Noise robust face morphing detection method

Le-Bing Zhang, Juan Cai, Fei Peng, Min Long, Yuanquan Shi

Le-Bing Zhang, Juan Cai, Fei Peng, Min Long, Yuanquan Shi, "Noise robust face morphing detection method," Proc. SPIE 12174, International Conference on Internet of Things and Machine Learning (IoTML 2021), 1217417 (22 April 2022); doi: 10.1117/12.2628711

SPIE.

Event: International Conference on Internet of Things and Machine Learning (IoTML 2021), 2021, Shanghai, China

Noise robust face morphing detection method

Le-Bing Zhang[1], Juan Cai[2], Fei Peng[3], Min Long[4], Yuanquan Shi[1]
[1]College of Computer Science and Engineering, Huaihua University, Huaihua 418000, China
[2]College of Electrical and Information Engineering, Huaihua University, Huaihua 418000, China
[3]College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[4]College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China
E-mail: zhanglebing@hhtc.edu.cn

Abstract

Face morphing attack has become a severe threat to the current face recognition systems. Though there are some methods for detecting face morphing, the performance of these methods is susceptible to noise. Aiming to enhance the performance of resisting noise in face morphing detection, a noise robust convolutional neural network is proposed in this paper. The structure of the network is divided into two parts: facial image adaptive denoising and face morphing detection. Before the face morphing detection, the auto-encoders are first utilized to adaptively denoise the noised facial images, which can effectively reduce the influence of noise on face morphing detection. Then, the pre-trained VGG19 convolution neural network with powerful classification ability is used for face morphing detection with the generated noise-free facial images. Experimental results indicate that the proposed method can effectively reduce the noise influence on face morphing detection, and can achieve better performance compared with some existing methods.

Keywords-Face morphing detection, noise robust, convolutional neural networks

1. Introduction

Face recognition technology has developed rapidly in the past ten years. So, face recognition systems (FRS) are commonly utilized in everyday life, such as Automatic Border Control (ABC) system. These ABCs can easily authenticate someone's identity by his electronic machine-readable travel document (eMRTD) [1]. However, face biometric counterfeits seriously affect the security of FRS. Recently, a novel identity theft scenario [2] was found, in this scenario, FRS can be simply spoofed. The theory of identity theft is: Firstly, a morphed face image is generated, which seems to be many real persons (a criminal and an accomplice). After that, an identity template of FRS is registered by the morphed facial image. Then, the wanted criminal and his accomplice can both match FRS's template, which signifies that a wanted criminal can get an official eMRTD via fusing his own face image with his accomplice. This may lead to the failure of the existing FRS in the ABC system, which will seriously affect the security of the society. Fig.1 shows some samples of morphed face images.

Recently, some research on the security vulnerabilities of commercial FRSs under face morphing attacks has been investigated. A series of face morphing detection methods were proposed in [2, 3, 4,

International Conference on Internet of Things and Machine Learning (IoTML 2021),
edited by Pushpendu Kar, Steven Guan, Proc. of SPIE Vol. 12174, 1217417
 · 0277-786X · doi: 10.1117/12.2628711

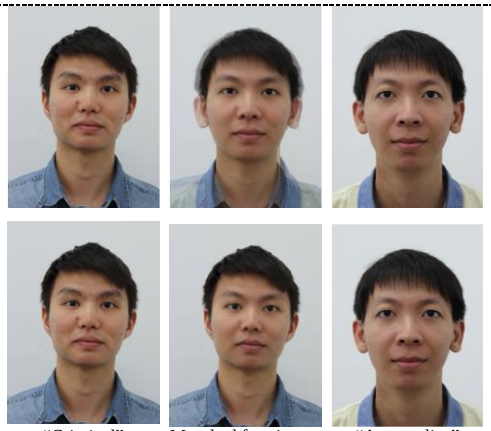

Figure 1. Some samples of morphed face images obtained from two subjects

5, 6, 7, 8, 9, 10]. However, some above-mentioned morphing detection methods ignored the detection stability under noisy conditions. In this manuscript, a noise robust face morphing detection scheme is proposed. It uses end-to-end convolutional neural network structure. The denoised facial images are firstly generated by convolutional auto-encoder network, and then the morphing discriminator network is used to detect face morphing attacks on the generated denoised facial images. The main contributions include:

- A novel deep learning-based noise-robust face morphing detection scheme is presented. As far as we know, this is the first noise-robust face morphing detection method.
- An auto-encoders adaptive denoising network is designed, and it can effectively reduce the noise influence on face morphing detection.
- A large number of experimental results prove the outstanding performance of the proposed method in detecting noised morphed facial images.

2. Related work

2.1. The effectiveness of face morphing attack

Ferrera et al. first investigated face morphing attack [2, 3]. They manually generated some morphed face images and successfully deceived FRS. Later, Andrey et al. proposed to automatically generate vivid facial images [4]. Two types of morphed facial images, which are named as complete morphing image and splicing morphing image, could be automatically obtained through this technique. These automatically generated morphed face images can easily deceive professional human inspectors and commercial FRSs, such as Luxand FaceSDK 6.1.

Lately, the potential ways to forge ID documents were investigated by Robertson et al [6]. They recognized that fraudulent identities via morphing face images are completely possible in practical applications. In addition to the face recognition systems, some other biometric systems (e.g. fingerprint recognition system and iris recognition system) are also vulnerable to face morphing attacks [7]. Furthermore, some metrics are proposed to evaluate the security of biometric systems under face spoofing attacks in [8, 9]. Moreover, Wandzik et al. studied the vulnerability of FRS based on deep learning to face morphing attacks [10]. It is proved that face morphing attacks can also deceive these FRSs, which seriously degrade the detection accuracy of the deep learning-based FRS.

2.2. The research on face morphing detection

The current face morphing detection algorithms can be classified to two types: blind detection and non-blind detection algorithms, which depend on whether auxiliary images are used or not.

1) Blind face morphing detection methods

Raghavendra et al. proposed the first automatic face morphing detection method [5]. It utilized binarized statistical image features (BSIF) to express the image texture difference between the morphing and real face image. Furthermore, since

the face morphing image is commonly restored in the JPEG style, image quality and JPEG artifacts will occur. Therefore, Andrey et al. [4] and Hildebrandt et al. [11] respectively presented a face morphing detection algorithm according to image quality features. The morphed face image is detected by the Benford feature, which is extracted from the quantized DCT coefficients. Kraetzer et al. [12] used eight point/edge operators to measure the image degradation effect after a facial morphing process. Similarly, T. Neubert [13] proposed a face morphing detection algorithm, which utilized the continuous degradation of JPEG images.

Raghavendra et al. proposed a deep convolutional neural network to classify digital morphed face images and print-scanned morphed face images [14]. Nowadays, a deep learning-based morphed face detection scheme was proposed by C. Seibold et al. [15]. In this scheme, some typical network architectures are researched and proved that the pre-trained VGG19 network [16] could get better performance than two other networks.

Inspired by the thought of camera model identification [17, 18], we presented a face morphing detection algorithm according to the statistical quantization feature of sensor pattern noise (SPN) [19]. Meanwhile, L. Debiasi et al. [20] used statistical characteristics of SPN spectrum histogram for face morphing detection.

2) Non-blind face morphing detection methods

Ferrara et al. used auxiliary images gotten from the FRSs and the face morphing image showed in biometric passport and presented an algorithm to reconstruct the facial image of morphing attacker's accomplice via inverting the morphing process [21]. Recently, we proposed an FD-GAN to restore facial images of morphing accomplices [22], which can restore the facial images of face morphing accomplices with good quality.

Based on the above analysis, it can be found that face morphing detection is a significant problem in biometric security. There remain many problems to be solved. Among them, how to improve the face morphing detection method to resist noise interference in real applications is very important. To this end, a noise-robust deep learning-based face morphing detection scheme is presented in this paper.

3. The proposed method

Differ from the above face morphing detection algorithms, our presented method aims to suppress the impact of noise on face morphing detection. First, adaptively denoise the noisy facial images, and then perform face morphing detection on the denoised face images. Fig. 2 shows the architecture of the presented method. It contains two parts: an adaptive denoising network and a morphing discriminator network. The details are described as follow.

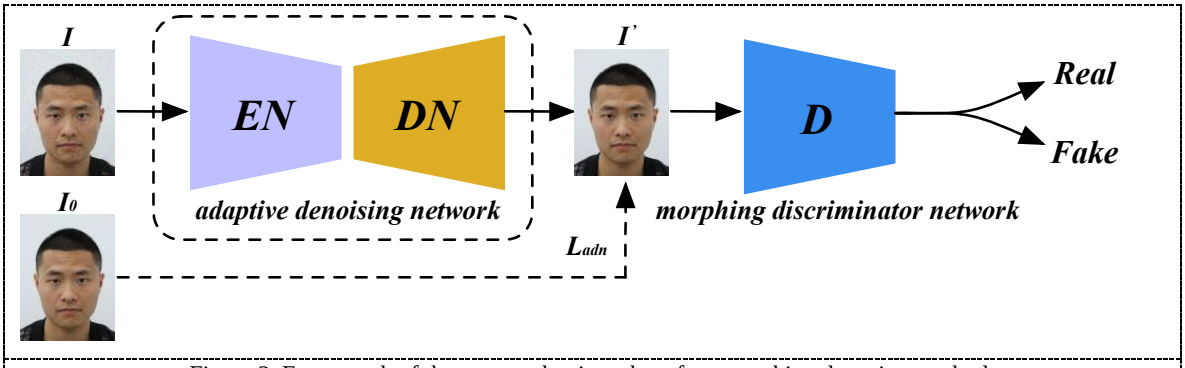

Figure 2. Framework of the proposed noise robust face morphing detection method.

3.1. The adaptive denoising network

It can be seen from Fig. 2, the proposed noise robust face morphing detection framework contains an adaptive denoising network. It is illuminated by the denoising auto-encoder, which is a noise robust unsupervised learning technique. The adaptive denoising network contains two parts: encoder network

Table 1. The detail of the encoder network (*EN*).

Group Name	Configuration (filter/stride)
Conv1	3×3/1 Conv@64 + BN + ReLU
Conv2	3×3/2 Conv@128 + BN + ReLU
Conv3	3×3/2 Conv@256 + BN + ReLU
Conv4	3×3/2 Conv@512 + BN + ReLU

Table 2. The detail of the decoder network *DN*.

Group Name	Configuration (filter/stride)
Upconv1	Upsampling + 3×3/1 Conv@256 + BN + ReLU
Upconv2	Upsampling + 3×3/1 Conv@128 + BN + ReLU
Upconv3	Upsampling + 3×3/1 Conv@64 + BN + ReLU
Upconv4	3×3/1 Conv@3 + Tanh

EN and decoder network *DN*. The structures of the encoder network *EN* and decoder network *DN* are respectively listed in Table 1 and Table 2.

Given a noised facial image *I*, the *EN* is utilized to capture the identity feature of *I*, and the decoder network is used to generate a noise-free facial image *I'*. In order to effectively suppress the noise in *I*, an auxiliary image (without noise) I_0 of *I* is given during the training stage. So as to make the generated noise-free facial image be as close as possible to the auxiliary image I_0. Here, L_1 loss is utilized, and the loss of adaptive denoising network L_{adn} is defined as

$$L_{adn} = \|I' - I_0\|_1. \tag{1}$$

3.2. Morphing discriminator network

With the generated noise-free facial image after adaptive denoising network, morphing discriminator network is used for detecting morphed face image. Here the VGG19 [16] with a good classification effect is selected. Although the network architecture of VGG19 is simple, it has achieved great success in the field of image recognition. The convolutional layer uniformly uses a 3×3 kernel, which has a predecessor layer and a successor layer. We only transform the output of the network to a 1×2 size vector on the last fully connected layer to distinguish that the image is a real image or a morphed face image. The loss of morphing discriminator network L_{mdn} is defined as

$$L_{mdn} = -\sum_j t_{i,j} \log(p_{i,j}), \tag{2}$$

where p_{ij} and t_{ij} represent the prediction and target of data *i* with class *j*, respectively.

4. Experiments and analysis

4.1. Database and evaluation criteria

As far as we know, there is no publicly available face morphing database, a noised facial morphing database is first built. To ensure the disjoint nature, we separately generated a large numbers of morphed facial images in three subsets: training set, development set, and testing set. On every subset, we follow the workflow proposed in [4] to automatically generate two types of morphed facial images (complete morphing images and splicing morphing images). For generating noised face images, two kinds of noise (0.01 density salt-and-pepper noise and 0.01 standard deviation Gaussian noise) are considered. A total of 4,502 noised bona fide, 3,432 noised complete morphing face images, and 3,656 noised splicing morphing face images are selected in the database. Table 3 shows the details of the noised face morphing database.

In the following experiments, two standardized ISO/IEC metrics, bona fide presentation classification error rate (BPCER) and attack presentation classification error rate (APCER), are selected to evaluate the detection performance [23]. The average classification error rate (ACER) is selected to measure the overall detection performance in the testing set.

Table 3. The summary of noised face morphing database on each type of noise.

Image size	Subset	#Subject (Male, Female)	#Bona fide	#Complete morphing	#Splicing morphing
360 × 480	Training set	50(30,20)	1121	1121	1121
	Development set	25(15,10)	564	299	330
	Testing set	25(15,10)	566	296	377

4.2. Reliability comparison with different types of noise

The presented scheme is compared with some current typical face morphing detection methods, such as texture feature-based method [5], JPEG compression feature-based methods [12, 13], SPN based methods [19, 20], and deep learning-based method [15]. Experimental results prove our method's good performance.

The performance comparison of these face morphing detection methods with two types of noises are shown in Table 4 and Table 5. We can realize that the proposed scheme can obtain better ACER than that of other methods in two types of noise. In different noise interferences (Gaussian noise and salt-and-pepper noise) and different morphing methods (complete morphing and splicing morphing), the ACER of the proposed scheme is generally 50% lower than other methods. For example, in Gaussian noise, splicing morphing, the ACER of the proposed method is 11.08%. It reduces the error rate of the second-best result of the method [15] by 53.52%.

Table 4. Performance comparison of different detection methods with Gaussian noise interference (%)

Feature	Complete morphing			Splicing morphing			All types of morphing		
	APCER	BPCER	ACER	APCER	BPCER	ACER	APCER	BPCER	ACER
BSIF [5]	4.05	13.07	8.56	50.66	28.09	39.37	34.32	**14.84**	24.58
Kraetzer et al. [12]	32.43	18.55	25.49	35.27	16.96	26.11	72.51	19.61	46.06
T. Neubert [13]	41.55	21.02	31.28	43.23	24.02	33.63	40.71	24.38	32.54
C.Seibold et al. [15]	0.99	13.97	7.48	15.84	31.83	23.84	21.58	20.51	21.05
L.B Zhang et al. [19]	41.89	7.42	24.65	49.86	30.38	40.12	51.56	18.37	34.96
L. Debiasi et al. [20]	34.12	**2.82**	18.47	52.25	41.87	47.06	16.49	31.09	23.79
Proposed	**0.34**	6.89	**3.61**	**8.75**	**13.40**	**11.08**	**4.42**	17.19	**10.81**

Table 5. Performance comparison of different detection methods with salt-and-pepper noise interference (%)

Feature	Complete morphing			Splicing morphing			All types of morphing		
	APCER	BPCER	ACER	APCER	BPCER	ACER	APCER	BPCER	ACER
BSIF [5]	5.06	18.19	11.63	37.93	15.54	26.73	21.09	20.84	20.97
Kraetzer et al. [12]	35.13	10.42	22.77	43.50	**8.65**	26.07	47.10	9.01	28.05
T. Neubert [13]	57.77	8.48	33.12	53.84	11.30	32.57	58.54	10.77	34.66
C.Seibold et al. [15]	1.94	12.97	7.45	25.58	38.92	32.25	24.93	19.97	22.45
L.B Zhang et al. [19]	**1.68**	22.61	12.15	15.64	28.97	22.31	6.53	36.21	21.37
L. Debiasi et al. [20]	40.87	29.50	35.19	46.41	30.56	38.49	44.72	30.38	37.55
Proposed	**1.68**	**5.64**	**3.66**	**2.91**	8.66	**5.78**	**3.54**	**8.42**	**5.98**

The detection error trade-off (DET) curves of different face morphing detection methods with two types of noise are shown in Fig. 3 and Fig. 4. Here, only all types of morphing is considered, the DET curves also show that our presented method could achieve the best detection performance.

From the experimental results, we could know that the presented scheme can remarkably reduce the impact of Gaussian noise and salt-and-pepper noise on face morphing detection.

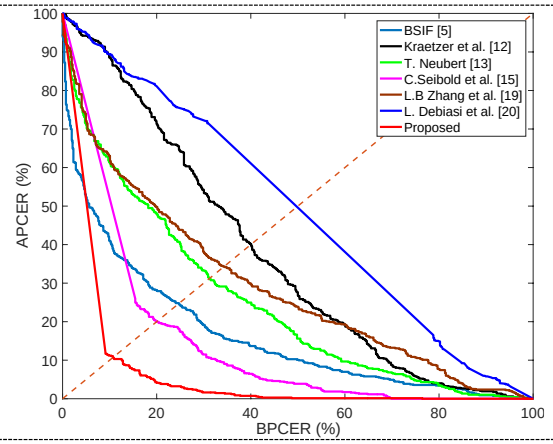

Figure 3. DET curves of different methods with Gaussian noise.

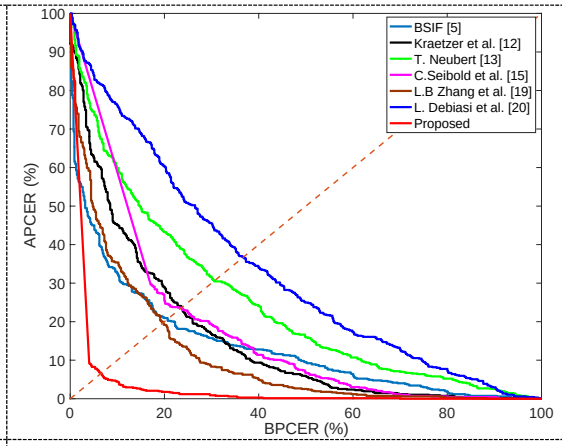

Figure 4. DET curves of different methods with salt-and-pepper noise.

5. Conclusion

We present a novel noise-robust face morphing detection method in this manuscript. It used an end-to-end convolutional neural network structure, which is composed of an adaptive denoising network and a morphing discriminator network. It can effectively suppress the impact of noise on face morphing detection. Experimental results show that compared with other current methods better performance can be achieved in the presented scheme. It illustrates that the proposed face morphing detection scheme is robust to noise. Our future work will be focused on more sophisticated adaptive denoising network structures to withstand more types of noise, and further study the face morphing detection of noisy printed/scanned facial images.

Acknowledgements

This research was supported by National Natural Science Foundation of China under grant nos. 62072055 and U1936115. It was also supported by Scientific Research Foundation of Hunan Provincial Education Department under grant nos. 20K098 and 19C1468, and co-funded by Key Laboratory of Intelligent Control Technology for Wuling-Mountain Ecological Agriculture under grant no. ZNKZN2019.

References

[1] Organization ICA 2006 Machine readable travel documents-part 9: Deployment of biometric identification and electronic storage of data in emrtds Tech. rep.
[2] Ferrara M, Franco A and Maltoni D 2014 The magic passport *IEEE International Joint Conference on Biometrics (IJCB)* pp 1–7
[3] Ferrara Matteo F A and Maltoni D 2016 *On the effects of image alterations on face recognition accuracy* pp 195–222
[4] Andrey Makrushin T N and Dittmann J 2017 Automatic generation and detection of visually faultless facial morphs *International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP)* pp 39–50
[5] Raghavendra R, Raja K B and Busch C 2016 Detecting morphed face images *IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS)* pp 1–7
[6] Robertson D J, Kramer R S S and Burton A M 2017 *PLOS ONE* **12** 1–12
[7] Gomez-Barrero M, Rathgeb C, Scherhag U and Busch C 2017 Is your biometric system robust to morphing attacks? *International Workshop on Biometrics and Forensics (IWBF)* pp 1–6
[8] Scherhag U, Raghavendra R, Raja K B, Gomez-Barrero M, Rathgeb C and Busch C 2017 On the vulnerability

of face recognition systems towards morphed face attacks *International Workshop on Biometrics and Forensics (IWBF)* pp 1–6
[9] Scherhag U, Nautsch A, Rathgeb C, Gomez-Barrero M, Veldhuis R N J, Spreeuwers L, Schils M, Maltoni D, Grother P, Marcel S, Breithaupt R, Ramachandra R and Busch C 2017 Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting *International Conference of the Biometrics Special Interest Group (BIOSIG)* pp 1–7
[10] Wandzik Lukasz G R V K G and Chen X 2017 Cnns under attack: On the vulnerability of deep neural networks based face recognition to image morphing *International Workshop on Digital Forensics and Watermarking (IWDW)* pp 121–135
[11] Hildebrandt M, Neubert T, Makrushin A and Dittmann J 2017 Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps *International Workshop on Biometrics and Forensics (IWBF)* pp 1–6
[12] Kraetzer C, Makrushin A, Neubert T, Hildebrandt M and Dittmann J 2017 Modeling attacks on photo-id documents and applying media forensics for the detection of facial morphing *ACM Workshop on Information Hiding and Multimedia Security* pp 21–32
[13] Neubert T 2017 Face morphing detection: An approach based on image degradation analysis *International Workshop on Digital Forensics and Watermarking (IWDW)* pp 93–106
[14] Raghavendra R, Raja K B, Venkatesh S and Busch C 2017 Transferable deep-cnn features for detecting digital and print-scanned morphed face images I*EEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* pp 1822–1830
[15] Clemens Seibold Wojciech Samek A H and Eisert P 2017 Detection of face morphing attacks by deep learning *International Workshop on Digital Forensics and Watermarking (IWDW)* pp 107–120
[16] Simonyan K and Zisserman A 2014 URL http://arxiv.org/abs/1409.1556
[17] Zhang L B, Peng F and Long M 2017 *Journal of Visual Communication and Image Representation* **48** 471–479
[18] Peng F, Zhou D L, Long M and Sun X M 2017 *AEU-International Journal of Electronics and Communications* **71** 72–81
[19] Zhang L, Peng F and Long M 2018 Face morphing detection using fourier spectrum of sensor pattern noise *IEEE International Conference on Multimedia and Expo (ICME)* pp 1–6
[20] Debiasi L, Scherhag U, Rathgeb C, Uhl A and Busch C 2018 Prnu-based detection of morphed face images *International Workshop on Biometrics and Forensics (IWBF)* pp 1–7
[21] Ferrara M, Franco A and Maltoni D 2018 *IEEE Transactions on Information Forensics and Security (TIFS)* **13** 1008–1017
[22] Peng F, Zhang L B and Long M 2019 *IEEE Access* **7** 75122–75131
[23] 2017 Information technology-biometric presentation attack detection-part 3: Testing and reporting Tech. rep.