A Novel Framework for Detection of Morphed Images using Deep Learning Techniques

Mohammed Ehsan Ur Rahman[1]
CSE Student, , Kakatiya Institute of Technology and Science, Warangal, 506015, Telangana, INDIA
ehsan81181@gmail.com

Md. Sharfuddin Waseem[2]
Department of Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal, 506015, Telangana, INDIA waseem7602@gmail.com

Abstract. The paper deals with the break-ins that the modern-day biometric verification systems like Automatic Border Control, facial unlocking scheme as in many smartphones, and other photo-ID documents generation and verification systems face. One of the most prominent attacks is the facial morphing attack, wherein the system is fooled by asking it to do facial recognition and matching of a person with a photo which is morphed and has features of two persons overlapped .The proposed framework gives a deep insight into the concept of image morphing and the way to analyze the features and allocate them priorities .The system tries to integrate all the features of image that could possibly have an influence on the face image if morphed with another face image .The paper also presents an account of the advantages and disadvantages as well as the intuition of various approaches of face image morphing detection ,especially we take into account the deep learning models that have been used previously and try to tune in the parameters and analyze their complexity in order to try various methods to reduce the overfitting of such models.

Keywords: ABC-Automatic Border Control, eMRTD-electronic Machine Readable, GIMP- GNU Image Manipulation Program v2.8, GAP- GIMP Animation Package, COTS- commercial off-the-shelf, ePassport, IQA-Image Quality Analysis.

1 Introduction

Face recognition systems gather information of image like facial landmarks , contours and edges around eyes , nose , eyebrows , chin , etc. But these features are prone to mutation and hence getting more detailed information of a face image is required which can be done by analysis and extraction of all features of a face image.

In contemporary scenario, morphing has become a big cause of unreliability on the face recognition systems. The problems concerning face recognition systems have a great deal of influence on the security and privacy services, authentication problems , computer forensics and media forensics .

The redesigning of the authentication systems that rely on biometrics is an urgent concern . The explosion of images on the internet has paved way for many new types of attacks and generation of variations of the images .

Under the general circumstances, it becomes easier with certain combinations of algorithms and systems along with some fine-tuning to detect facially morphed images.

The automatic generation and detection of visually faultless facial morphs motivated us to use the concept of visually faultless facial morphs[40]. Generation of facial morphs is crucial and serves as an essential part of the performance evaluation of morph detector. The contemporary auto face recognition systems are poor in measuring the dissimilarity between a visually faultless morphed face image and a genuine face image which raises concerns with regards to its ability to authenticate people.

As computer vision is all about the construction of explicit and meaningful descriptions of all physical objects from images, morphing which is also known as metamorphosis[20] be a mixture of techniques and hence dealing with mapping functions which are applicable on image segments shall be dealt in a reverse fashion.

The seamless stitching done during morphing poses a great challenge in designing algorithms that can differentiate between original and morphed images. This can be overcome by the use of the general template established by deep learning-based algorithm[5] namely the autoencoder; which is generated during learning from the face databases. These methods indeed analyze the specific artifacts of an image present in its image statistics; though this doesn't ensure that all morphed images have their camera-specific fingerprint completely deleted and that the image was really morphed ,the only solution for this is that the document generation must be done with an onsite image of the candidate and appropriate measures must be taken to block any kind of interference to the document generation system by any traffic on Internet.

2 Related Work and Study

A face recognition system predicts classes and detects faces using all the available features of an image , by passing the image through the series of modules like face detection , feature extraction , comparison etc. We have included in our proposed system other modules which are the comparisons of the face image with a well-defined and generic human face template build using Deep Learning by training it through many face images from a variety of face databases.

[32] presents the new and unique approach of detection of face morphing

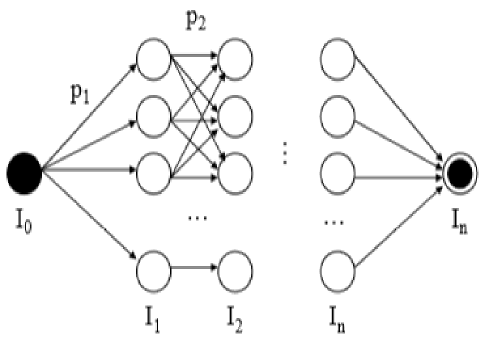
through analysis of illumination of the morphed face image , the only limitation being that this approach is that it inherently deals with the light environment of the image and hence can be easily manipulated if required.

The basic motivation behind the proposed system is [38].image editing history model proposed by them gives a great insight into how to analyse the features and deciding which features to use .

Auto-detection of facial morphing is manifested in [30] using the Benford features , a derivative of the quantized values of the DCT coefficients but the limitation is its applicability to only JPEG type face images .

Extraction of micro-textures[3] using binarized statistical image features help saving space and memory; runs faster and reduces the complexity of the feature vector thereby avoiding the chances of random noise being fed into our image editing history model. Special care is taken to deal with noise; even though we have used deep learning-based methods which tend to overfit easily. There is a dire need of extensive and all-inclusive experimental analysis of such systems so that there are least chances of errors in huge and important systems such as the automated border control.

The knowledge of editing history makes the analysis of the images easy by giving us the access to the artifacts that can reveal the sequence of editing operations.



[Figure 2, the image editing history model taken from [38]]

Image-editing history model [38], even though doesn't assure morphing of a face image , but this approach paves a better way to this problem , because it gives us the first-hand detailed report and description of the attack in detail . These details are with regards to the image statistics which are prone to mutation during capture , face alignment , warping and blending , etc . [36] model makes a systematic and fine-grain description of attack realizations and traces of image anomalies resulting from the editing operations feasible .

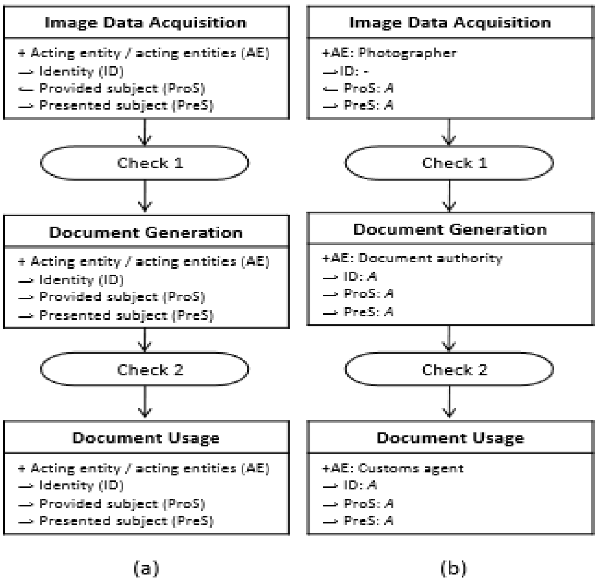
Image editing history plays an important role in analysing and finding out dependent features and terms of their manipulations. Features of a morphed image generally lack a lot of facial details and hence will cause unusual values to pop up in the feature vector during its extraction using various methods .

Their results show that the most prominent effect comes from the common and basic operations of blending and warping . [5]

Search for an optimal classifier can end only if we have the knowledge of the interlinking of specific features that are performing well are supported by the certain classification algorithm. Selection of this stage of system framework is crucial because it is the one that does the integral task of comparison/analysis of images and evaluation of the whole system's results. it's a known fact that a classifiers relation with the features it's operating with is crucial and still remains an active area of research. Following the traditional fraud detection system framework, we tend to use SVM and weigh it more than Decision trees.

A. The magic passport – a detailed description of facial morphing attack

We were inspired through-out our research work by [4] by Ferrara et al., because it serves as a great identity theft scenario. The paper elaborates upon the loop-holes in the current system and a general overview of the image morphing methods .



[Figure 3 ,depicting the generalized life-cycle of a photo-ID document along with a standard use-case without attack taken from the [38] ID stands for the identity assigned to a document/person, ProS stands for the set of subjects (only one subject if no attack two or more if morphing attack took place) PreS stands for presented subject(either of the two persons whose face images have been morphed and submitted for photo-ID document generation)]

The problem with issuance process of an ePassport is that morphed images can get into such systems[6] easily and hence making the relationship between individuals and their biometric reference data weak and unreliable .this can lead to big havoc in the ICAO and ABC like systems .
Simple spoofing attacks include [41][42]

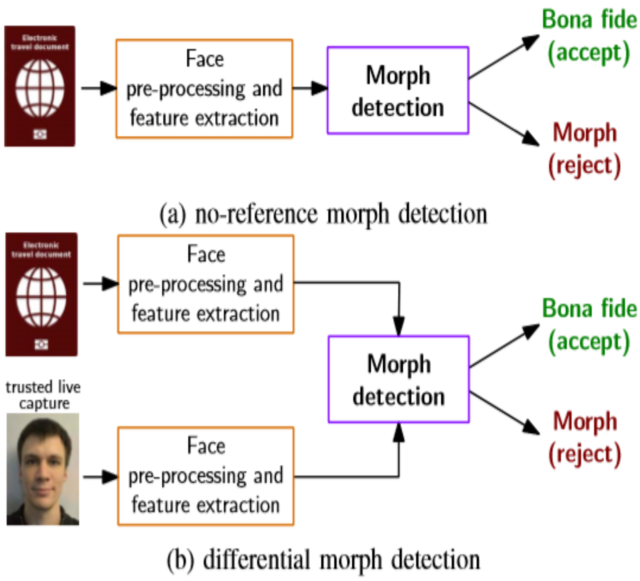
3 Proposed System Framework and Methodology

To the best of our knowledge right now no extensive research study can accurately describe such models and the various types of problems faced by the facial morphing attacks and there is no systematic and generalized strategy that can address this threat.Detecting the type of morphing algorithms applied to an image by and large assists in deciding whether an image is morphed or not, because different morphing methods will give different inconsistencies in an image pixel.

Here we have proposed a system keeping in mind the various possible image and face features and the influence they could probably have on the image morphing detection system's performance. These are none but the general high and low-level image statistics that are around since the dawn of fields of image processing and computer vision. The only difference comes when we approach them in a different way, perception and intuition and with subtle differences and fine-tuning the system becomes a state of art for face image morphing detection. We have classified the methods into two broad categories so that their contexts are clear and distinct in the mind of the reader.

In general, we can detect a face image morphing attempts in the two below mentioned scenarios [43]: -

1. When we have the reference images i.e. the original images; this is a deferential morphing detector.
2. When we don't have a reference image i.e. single image- similar applies to the fraud detection for the electronic travel photo-ID based documents like ePassports, etc.



[Figure 3, depicting the two approaches to detection of facial morphing extracted from [43]]

Automatic facial morphing detection algorithms based on the simple, yet robust features of a face image include: -

1. Sobel/Canny edge detection;
2. Using the Haar wavelet transform and then apply Benford features [30];
3. Squeeze and excitation of lower ranges and semantic segmentation;
4. The best machine learning classifier for visual recognition for classification and deep learning purpose are those techniques which are best suited for ImageNet classification. These can include deep convolutional neural networks with lower learning rates and those which start at a better place in the hyper-plane using the stochastic gradient descent, a variation of the gradient descent algorithm; if a reference is provided then the framework shall ignore the pre-existing template, and if no reference is provided then the comparison is done between input image and face template.
5. Reinforcement learning which will help the feedback mechanism;
6. Facial landmark with more detailed specifications;
7. CNN's for visual recognition with hyperparameter tuning [22];
8. ReLU for the non-linearity activation functions [25];
9. Residual learning [27];
10. Obtaining a face template using CNN[19] technique;
11. SVM classifier trained using the inputs as training instances and outputs as their labels of the CNN technique;(ML algorithm that perform well on data with outliers (here, facial morphs))

A. Use of algorithms which work on low-level features of a face image

Auto-detection of facial morphing can be manifested using the Benford features[30] , a derivative of the quantized values of the DCT coefficients but limitations with Benford methods application being its inapplicable to image data with range limits(range implies resolutions and other features of an image) and with categorical image data.

The extraction of image statistics in order to derive the image editing history of a face image .This leads us to know that the reduction of facial information or the so-called image statistics can be mapped back to predict the type of operations that were possibly implemented on the face image.

The key point extraction is done using the AGAST (Adaptive and Generic Accelerated Segment Test) features without any variations or modifications.

Classification results are supposed to vary because of the pre-processing and post-processing schemes applied to various images such as the median filtering[17] , anti-forensic[34] techniques like unsharp masking, etc.

B. Algorithms involving Deep Learning-based methods

Creation of a facial template is of prime importance and is done here using the CNN's . CNN's are really good at learning the low and as well as high-level features of images . But the desired product is to have an image template which learns from new images fed into it all the time , don't overfit but regularise well . The end to the search of such an algorithm requires deep analysis of all the deep learning methods .The dimensionality of modern-day face images being very high , forced us to use the very subtle yet powerful tool of machine learning toolbox ;the SVM as its implements various ways to do dimensionality reduction of the data thereby increasing the performance and making this algorithm faster when compared with decision tree and K-nearest neighbours. As the prediction classes here are only two i.e. whether the image is original or a morphed one ,we use a binary SVM classifier.Applying this system with an inbuilt feedback mechanism will make it more practical and robust and this type of learning will go side by side with the CNNs and compliments the deep learning approach as it follows the similar lines.

Transfer learning model using AlexNet, GoogleNet and VGGNet is an easier approach[26] to solve this visual recognition problem but the drawback of such model is that the network of layers formed was not built for the specific task of facial morphing detection and hence creating a network of layers from scratch keeping in mind those activation functions that tend to perform extraordinarily on such tasks is necessary.

C. Features Analysis

Image quality analysis (IQA) can be done using LBP, LPQ, 2-DFFT.The features mentioned below are being considered in this framework. These features include those that are analyzed using image processing techniques and computer vision algorithms.Texture descriptors :- Image processing algorithms giving information regarding the texture i.e. the measure of similarity between adjacent image segments .

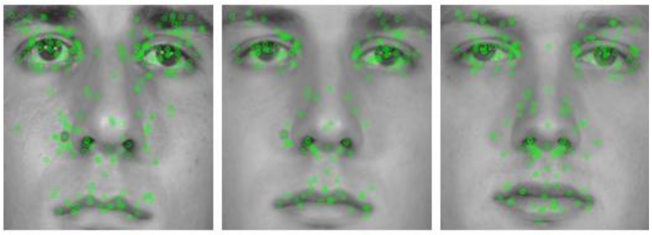
1. LBP(Local Binary Patterns) – Pattern which accounts for the texture of the image calculated for every image pixel utilizing information of all of its neighbours . The number of neighbours depends on the size of the sliding window used in its implementation It acts as a local feature descriptor.[8]
2. BSIF(Binarized Statistical Image Features):- These are the features of JPEG type of images , calculated by quantizing the DCT(Discrete Cosine Transform) coefficients into some arbitrarily selected number of bins. [1][30]

Key point descriptors:-

1. SIFT (Scale Invariant Feature Transform):- It's a very useful image

processing tool to access the local features of a face image .There prominent role in applications like image stitching motivates us to use it for face image morphing detection.[39]

2. SURF(Speed Up Robust Feature)[9]:- A local feature descriptor , similar to SIFT but much faster. It extracts output of the operations like Haar wavelet and Hessian blob detection algorithms . [39]



(a) Subject 1 (b) Morph (c) Subject 2

[Figure 4, showing the SURF keypoint detection taken from the paper [37]]

Deep facial features :-

1. One of the most prominent computer vision cues are the corners of an image , especially of face images . These qualifiers tend to give detailed structural landscape of a face and are the basis on which many other algorithms of facial recognition work upon.

Edge and corner detectors:-

1. FAST (Features from Accelerated Segment Test)
2. AGAST (Adaptive and Generic Accelerated Segment Test)

Gradient estimators:-

1. HOG(Histogram of Gradients):- This estimator enumerates the number of occurrences of the gradients/orientations of every pixel element within its local neighbourhood .[29]

Interpolation and other image statistics analysis :-

1. Interpolation[38]
2. Blob detection methods are aimed at detecting regions in a digital image that differ in properties, such as brightness or colour, compared to surrounding regions.

3. Interest point detection is a very recently added terminology in computer vision and image processing that is detection of interest points for further processing. Interest points can be defined as pixels or points in an image that are mathematically discrete , stable , having well-defined positions and rich in terms of local information contents.

All of the aforestated feature descriptors if applied before processing of the face image can have a great impact on the classification results .

D. Mathematical models and Intuitions

Autoencoder approach also helps in forming a great template without applying of any form of constraints . Eigenvalues and eigenvectors applied on problems arising from the Markov processes which are stochastic in nature . This approach is very innovative and involves simple operations involving matrices which all face images inherently are.[24][44]

Let D be a linear differential operator on the space C∞ of infinitely differentiable real functions of a real argument t. The eigenvalue equation for D is the differential equation 1.

$$Df(t) = \lambda f(t) \quad \ldots..(1)$$

Reflection analysis [32] method assisted with the orthogonal transformation which is of immense use in problems involving rotation and/or reflections of face images without causing much distortion to the length or changing the norm of any vector or matrix(image).Reflection approach can also be complimented if we analyse the image not in its original colour space i.e. RGB but in another colour space like the HSV. Image information or entropy is also an area to analyse . [33] belief propagation method uses the intuition that image entropy distributed in a way that's unusual to observe in human face images can be proven helpful in detecting face image morphing.Creating a probabilistic distribution curve based on the learning outcomes of the networks will serve as a naïve classifier for new images though this is not what we are in search of.

In binary classification, where the number of classes equals 2, cross-entropy or the logarithmic loss function can be calculated as:

$$-(y log(p) + (1 - y) log(1 - p)) \quad \ldots..(2)$$

where y is binary indicator (0 or 1) and p is the predicted probability

Basic intuition for applying probabilistic models in CNNs is that the problem is inherently a stochastic one and not a deterministic one , hence approach of optimization will work only when we have an objective function which works well for stochastic problems.[23]

Hence the objective functions we choose here are: activation function ReLU(leaky) and logarithmic loss also called as the binary crossentropy as the loss function is the best according to our research work till date .

Instead of the function being zero when x < 0(the "dying ReLU" problem), a leaky ReLU will instead have a small negative slope, for example 0.01. This function can be computed using the equation :-

$$f(x) = 1(x < 0)(\alpha x) + 1(x >= 0)(x) \text{ …..(3)}$$

where α is a small constant

E. Deep Learning as a modern day efficient tool in the context of visual recognition

More detailed account of deep learning on and its advantages over other traditional feature-based face image morphing detection techniques [18][22][23][25][27][28] is given here.

4 Datasets and Facial Morphing Generation

Here we give a detailed account of the different morphing techniques used extensively.

A. Facial morphing techniques and pipeline

The basis for any sort of image manipulation or morphing technique is recognising the feature space of the system and then combining the features that belong to that space .[29]

List of operations performed

1)Cropping: -

The image processing operation that resizes an image by modifying the number of row and columns or resolution of the image, to make the two images of comparable size so as to assist in an overlapping of them.

2)Scaling: -

Scaling is the technique in computer graphics means to resize[16] an image from lower resolution to higher resolution also known as upscaling or resolution enhancement. This can be done using geometric transformations and no loss of image quality.

3)Downsampling: -

The computer vision method used to resize an image by shrinking it to reduced size by throwing away image information.

4)White-balance adjustment: -

This technique allows a photographer to capture images in any sort of illumination conditions, it adjusts the color balance (global adjustment of the intensities of the colors) of light by analyzing the colors in the image and neutralizing them automatically.

5)ICC color management transformation: -

Mapping the pixels of an image from one color space to another color space, for example from RGB to CMYK.

These are well-defined transformations using white points as references in both color spaces.

6)Compression: -

Type of data compression performed on images, to lower irrelevance and redundancy of image data. There are two types of compression techniques generally in use 1) Lossy and 2) Lossless

7)Color Filter Array (CFA): -

Application of CFAs is of prime importance in dealing with images captured by photosensors as they lack the ability to detect light intensities with little or no wavelength specificity and hence unable to separate color information.

Some common filter algorithms include RGBW and CYGM
CFAs.

8)Interpolation patterns: -

These image processing methods are used to lower the distortions due to zooming, done by discarding the fractional part of pixel values' addresses of neighboring pixels but rather copying the pixel brightness value at the resulting integral address in the source image to the zoomed image. Physical deformations .[12]

9)Splicing: -

Cutting a section of the image and pasting it into the same image. Generally applied to bring in symmetry to multiple objects of same sizes not present in the original image.

Face morphing step by step: -

1. Find point correspondences using facial feature[31] detection
2. Delaunay triangulation
3. Warping images and Alpha blending
4. Finding locations of feature points in morphed images
5. Calculating affine transformations
6. Applying warping triangles/ Warping
7. Applying the alpha blending technique on the resultant image obtained after warping the two images
8. Facial landmarks are those regions of face that are most important features in face recognition systems

Preprocessing steps comprise of extraction of face region followed by face detection using the Viola-Jones algorithm and the reason for using the algorithm is because it's a great combination of the powerful tools like Haar features extractor, integral image builder, Adaboost and classifier cascade [2]. Voting between different types of feature extraction methods tend to establish correlation among the features thereby providing our system an inference/intuition that is more complex to break, attack and overcome and to analyze too and this inference is more foolproof.

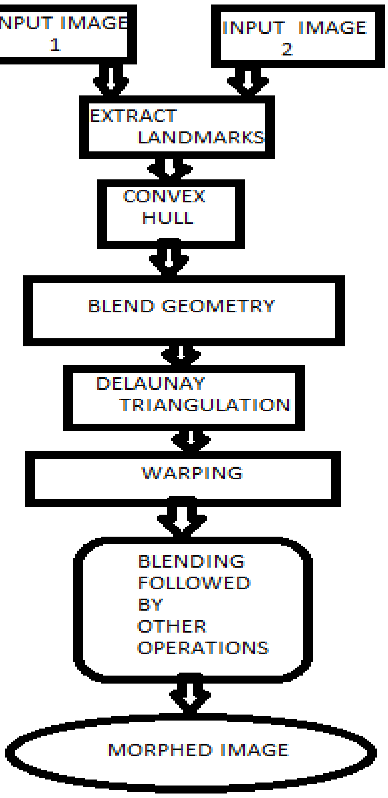
Postprocessing: -

Stir Trace [15] [30] [36] is used to simulate the various post-processing approaches to challenge the media face morphing detectors. Motivation for the proposed the work find a basis for the same is the research output of the media forensics community, where a model has been set up for detecting manipulation histories of images in multi parenting relations [35] and for detection of compositions of images that were made by combining parts from various images but the which is of course not a system to solve the problem of face morphing detection.

We want to combine several distinct features like textures , color , shape , etc. with worrying about the preprocessing and postprocessing techniques applied on the face images and also about the normalization of the aggregated feature vector , seemingly not so feasible , but will have a definite influence on the classifier results and this statement can be backed up by the results obtained from the feature fusing techniques[10] and on those obtained from the combinations of the various binary classifiers used in the [18]past.

[Figure 5 showing some warping methods landmarks estimated by dlib in red and additionally added landmarks in green (left), triangle mesh for triangle warp (center), lines for field morphing (right) taken from [25]]

[Figure 7,depicting a morphing attack taken from [5]]



[Figure 6 depicting the general image morphing pipeline]

B. Datasets analysed and evaluations metrics best suited

The datasets being used in your research work include :-

1. FERET(Face Recognition Technology)
2. FEI
3. CFD(Chicago Face Database)
4. Utrecht-ECVP(European Conference on Visual Perception)
5. BU-4FDE
6. ScFace(Surveillance Cameras Face Database)
7. PUT

Evaluation[14] is critical to know the performance of the system. The evaluation measure generally in use include[29][5][41][42]:-

1. Mated Morph Presentation Match Rate(MMPMR):- Defined as the total number of images in which certain pre-assigned threshold is exceeded and hence gets classified as morphed divided by number of images in the face image database.
2. Attack Presentation Classification Error Rate(APCER):-Defined as the proportion of attack presentations using the same presentation attack's original images/species to those images that are incorrectly classified as bona fide presentations for a specific morphed and original images pairs.
3. Average Classification Error Rate (ACER) defined as:

(NFCM+MFCN)/2) Normal Face image Classified as Morphed face image (NFCM): The ratio of normal face images classified as morphed face image. (2) Morph Face image Classified as a Normal face image (MFCN): The ratio of morphed face images classified as normal face.

Other evaluation metrics are general-Imposter Attack Presentation Match Rate(IAPMR) , Detection Equal Error Rate (D-EER)

5 Future Scope

In our future work we are going to include the results and analysis of the performance of the system on the datasets mentioned above .It may also include few more modifications , hyperparameter tuning , adjustment of weights allotted to the various different parts of the feature vector that's being used for comparison by the SVM classifier.

References

1. [1] J. Kannala and E. Rahtu. Bsif: Binarized statistical image features. In Pattern Recognition (ICPR), 2012 21st International Conference on, pages 1363–1366, 2012.

[2] P. Viola and M. J. Jones. Robust real-time face detection. International Journal of Computer Vision, 57(2):137–154.

[3] J. Maatta, A. Hadid, and M. Pietikainen. Face spoofing detection from single images using micro-texture analysis. In Biometrics (IJCB), 2011 International Joint Conference on, pages 1–7, Oct 2011.

[4] M. Ferrara, A. Franco, and D. Maltoni. The magic passport. InBiometrics(IJCB),2014IEEEInternationalJointConference on, pages 1–7, 2014.

[5] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert. Detection of face morphing attacks by deep learning. In Proc. Int. Workshop on Digital Watermarking (IWDW), pages 107–120, 2017.

[6] U. Scherhag, et al . Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In Int. Conf. of the Biometrics Special Interest Group (BIOSIG), pages 1–12, 2017.

[7] R. Ramachandra, K. Raja, N. Vetrekar, S. Venkatesh, and C. Busch. Face morphing versus face averaging: Vulnerability and detection. In Proc. Int. Joint Conf. on Biometrics (IJCB), pages 1–6, 2017.

[8] S. Liao, X. Zhu, Z. Lei, L. Zhang, and S. Z. Li. Learning multi-scale block local binary patterns for face recognition. InProc.Int'lConf.onBiometrics(ICB'07),pages828–837, 2007.

[9] H. Bay, A. Ess, T. Tuytelaars, and L. V. Gool. SpeededUp Robust Features (SURF). Computer Vision and Image Understanding, 110(3):346 – 359, 2008.

[10] E. Rosten and T. Drummond "Fusing Points and Lines for High Performance Tracking" (2005) IEEE International Conference on Computer Vision. 2: 1508– 1511 DOI:10.1109/ICCV.2005.104

[11] A. Lanitis, C. J. Taylor, and T. F. Cootes, "Automatic Face Identification System Using Flexible Appearance Models", Image and Vision Computing,pp. 392-401, Vol. 13, No. 5, 1995.

[12] Ch. Nastar, B. Moghadam, and A. Pentland, "Generalized Image Matching: Statistical Learning of Physically-Based Deformations", Lecture Notes in Computer Science, Computer Vision - ECCV '96, B. Buxton and R. Cipolla (Eds.), Springer, pp. 589-598, 1996.

[13] P. J. Benson. Morph transformation of the facial image. Image and Vision Computing, 12(10):691–696, 1994.

[14] P. J. Grother, R. J. Micheals, and P. Phillips. Face recognition vendor test 2002 performance metrics. In Proceedings of the 4th International Conference on Audio Visual Based Person Authentication, AVBPA'03, pages 937–945, Guildford, UK, June 2003.

[15] Popescu, A.C., Farid, H.: Exposing digital forgeries by detecting traces of resampling. IEEE Trans. Sig. Process. 53(2), 758–767 (2005)

[16] Kirchner, M., Gloe, T.: On resampling detection in re-compressed images. In: 2009 First IEEE International Workshop on Information Forensics and Security (WIFS), 21–25 December 2009

[17] Kirchner, M., Fridrich, J.: On detection of median filtering in digital images. Proc. SPIE 7541, 754110–754110–12 (2010)

[18] Lapuschkin, S., Binder, A., Montavon, G., M¨uller, K.R., Samek, W.: Analyzing classifiers: fisher vectors and deep neural networks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2912–2920 (2016)

[19] Yu, J., Zhan, Y., Yang, J., Kang, X.: A multi-purpose image counter-anti-forensic method using convolutional neural networks. In: Shi, Y.Q., Kim, H.J., PerezGonzalez, F., Liu, F. (eds.) IWDW 2016. LNCS, vol. 10082, pp. 3–15. Springer, Cham (2017). doi:10.1007/978-3-319-53465-7 1

[20] Beier, T., Neely, S.: Feature-based image metamorphosis. In: Proceedings of the 19th Annual Conference on Computer Graphics and Interactive Techniques, SIGGRAPH 1992, pp. 35–42. ACM, New York (1992)

[21] Raghavendra, R., Raja, K.B., Busch, C.: Detecting morphed face images. In: 8th IEEE International Conference on Biometrics Theory, Applications and Systems, BTAS 2016, Niagara Falls, NY, USA, pp. 1–7, 6–9 September 2016

[22] Krizhevsky, A., Sutskever, I., Hinton, G.E.: Imagenet classification with deep convolutional neural networks. In: Advances in Neural Information Processing Systems 25. Curran Associates, Inc., pp. 1097–1105 (2 Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V., Rabinovich, A.: Going deeper with convolutions. In: Computer Vision and Pattern Recognition (CVPR) (2015)

[23] Federico Monti et al., Geometric deep learning on graphs and manifolds using mixture model CNNs, arXiv:1611.08402v3 [cs.CV] 6 Dec 2016

[24] Vilas H. Gaidhane, Yogesh V. Hote, Vijander Singh , A New Approach for Estimation of Eigenvalues of Images, International Journal of Computer Applications (0975 – 8887) Volume 26– No.9, July 2011

[25] Clemens Seibold, Wojciech Samek, Anna Hilsmann and Peter Eisert, Accurate and Robust Neural Networks for Security Related Applications Exampled by Face Morphing Attacks, arXiv:1806.04265v1 [cs.CV] 11 Jun 2018

[26] Alex Krizhevsky et al., Dropout: A Simple Way to Prevent Neural Networks from Overfitting, Journal of Machine Learning Research 15 (2014) 1929-1958

[27] Kaiming He Xiangyu Zhang Shaoqing Ren Jian, Deep Residual Learning for Image Recognition, arXiv:1512.03385v1 [cs.CV] 10 Dec 2015

[28] Chiyuan Zhang et al., Understanding deep learning requires rethinking generalization, arXiv:1611.03530v2 [cs.LG] 26 Feb 2017

[29] Ulrich Scherhag , Christian Rathgeb, Christoph Busch, Morph Deterction from Single Face Image: a Multi-Algorithm Fusion Approach, ICBEA '18 Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications, Pages 6-12 ,Amsterdam, Netherlands — May 16 - 18, 2018

[30] Andrey Makrushin,Christian Kraetzer, Tom Neubertand Jana Dittmann, Generalized Benford's Law for Blind Detection of Morphed Face Images, Session: Biometrics and Forensics IH&MMSec'18, June 20–22, 2018, Innsbruck, Austria

[31] Yasushi Yagi, Facial Feature Extraction'from Frontal Face Image, Proceedings of ICSP2000

[32] Clemens Seibold, Anna Hilsmann, Peter Eisert, Reflection Analysis for Face Morphing Attack Detection, arXiv:1807.02030v1 [cs.CV] 5 Jul 2018

[33] Christian Lipski, Christian Linz, Marcus Magnor. Belief Propagation Optical Flow for High-Resolution Image Morphing, SIGGRAPH 2010, Los Angeles, California, July 25 – 29, 2010. ISBN 978-1-4503-0210-4/10/0007

[34] Stamm, M.C., Liu, K.J.R.: Anti-forensics of digital image compression. IEEE Trans. Inf. Forensics Secur. 6(3), 1050–1065 (2011)

[35] Kirchner, M., Bohme, R.: Hiding traces of resampling in digital images. IEEE Trans. Inf. Forensics Secur. 3(4), 582–592 (2008)

[36] M.Hildebrandt,T.Neubert,A.Makrushin,andJ.Dittmann.2017. Benchmarking face morphing forgery detection:Application of stirtrace for impact simulation of different processing steps .In Proc.5th Int.Workshop on Biometrics and Forensics (IWBF).1–6.

[37] Ebrahim Karami, Siva Prasad, and Mohamed Shehata, Image Matching Using SIFT, SURF, BRIEF and ORB: Performance Comparison for Distorted Images,

[38] Christian Kraetzer et al., Modeling Attacks on Photo-ID Documents and Applying Media Forensics for the Detection of Facial Morphing, Session: Media Forensics & Counterforensics IH&MMSec'17, June 20-22, 2017, Philadelphia, PA, USA

[39] arXiv:1710.02726

[40] Makrushin, Andrey, Tom Neubert and Jana Dittmann. "Automatic Generation and Detection of Visually Faultless Facial Morphs." VISIGRAPP (2017).,

[41] I. Chingovska, A. R. d. Anjos and S. Marcel, "Biometrics Evaluation Under Spoofing Attacks," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2264-2276, Dec. 2014.

[42] A. Hadid, N. Evans, S. Marcel and J. Fierrez, "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 20-30, Sept. 2015.

[43] U. Scherhag, C. Rathgeb and C. Busch, Towards detection of morphed face images in electronic travel documents, 2018 13th IAPR International Workshop on Document Analysis Systems

[44] Erwin Kreyszig,Advanced Engineering Mathematics 9TH edition