methods there are seven different deep learning approaches and seven different non-deep learning approaches. All benchmark results are obtained using the IS0/IEC 30107-3 [10] with BPCER computed at APCER = 5% and 10%.

The rest of the paper is organised as follows: Section 2 presents the proposed method, Section 3 will discuss the experimental results and Section 4 will draw the conclusion.

2. Proposed method

Figure 2 shows the block diagram of the proposed method that extracts the hybrid colour textures to automatically detect the morphed images. The primary objective of the proposed approach is to extract complementary features and subsequently classify the given image as bona fide and morphed face image. To this extent, the proposed method uses multiple colour spaces to extract complementary data from each colour space that are further processed to represent spatial information in multi-scales. The proposed method can be structured in the four steps as discussed below:

Multiple colour space decomposition: The first step of the proposed method is to extract multiple colour spaces. In this work, we have used only two different colour spaces namely HSV and $YCbCr$ by considering the robustness in extracting the complementary features [3]. Given the face image I, we obtain six different colour space images as follows:

$$HSV(I) = [I_H, I_S, I_V] \tag{1}$$

$$YCbCr(I) = [I_Y, I_{Cb}, I_{Cr}] \tag{2}$$

Where the colour space images are $I_{Ci} = \{I_H, I_S, I_V, I_Y, I_{Cb}, I_{Cr}\}, \forall_i = \{1, 2, 3, 4, 5, 6\}$

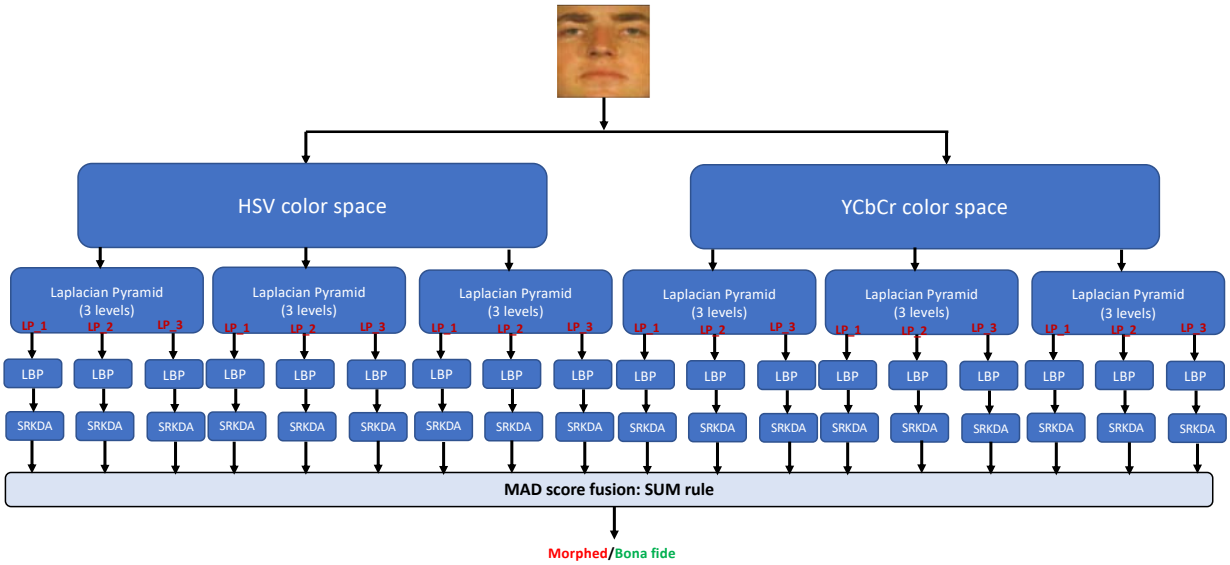


Figure 2: Block diagram of the proposed method

Laplacian scale decomposition: In the second step, we try to extract the spatial information by decomposing the given colour space image I_{Ci} into multiple scales using Laplacian pyramid [4]. Given the colour space image I_{Ci}, the Laplacian pyramid represents the I_{Ci} at different levels l with different scales. Each scale corresponds to multiple frequency bands. The decomposed image in a particular level k is the difference between the Gaussian pyramid image of level k and level $k+1$ which can be defined as:

$$L_k = G_k - upsample(G_{k+1}) \tag{3}$$

In this work, we have used the three-level decomposition of the Laplacian pyramid such that each colour space image C_i is represented by the three sub-images. Since we have six different colour space images and each of them is represented using three level of Laplacian pyramid decomposition, this will result in a total of $6 \times 3 = 18$ sub-images. Let these sub-images be presented as $LP_j = \{LP_1, LP_2, LP_3, \ldots, LP_{18}\}, \forall j = \{1, 2, 3, \ldots, 18\}$.

Figure 3 illustrates the quantitative results of the proposed approach with both colour space images and Laplacian decomposed images that demonstrate the complementary features. Similar observation can be made in the decomposed sub-images.

Texture Features: Local Binary Patterns (LBP) In the next step, we extract the texture features T from each sub-images LP_j using Local Binary Patterns (LBP). In this work, we divided the sub-images LP_j to have image block of size 20×20 pixels with 10 pixel overlapping. The LBP

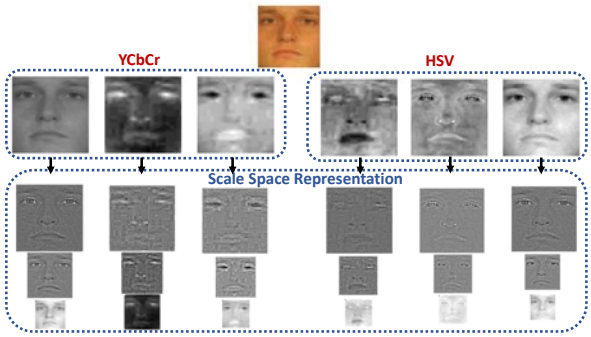


Figure 3: Illustration of colour space and Laplacian decomposition employed in the proposed method

texture patterns are obtained on each block with a gray values of $P = 8$ equally spaced pixels on a circle of radius $R = 1$. Finally, the texture features obtained on each block are represented using a histogram and concatenated to form a single vector. Thus, the LBP representation of each block $b_e, \forall e = 1, 2, \ldots, E$ in a given sub-image LP_j can be represented as:

$$T_b^e = \sum_{P=0}^{P-1} s(g_p - g_c) 2^P \tag{4}$$

Where, g_c corresponds to the gray value of the central pixel of a local neighbourhood, g_p corresponds to the P equally spaced pixels on a circle of Radius R.

Detector: Spectral Regression Kernel Discriminant Analysis (SRKDA) In this work, the detection is carried out using the SRKDA classifier independently on the texture features corresponding to every sub-image $T_b^e, \forall e = 1, 2, \ldots, E$. Let T_{ri} be the training vector such that, $T_r \in \Re^d, r = 1, \ldots, M$, let $K = M \times M$ be the kernel matrix. In this work, we have used the Gaussian RBF as a kernel function. Then the objective function for the KDA can be given as:

$$max_U \quad D(U) = \frac{U^T C_b U}{U^T C_t U} \tag{5}$$

Where, U is the projection function into kernel space, C_b and C_t denote the between class and total scatter matrix. It is shown in [2] that Equation 5 can be written as:

$$max_\alpha D(\alpha) = \frac{\alpha^T K W K \alpha}{\alpha^T K K \alpha} \tag{6}$$

Where, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_{MM}$ is the Eigenvector satisfying $KWK\alpha = \lambda KK\alpha$. W is a block diagonal matrix of labels assigned such that upper block corresponds to the bona fide labels and lower block correspond to the morphed labels. It is also shown in [5] that, KDA project can also be obtained as follows:

$$W\alpha = \Lambda\Phi \tag{7}$$

$$(K + \delta J)\alpha = \Phi \tag{8}$$

Where, Φ is an Eigenvector of W, J is the identity matrix and $\delta > 0$ is a regularization parameter. Eigenvectors Φ can be obtained directly using the Gram-Schmidt method. As $(K+\delta J)$ is positive definite, the Cholesky decomposition is used to solve above equations 7 and 8. Thus, SRKDA only needs to solve a set of regularised regression problems that will results in less computational cost. For the no-reference scenario given the test image T_e, the SRKDA will generate a MAD score corresponding to each sub-image. This will result in 18 different MAD scores for the test image T_e. Finally, we combine these MAD scores using the SUM rule to make the final decision of morphed / bona fide.

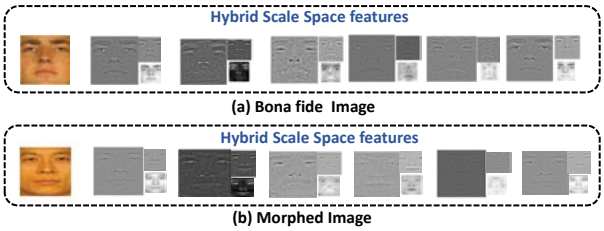


Figure 4: Illustration of the proposed method on (a) Bona fide (b) Morphed face images

Figure 4 illustrates the qualitative results of the proposed features on both bona fide and morphed face images that can indicate the visual differences. These differences may reflect the variations due to the process of morphing. Furthermore, the use of multiple colour spaces also indicates the distinct features across bona fide and morphed faces. This justifies the applicability of the proposed feature extraction method for MAD.

3. Experimental results and discussion

In this section, we present the results of the proposed method on the semi-public database available from [17]. The 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 3791 samples. To the best of our knowledge, this is the largest database containing print and scanned morphed faces available for research purpose. Further, it is also illustrated in [17] that, the image quality of the bona fide and morphed face images in the database is equivalent. This is relevant to avoid that the classification results are purely based on quality differences stemming from compression artefacts.

In this work, we present the quantitative results regarding the MAD accuracy following the IS0/IEC 30107-3 [10] metrics: *Bona fide Presentation Classification Error Rate (BPCER) and Attack Presentation Classification Error Rate (APCER)*. **BPCER** is defined as proportion of bona fide presentations incorrectly classified as attacks while **APCER** is defined as proportion of attack presentations incorrectly classified as bona-fide presentations. In particular, we report the performance of the proposed method by reporting the value of BPCER while fixing the APCER to 5% and 10% according to the recommendation from IS0/IEC 30107-3 [10].

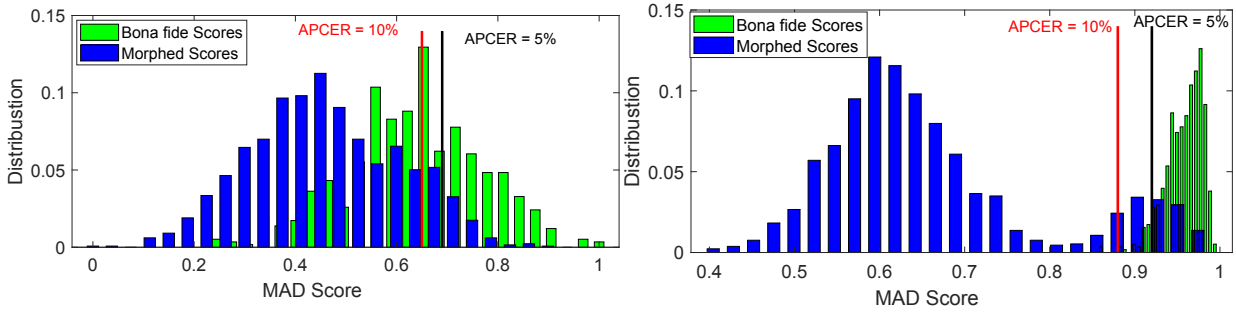
Table 2 indicates the quantitative result of the proposed method together with fourteen different state-of-the-art methods in which seven methods correspond to deep learning methods and the remaining seven different methods correspond to non-deep learning techniques. The following are the important observations from the Table 2:

- In general, the deep learning techniques show better performance when compared with non-deep learning state-of-the-art methods.

- The proposed method has indicated the best performance with BPCER = 0.86% @ APCER = 10% and BPCER = 7.59% at APCER = 5%. The improved performance of the proposed system can be attributed to the texture features extracted from the multi-scale spatial sub-images derived from complementary colour spaces. Further, it is also illustrated in Figure 4 that

Table 2: Quantitative performance of the proposed method

Algorithm Type	Techniques available	BPCER (%) @	
		APCER = 5%	APCER = 10%
Deep Learning Methods	AlexNet [17] [23] [16]	32.76	23.62
	VGG16 [17] [23] [16]	36.38	24.83
	VGG19 [17] [23]	33.62	21.55
	ResNet50 [17]	32.24	20.17
	ResNet101 [17]	30.34	22.59
	Google LeNet [17]	41.38	30.86
	Google Inception V3 [17]	73.97	59.83
Non-Deep Learning Methods	LBP-SVM [20] [14]	89.63	75.14
	LPQ-SVM [20] [14]	94.64	82.13
	IG-SVM [20] [14]	68.08	56.47
	BSIF-SVM [20] [14]	96.29	86.87
	HoG-SVM [20]	88.94	62.69
	Color Textures [14]	80.48	51.64
	Steerable textures [17]	45.76	13.12
	Proposed Method	**7.59**	**0.86**



(a) Image Gradient - SVM

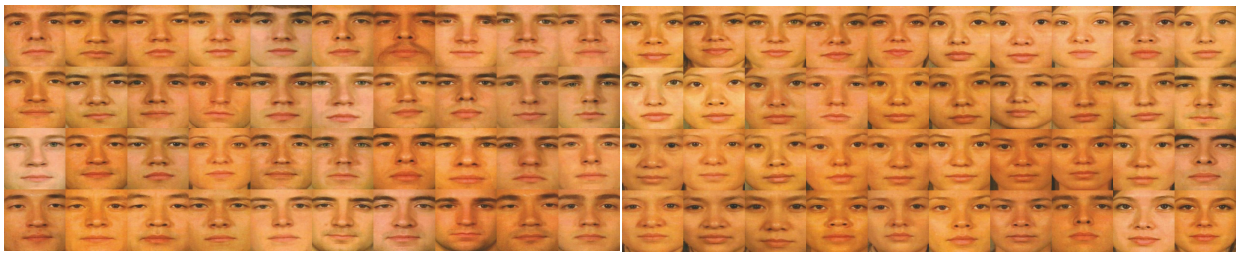
(b) Proposed Method

Figure 5: Distribution of Bona fide and Morphed scores (best viewed in colour)

these features are discriminant for bona fide and morphed face images.

- Figure 5 illustrates the MAD score distribution of the proposed method (See Figure 5b) benchmarked with the image gradient method (See Figure 5a). We have considered the image gradient method as an example as it is a non-texture based method. It can be observed from the score distribution of the proposed method that, the small amount of MAD scores are overlapping with the bona fide scores when compared to that of the image gradient method. Further, Figure 5 also shows the thresholds indicated in the vertical lines at APCER = 10% and 5%.

Thus, based on the obtained results the proposed method has demonstrated the best performance when compared with 14 different state-of-the-art methods on the semi-public print-scanned morphed face images.



(a) Morphed faces: Easy to detect

(b) Morphed faces: Difficult to detect

Figure 6: Example of morphed face images that are easy and difficult to detect using the proposed method

3.1. Analysis of results

In this section, we present an extended analysis of the results obtained using the proposed method, more particularly on analyzing the morphed images that have been printed and scanned. Figure 6 shows example morphed images that are easy (see Figure 6a) and hard (see Figure 6b) to detect using the proposed method. Those morphed face images that are shown as *hard* were misclassified by our method as bona-fide. Following are the main observations:

- It can be stated that it is challenging to detect a morphed face image corresponding to a female subject irrespective of the ethnicity. Careful examination of the source images that are used to generate these morphed face images indicates a possible reason the impact of regular make-up.
- It is also interesting to note that the morphed face images, which are easy to detect, are those corresponding to a male subject. Careful examination of the source images corresponding to these morphed face images reveals a significant difference in shape and geometry between the source images as the potential reason.

4. Conclusion

Reliable detection of morphed face images is of paramount interest to combat recently published attacks on ePassports by deceiving the passport application protocol by submitting a morphed face image. In this paper, we have presented a novel no-reference morphing attack detection technique for face images that have been printed and scanned, to reflect the real-life passport application scenario. The proposed method is based on extracting the texture features from the scale-space representation of multiple colour space of the given image. The proposed approach is based on two different colour spaces (HSV and $YCbCr$) and Laplacian pyramid decomposition with 3 levels to extract the scale-space features from each colour space images followed by texture extraction using LBP. Texture features corresponding to individual sub-bands are further classified using SRKDA to obtain the morphing attack detection scores. Finally, the scores are combined using the SUM rule to make the final decision. Extensive experiments are carried out on the semi-public print-scanned morphed face database with 3791 samples. The proposed method is benchmarked against 14 different state-of-the-art techniques. Obtained results demonstrate the best performance of the proposed method with BPCER = 0.86% at APCER = 10% and BPCER = 7.59% at APCER = 5% compared to existing state-of-art techniques.

Acknowledgment

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

References

[1] A. Asaad and S. Jassim. Topological data analysis for image tampering detection. In *International Workshop on Digital Watermarking*, pages 136–146, 2017.

[2] G. Baudat and F. Anouar. Generalized discriminant analysis using a kernel approach. *Neural Computing*, 12(10):2385–2404, 2000.

[3] Z. Boulkenafet, J. Komulainen, and A. Hadid. Face spoofing detection using colour texture analysis. *IEEE Transactions on Information Forensics and Security*, 11(8):1818–1830, 2016.

[4] P. J. Burt and E. H. Adelson. The laplacian pyramid as a compact image code. *Communications, IEEE Transactions on*, 31(4):532–540, 1983.

[5] D. Cai, X. He, and J. Han. Speed up kernel discriminant analysis. *The VLDB JournalThe International Journal on Very Large Data Bases*, 20(1):21–33, 2011.

[6] L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, and C. Busch. Prnu-based detection of morphed face images. In *2018 International Workshop on Biometrics and Forensics (IWBF)*, pages 1–7, 2018.

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

[8] M. Ferrara, A. Franco, and D. Maltoni. Face demorphing. *IEEE Transactions on Information Forensics and Security*, 13(4):1008–1017, 2018.

[9] 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 *International Workshop on Biometrics and Forensics (IWBF 2017)*, pages 1–6, 2017.

[10] 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.

[11] C. Kraetzer, A. Makrushin, T. Neubert, M. Hildebrandt, and J. Dittmann. Modeling attacks on photo-id documents and applying media forensics for the detection of facial morphing. In *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, IH&MMSec '17, pages 21–32, 2017.

[12] 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*, IH&MMSec '18, pages 49–54, 2018.

[13] A. Makrushin, T. Neubert, and J. Dittmann. Automatic generation and detection of visually faultless facial morphs. In *VISAPP)*, pages 39–50, 2017.

[14] 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)*, pages 555–563, 2017.

[15] R. Raghavendra, K. B. Raja, and C. Busch. Detecting Morphed Face Images. In *8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–8, 2016.

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

[17] R. Raghavendra, S. Venkatesh, K. Raja, and C. Busch. Detecting face morphing attacks with collaborative representation of steerable features. In *IAPR International Conference on Computer Vision & Image Processing (CVIP-2018)*, pages 1–7, 2018.

[18] D. Robertson, R. S. Kramer, and A. M. Burton. Fraudulent id using face morphs: Experiments on human and automatic recognition. *PLoS ONE*, 12(3):1–12, 2017.

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

[20] U. Scherhag, R. Raghavendra, K. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch. On the vulnerability of face recognition systems towards morphed face attack. In *International Workshop on Biometrics and Forensics (IWBF 2017)*, pages 1–6, 2017.

[21] 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)*, pages 187–192, 2018.

[22] C. Seibold, A. Hilsmann, and P. Eisert. Reflection analysis for face morphing attack detection. *arXiv preprint arXiv:1807.02030*, 2018.

[23] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert. Detection of face morphing attacks by deep learning. In C. Kraetzer, Y.-Q. Shi, J. Dittmann, and H. J. Kim, editors, *Digital Forensics and Watermarking*, pages 107–120. Springer International Publishing, 2017.