Generalized Facial Manipulation Detection with Edge Region Feature Extraction

Dong-Keon Kim
Sungkyunkwan University
kdk1996@skku.edu

Kwangsu Kim
Sungkyunkwan University
kim.kwangsu@skku.edu

Abstract

This paper presents a generalized and robust face manipulation detection method based on the edge region features appearing in images. Most contemporary face synthesis processes include color awkwardness reduction but damage the natural fingerprint in the edge region. In addition, these color correction processes do not proceed in the non-face background region. We also observe that the synthesis process does not consider the natural properties of the image appearing in the time domain. Considering these observations, we propose a facial forensic framework that utilizes pixel-level color features appearing in the edge region of the whole image. Furthermore, our framework includes a 3D-CNN classification model that interprets the extracted color features spatially and temporally. Unlike other existing studies, we conduct authenticity determination by considering all features extracted from multiple frames within one video. Through extensive experiments, including real-world scenarios to evaluate generalized detection ability, we show that our framework outperforms state-of-the-art facial manipulation detection technologies in terms of accuracy and robustness.

1. Introduction

As various AI-based generative models are developed [22, 39, 13], facial manipulated videos, so-called DeepFake, are becoming a major social issue. These forged videos are becoming so sophisticated that it is difficult to determine the authenticity with the human eye. Moreover, the advent of these realistically synthesized videos allows malicious actions to threaten the creditability of public media and individual privacy [46], e.g., politicians’ fake news, celebrity pornography. Therefore, effective detection of facial manipulation is a significant issue in the computer vision field.

Most contemporary face synthesis algorithms generate a face shape (expression, mouth shape, etc.) learned by source images and pasting the shape into the face area of target images [47]. Early DeepFake videos in public datasets such as UADFV [26] and DeepfakeTIMIT [23] commonly synthesized faces in target images without pixel-level correction, resulting in color awkwardness in the face edge region. In response, more advanced manipulation methods add post-processing procedures such as Gaussian blurring or Bi-linear interpolation to express the face-synthesized image more naturally [28, 35], as shown in Figure 1.

We observe that several modern face synthesis methods have the following common features: 1) Post-processing is done only on the facial part. Since the color correction is not performed on unrelated background parts, the inherent features of the background part are not damaged. 2) The face synthesis process does not involve the time concept. The intrinsic features vary in each frame, even with a slight change of pixels. However, the artificially synthesized videos do not highly consider the sequential changes.

Based on these observations, we propose a generalized detection model of synthesized images. We mainly focus on a robust facial image forensic method through color distribution changes in the face-synthesizing process. Our proposed method pays attention to pixel-level features from the edge region in the entire, not only on the features appearing in the face, like other existing studies [1, 18, 36].

Also, a classification model including the temporal concept is introduced to improve detection performance. The latest studies [37, 50] have already demonstrated that the
framework that includes the time-domain properties has a much better forgery detection performance. Existing studies use known networks such as SlowFast [12] and Xception [4] as backbone. However, these models are not suitable for handling very small-sized chronospatial inputs. Therefore, a 3D classification model based on DenseNet [17] is introduced for dealing with the extracted small-size edge region features spatiotemporally.

This paper has great potential to contribute to the field of face manipulation detection. More specifically, our framework is unique in that it reflects the edge attributes appearing throughout the whole image and interprets these features spatiotemporally. Several cross-experimental results show that our method outperforms other existing detection frameworks in accuracy and generalization ability.

2. Previous Work

In response to the rising threats of AI-generated facial forgeries, many researches [10, 30, 38, 8, 14, 26] have been held to detect forged images. Existing studies devise their methods based on the abnormality revealed in the synthesized facial area. For example, Matern et al. [33] present a detection method based on visual artifacts in eyes and noses. Yang et al. [49] suggest a DeepFake detection methodology focusing on the inconsistency of head poses. While these works pay attention to the awkwardness features of synthesized faces, many recent works [1, 42, 54, 53] presents detection methods with state-of-the-art artificial neural networks such as the recurrent neural network [14] and capsule network [36]. All of these studies commonly focus on the forged image itself rather than the synthesis process. This approach inevitably exposes limitations in practical situations where it is necessary to determine the authenticity of video data made from various sources.

The facial manipulation detection should remain robust even with unseen forged data to apply the detection framework in real-world situations. The latest studies [5, 10, 48, 6, 19] focus on the innate artifacts that appear in the face image synthesis process for a more practical detection framework. For instance, Face X-ray [25] focuses on common blending procedures and shows their generalization ability with unseen datasets. SPSE [29] analyzes forged images as a phase spectrum that emphasizes the abnormal features from the up-sampling procedure in generative models. These novel studies also show good performance in cross-dataset experiments, but they also have a problem of observing only the features of the face part. This limitation critically loses generality when cross-validating the source data with completely disparate datasets (e.g. FaceForensics++ [40] for train, Celeb-DF [28] for test). Our study further derives a better performance with more generality by comparing the extracted features between facial edges and background edges.

3. Edge Region Feature

Early research in image forensics [11] mentions that un-forged natural images have unique fingerprints and artifacts. These traces are affected by external factors such as the surface of a camera lens, the direction of the light entering the camera, and the image processing procedure. Moreover, recent studies [24, 34, 51, 31] show that AI-based generative models do not address color component distortion or unnatural (artificial) imprints, resulting in imperfect reproduction of original imprints. Thus, the face-replacing and the color-correcting process damage the raw image fingerprints across the facial boundary. We pay attention to this point by extracting the color difference features in both the facial part and the background area at the edge region.

3.1. Facial Edge Region Feature

With the frame image I extracted from the video, the face area from I is detected with the frontal face detector in dlib [20]. Then the 68 feature points are extracted from the detected face with 68 face landmark shape predictors in dlib. Among them, we define the first 17 feature points representing the facial contours as facial boundary points, FBPs. We would like to create a line segment perpendicular to the facial boundary line to obtain color features along the face edge region. The x-coordinate and y-coordinate corresponding to the line segment element \( P_{i+1} \) are generated with the coordinates of two neighboring landmark points \( L_i \) and \( L_{i+1} \) in FBPs. The creation method follows parametric equations (1) and (2).

\[
P_x(t)_{i+1} = \frac{(L_{i+1,y} - L_{i,y})\sqrt{S_x}}{D_{i+1}} t + M_{i+1,x} \tag{1}
\]

\[
P_y(t)_{i+1} = -\frac{(L_{i+1,x} - L_{i,x})\sqrt{S_y}}{D_{i+1}} t + M_{i+1,y} \tag{2}
\]

Here, \( t \) is a 20 integer parameter with a range of -10 to 9, from the inside to the outside of the face. \( D_{i+1} \) and...
Figure 3. Facial boundary window generation pipeline. (a) Capture image $I$ from video. (b) Get a facial boundary line with face landmark points detected from (a). (c) Make perpendicular line segment $P_{i,i+1}$ with neighboring landmark points. (d) Create a set of horizontal lines $V_{i,i+1}$ perpendicular to line segment $P_{i,i+1}$ at equal intervals.

$M_{i,i+1}$ indicates distance and midpoint between two landmark points $L_i$ and $L_{i+1}$ each. Midpoint $M_{i,i+1}$ is located on $t = 0$. Note that $x, y$ in subscript are $x$-coordinate and $y$-coordinate, respectively. $S_I$ is a scale-factor for adjusting the length of the perpendicular line segment according to the size of the face in the image $I$. $S_I$ is obtained through the following equation (3).

$$S_I = \frac{\alpha}{A_I}$$ (3)

$A_I$ is the convex area value covering the face contour created from the FBP, which are obtained from image $I$. $\alpha$ is a tunable hyper-parameter that is related to the interval between line segment coordinates. By tuning with the scale-factor, the perpendicular line segment $P_{i,i+1}$ passes through a specific range of the facial boundary, regardless of face size in the image.

With gathered line segments, we create window-shaped features to reflect the boundary region features spatially. A set of horizontal line segments $V_{i,i+1}$, which are parallel to the facial boundary line, are considered. This horizontal line goes through the $t$ point of obtained line segment $P_{i,i+1}$. The concrete coordinates of horizontal line segments $V_{i,i+1}$ are generated by following parametric equations (4) and (5).

$$V_x(u, t)_{i,i+1} = \frac{(L_{i+1,x} - L_{i,x})\sqrt{2S_I}}{\beta} u + P_x(t)_{i,i+1}$$ (4)

$$V_y(u, t)_{i,i+1} = \frac{(L_{i+1,y} - L_{i,y})\sqrt{2S_I}}{\beta} u + P_y(t)_{i,i+1}$$ (5)

Horizontal line segments are also represented by a parametric equation. Note that parameter $u$ which has 20 integer parameters with range -10 to 9. $\beta$ is a tunable hyper-parameter related to interval between horizontal line segment coordinates. The window-shaped $20 \times 20$ corresponding coordinates are specified by a set of 20 horizontal lines. Figure 2 illustrates an example of an extracted edge window. We will refer to these 400 coordinate features as edge window $W_i$, a set of horizontal lines $V_{i,i+1}$ with two parameters $t$ and $u$. A total of 16 windows are created per single image $I$ with facial boundary points (i.e., $i \in \mathbb{N} | 1 \leq i \leq 16$). A summarized pipeline of window generation from a facial image is shown in Figure 3.

After creating the edge window $W_i$, we compute the absolute difference of the RGB pixel values according to the parameter $t$ to find out how the RGB pixel values in edge window $W_i$ change from the inside to the outside of the face. These extracted 16 windows shaped $20 \times 19 \times 3$ color value differences are $F_I$, which is the facial boundary features of the image $I$. Note that 20 refers to the number of $u$-direction coordinates in edge windows, 19 implies the modified parameter $t$ ($t = 0$ is center) on which differentiated color value lie, and 3 indicates RGB.

3.2. Background Edge Region Feature

Before extracting background edge points’ features, we make a background edge image $E_I$ from frame image $I$. We firstly blur image $I$ with $5 \times 5$ Gaussian filter to removing
noise of background and extract distinctive boundary parts. Then, the rough edge image $E'_I$ including edge points on the face is generated with the Canny edge detector [3].

The facial edge points in $E'_I$ must be excluded to extract the natural fingerprint of the background edges. We considered convex image $C_I$ that covers face contour made with the FBPs. $C_I$ is a binary image with the same size as the original image $I$ with inner points of convex are 0, and the outer points of convex are 1. A big-face convex image $C_I'$ is created by blurring $C_I$ with $15 \times 15$ Gaussian Filter and rounding down each value in blurred $C_I$ to 0, except the pixels with the values of 1. We can get an edge image $E_I'$ that excludes facial edge points by multiplying $C_I'$ and $E'_I$, element-wise. A brief pipeline of making background edge image $E_I$ is shown in Figure 4.

With edge image $E_I$, 10% of the total edge points in $E_I$ are randomly sampled to get statistical information that appears along background edges. Then background windows are extracted with sampled edge points in the same way as facial boundary features are, with $L_i$ and $L_{i+1}$ corresponding to the two nearest points of a sampled point. The extracted features are $N$ windows shaped $20 \times 19 \times 3$ where $N$ is the number of sampled edge points in background edge image $E_B'$. While $20$, $19$, and $3$ are equivalent to that mentioned in Section 3.1. A summarized procedure of the background edge windows generation is shown in Figure 5.

The direction of parameter $t$ in the background edge windows from the $E_I$ cannot be specified except that their boundary lines are in a vertical direction of edge points. For this reason, we fold the background edge feature and symmetrically unfold with the basis on $t = 0$ to remove the directional information in the edge window ($e.g.$, all feature values in $t = -9$ and $t = 9$ are averaged by the axis). Finally, the values of the $N$ windows are averaged to get statistical information of the sampled $N$ window features. A $B_I$, which is the final background boundary feature of image $I$, is the averaged background edge region features shaped $20 \times 19 \times 3$.

4. Analysis with Extracted Features

We apply the proposed feature extraction method to face forensic datasets. Several datasets are adopted: FaceForensics++ (FF++) [40], Celeb-DF [28], and DFDC [9]. All of these datasets contain genuine video data and face manipulated video data forged from genuine ones. We randomly choose 750 genuine videos and 750 manipulated videos for FaceForensics++, and DFDC each. Exceptionally, the Celeb-DF dataset has less than 750 genuine video data, so we choose 563 genuine video data and 750 manipulated video data in the Celeb-DF dataset. Since the length of videos included in datasets varies, 24 consecutive frames at random timepoint are extracted.

The features extracted in Sections 3.1 and 3.2 are additionally post-processed for statistical analysis. The $F_I$, which has 16 edge windows, is replaced with the averaged edge window. Then the edge region feature values of both face and background are averaged along the $u$-axis. The averaged $F_I$ and $B_I$, which both are shaped $19 \times 3$, are the statistical data of the extracted edge region features. Here, 19 indicates the $t$-axis, which is the vertical direction of the boundary line, and 3 refers to RGB.

We plotted a graph to statistically analyze the change in the color difference along the vertical line of the edge regions. Figure 6 shows the dataset-wise distributions of facial features and background features along parameter $t$-direction. Note that boundary edge points are at $t = 0$. We observe a distribution difference between the facial features derived from the face manipulated image and those of the real image. There is a significant difference in distribution points close to $t = 0$, indicating the point along the facial boundary line.

In all three datasets, only the color distribution of the facial edge region has a distinct difference between the real and the fake. In addition, the difference between the color distribution of the forged facial boundary area and those of the background boundary area is similar regardless of the
dataset. This observation shows that reflecting the facial information and background information together could help solve the generalization problem.

5. Classification Model

Recent studies [6, 25, 27] attempted to find a more generalized image forensic solution by localizing the face synthesized parts. They used well-known neural networks as the backbone network such as HRNet [43] or XceptionNet [4] with combining their own methods. These existing 2D CNN-based models have good classification performance for single image input. However, these models are not suitable for determining the authenticity of a video because these 2D models are limited to extract only spatial features rather than temporal features.

Even for the same video, fingerprints appearing in a frame vary slightly over time due to external factors such as lighting brightness and camera shake. Contemporary face synthesizing algorithms cannot blend faces by reflecting these fingerprint’s subtle changes. Therefore, spatial and temporal interpretation of the extracted edge region features can lead to higher performance in determining the authenticity of a video.

Lately, 3D-CNN models are designed by borrowing the structure of an existing 2D-CNN model for action recognition and medical image analysis [16, 2]. In particular, a recent face manipulation detection study [37] uses a SlowFast [12], which is for video feature extraction, as a backbone network. Studies applying these 3D-Models to video-related tasks show remarkable performance in each field. However, all 3D networks of previous studies have structures that receive relatively large input sizes, usually whole frames. On the other hand, our extracted features have a small size, around 20 pixels in height and width. Therefore, it is not appropriate to utilize other existing networks as a backbone for our framework.

Considering these observations, we designed a 3D-CNN model for our framework to classify facial manipulated video. A 3D-LightDenseNet by referring to the DenseNet [17, 15] model is devised to obtain richer spatio-temporal information from the processed features. This model takes the edge region features extracted from several consecutive frames within a video as input. The 3D-LightDenseNet has a shallower structure than the existing DenseNet because the size of the extracted edge region is smaller than the entire image.

Overall, this model behaves in a similar way to the existing DenseNet. This model also consists of Dense Block and Transition Block. We simply convert all 2D-Layers to 3D-Layer. The notable difference is that there is no pooling layer in Dense Block. This is because the size of the initial input is very small. The detailed network structure is shown in Figure 7.
6. Experiment

We perform extensive experiments using the DFD dataset [7] and 3 face forensic datasets mentioned in Section 4. In addition to cross-validation and comparison experiments, in-depth experiments and ablation studies are designed to test the proposed method’s robustness and practicality.

**Experiment Inputs.** First, we split each dataset into 80% for training data and 20% for test data. As with the frame extraction method described in Section 4, 24 consecutive frames at random timepoint are extracted per video. Then edge region features are extracted frame-wisely with referring to Section 3. The hyper-parameters $\alpha$ and $\beta$ in Section 3 are empirically set to 25, 54, respectively. Extracted features $F_I$ are shaped $20 \times 19 \times 24$ with $16 \times 3$ channels, of which 16 refers to the number of facial boundary windows, and 3 indicates RGB. Additionally, we make a difference features $D_I$ with $F_I$ and $B_I$ by referring to the Equ. (6). Note that $D_I$ is a post-processed $B_I$ to reflect the color distribution differences between the background edge region and the face edge region in the classification framework.

$$D_{I,i} = F_{I,i} - B_I$$  (6)

Here, the $i$ indicates the enumerated edge window. The calculated $D_I$ is an index indicating how much more focus is placed on the face compared to the background in one image data.

The computed difference features $D_I$ have the same shape and the same number of channels as the $F_I$. The final input shape for 3D-LightDenseNet is $20 \times 19 \times 24$ with 96 channels, which 96 indicates sum of the number of channels of the $F_I$ and those of the $D_I$.

**Model Details.** The total epoch is set to 1000, and the batch size is set to 20. The learning rate is set as 0.00075 using the Adam [21] optimizer. Additionally, we scheduled the optimizer to multiply 0.5 to the learning rate at every 200 epochs in case of a decaying learning rate. The growth rate is set to 32, and the dense block layers are set to 6, 12, 8 each. The cross-entropy function is used for loss function.

**6.1. Cross-Validation with Various Datasets**

We firstly design a cross-validation experiment to test our approach in the aspect of robustness to real-world scenarios. In this experiment, we train our model with one dataset and test with another dataset to make scenarios that detect manipulated images with unseen datasets. Table 1 shows the cross-validation performance result of our approach in terms of AUC(Area Under the receiver operating curve).

| Training | Test       | FF++ | DFD | DFDC | CelebDF |
|----------|------------|------|-----|------|---------|
| FF++     | 99.8       | 95.1 | 90.0 | 87.8 |
| DFD      | 96.3       | 99.8 | 89.2 | 87.9 |
| DFDC     | 98.7       | 93.2 | 98.1 | 88.5 |
| CelebDF  | 99.8       | 99.6 | 97.3 | 95.4 |

Table 1. Cross-validation performance results.
Detection Performance (AUC)

| Method     | Training | Test   |
|------------|----------|--------|
| Comp.      |          |        |
| FF++       | 95.4     | 82.3   |
| DFD        | 83.1     | 95.3   |
| DFDC       | 80.0     | 85.5   |
| CelebDF    | 84.4     | 83.3   |

| Method     | Training | Test   |
|------------|----------|--------|
|             |          |        |
| FF++       | 96.5     | 85.7   |
| DFD        | 89.8     | 96.9   |
| DFDC       | 82.7     | 86.2   |
| CelebDF    | 89.4     | 91.1   |

Table 2. Performance results with pixel-level manipulated video. Comp. indicates image compression, and Resize refers to image downsizing. The results with raw video datasets are in Table 1.

Table 3. Single dataset experiment result compared with contemporary works.

Detection Performance (AUC)

| Study         | FF++ | CelebDF |
|---------------|------|---------|
| FWA [27]      | 93.0 | 64.6    |
| Face X-ray [25]| 98.5 | 74.8    |
| Evolution [45]| 99.5 | 83.6    |
| Two-Branch [32]| 93.2 | 73.4    |
| F³ Net [37]   | 98.0 | -       |
| VST [48]      | 99.6 | 96.2    |
| SPSL [29]     | 96.9 | -       |
| Ours          | **99.8** | **98.8** |

Table 4. Generalization performance results compared with recent studies. All comparison frameworks are trained using only the FaceForensics++ dataset.

We figure that cross-validating models trained with Celeb-DF features can obtain more generalized results than models trained with other datasets. This inconsistency may occur because the features extracted from the Celeb-DF dataset have relatively less distinctive differences between unforged images and manipulated images when compared to the other three datasets. We can see that a model trained with a dataset with relatively less prominent features performs well when verifying a dataset with more prominent features. Nevertheless, any experiment result with DFDC and Celeb-DF outperforms other referred face manipulation detection methods to be described later.

6.2. Comparison with Latest Works

Detection Accuracy. As with the experimental method mainly conducted in other previous studies, we experiment with one specific dataset for both training and testing. The performance results of several existing methods [27, 25, 45, 32, 37, 29, 41] are compared with those of our proposed method. Experiments are conducted with the FF++ and Celeb-DF datasets, which have been mainly covered in other studies. The summarized performance comparison is in Table 3.

The detection results for the Celeb-DF dataset are slightly inferior compared to the latest studies [41, 48], while results of the FaceForensics++ dataset are superior to other studies. The comparison results of other latest detection frameworks show that the general detection performance itself is also excellent.

Generalization Ability. We compared our performance results with the latest works [52, 27, 25, 29, 37, 48] that deal with generalized forgery detection ability for a more precise evaluation of universality. Similar to the cross-validation experiments conducted in other studies, our framework is trained with only the FaceForensics++ dataset to perform comparison experiments. The Celeb-DF dataset and DFDC dataset are used for cross-validation tests. The forged videos in these datasets are made with totally different source data from the those of FaceForensics++ dataset. Table 4 summarizes the AUC results compared with these existing contemporary works and ours.

We observe that our framework outperforms the other several approaches in terms of the AUC results. Compared to FF++ results verified with the same dataset, the performance results of cross-validation with DFDC and Celeb-DF are much better than the latest generalization studies.

6.3. Forgery Detection Against Pixel Manipulation

Image Compression. We evaluate whether the proposed detection framework has robust detection capabilities in terms of image compression. The experiment is performed by compressing the image quality of videos in existing datasets. Image compression is performed on all datasets.
Detection Performance (AUC)

| Method   | Training | Test  | Method   | Training | Test  |
|----------|----------|-------|----------|----------|-------|
| w/o BG   | FF++     | 98.5  | DF       | 91.2     | 84.8  |
|          | DFD      | 88.2  | DFD      | 96.1     | 84.1  |
|          | DFDC     | 91.1  | DFDC     | 86.7     | 97.3  |
|          | CelebDF  | 94.2  | CelebDF  | 91.9     | 87.4  |

2D

| Method   | Training | Test  | Method   | Training | Test  |
|----------|----------|-------|----------|----------|-------|
| FF++     | 95.7     | 92.8  | 89.5     | 96.2     | 85.4  |
| DFD      | 89.5     | 96.2  | 86.0     | 92.8     | 83.3  |
| DFDC     | 91.7     | 88.5  | 94.6     | 94.6     | 82.8  |
| CelebDF  | 95.0     | 94.5  | 91.2     | 94.5     | 89.9  |

Table 5. Performance results of ablation studies. w/o BG refers to without background features, and 2D indicates 2D-variation model of 3D-LightDenseNet. The vanilla results are in Table 1.

used for training and testing. A low-quality(LQ) compression method referred to by [40] is applied to experimental datasets. The test results are in the left part of Table 2.

Compared with Table 1, we see that the experimental results that verifying with the same dataset don’t get much worse. But, the detection performance that verifying with other datasets are poorer than the original results. Hence, feature extraction at the pixel level is especially affected by image quality in cross-validation experiments.

**Image Downsizing.** We additionally test whether the framework shows robust performance even for small-resolution videos. The video used in the experiment is 1/16 (1/4 width, 1/4 height) of the video resolution of the existing dataset. A simple bilinear resizing method is used. The experimental results are shown in the right part of Table 2.

The performance deterioration is unavoidable with reduced pixel information like the image compression experiment. However, it shows similar detection performance compared with existing studies referred at Section 6.2, even with downsized videos tests. Comparing these experimental results with the performance of other existing studies, it appears that our method is relatively more robust to data laundering like the resolution reduction.

6.4. Ablation Studies

**Effect of Background Features.** We conduct an ablation study to see how much the background edge features affect the detection performance. The experiment evaluates the detection performance by using only the 48 input channels representing the facial edge region features. We change the input channel of the detection model from 96 to 48. Additionally, the numbers of output channels of the convolution layers in the classification model are also proportionally halved. The detection model is then fine-tuned. The test results are presented in the left part of Table 5.

The ablation experiment result of the background edge information is worse than the original test result. Especially in cross-validation experiments, AUC results deteriorated by 5-8%. The experimental results demonstrate that reflecting the features of the background boundary together in the detection framework leads to better generalization performance.

**Effect of Time-domain information.** Most of the contemporary existing face manipulation [36, 27, 44, 29] detection studies do not determine the authenticity of the whole video but in units of frames that exclude the concept of time. We utilize 2D-LightDenseNet to evaluate detection performance with only frames, excluding the concept of time. A 2D-LightDenseNet is a transformed model that replaces all 3D layers of 3D-LightDenseNet with 2D layers. The model takes an input with the dimension of the number of frames removed. The evaluation method for determining the authenticity of an image proceeds with reference to [40]. The experimental results are in the right part of Table 5.

The performances of the time-domain ablation study are inferior to the experimental results through the original 3D model. It shows a performance drop of about 4-7% in all cross-validation AUCs. As a test result shown above, it is important to include the time-domain features when detecting facial tampered videos.

7. Conclusion

We tackle the generalized facial forgery detection problem by leveraging the pixel-level difference in the boundary area made by the post-processing procedure of synthesis algorithms. Our work shows the importance of utilizing both face edge information and background edge information for generalized detection abilities. Furthermore, we demonstrate that spatiotemporal interpretation of these edge region features is more advantageous for image authenticity determination. Outstanding performance results from extensive cross-dataset experiments demonstrate that our approach not only performs well with a specific dataset but can also be fully applied in real-world situations.

Acknowledgements. This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (IITP-2021-2015-0-00742, Grand Information Technology Research Center support program, 50%) and National IT Industry Promotion Agency of Korea(NIPA) grant funded by the Korea government(MSIT) (No.S0316-21-1006, Healthcare AI Convergence Research & Development Program, 50%).
References

[1] Darius Afchar et al. “Mesonet: a compact facial video forgery detection network”. In: 2018 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE. 2018, pp. 1–7.

[2] Toan Duc Bui, Jitae Shin, and Taesup Moon. “3D densely convolutional networks for volumetric segmentation”. In: arXiv preprint arXiv:1709.03199 (2017).

[3] John Canny. “A computational approach to edge detection”. In: IEEE Transactions on pattern analysis and machine intelligence 6 (1986), pp. 679–698.

[4] François Chollet. “Xception: Deep learning with depthwise separable convolutions”. In: Proceedings of the IEEE conference on computer vision and pattern recognition. 2017, pp. 1251–1258.

[5] Davide Cozzolino et al. “Forensictransfer: Weakly-supervised domain adaptation for forgery detection”. In: arXiv preprint arXiv:1812.02510 (2018).

[6] Hao Dang et al. “On the detection of digital face manipulation”. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020, pp. 5781–5790.

[7] DFD. Contributing Data to Deepfake Detection Research. Sept. 2019. URL: https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html.

[8] Xinyi Ding et al. “Swapped face detection using deep learning and subjective assessment”. In: EURASIP Journal on Information Security 2020 (2020), pp. 1–12.

[9] Brian Dolhansky et al. The Deepfake Detection Challenge (DFDC) Preview Dataset. 2019. arXiv:1910.08854 [cs.CV].

[10] Mengnan Du et al. “Towards generalizable forgery detection with locality-aware autoencoder”. In: arXiv preprint arXiv:1909.05999 (2019).

[11] Hany Farid. “A survey of image forgery detection”. In: IEEE Signal Processing Magazine 2.26 (2009), pp. 16–25.

[12] Christoph Feichtenhofer et al. “Slowfast networks for video recognition”. In: Proceedings of the IEEE/CVF international conference on computer vision. 2019, pp. 6202–6211.

[13] Ian Goodfellow et al. “Generative Adversarial Nets”. In: Advances in Neural Information Processing Systems. Ed. by Z. Ghahramani et al. Vol. 27. Curran Associates, Inc., 2014, pp. 2672–2680. URL: https://proceedings.neurips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf.

[14] David Güera and Edward J Delp. “Deepfake video detection using recurrent neural networks”. In: 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). IEEE. 2018, pp. 1–6.

[15] Kensho Hara, Hirokatsu Kataoka, and Yutaka Satoh. “Can spatiotemporal 3d cnns retrace the history of 2d cnns and imagenet?” In: Proceedings of the IEEE conference on Computer Vision and Pattern Recognition. 2018, pp. 6546–6555.

[16] Kensho Hara, Hirokatsu Kataoka, and Yutaka Satoh. “Learning spatio-temporal features with 3d residual networks for action recognition”. In: Proceedings of the IEEE International Conference on Computer Vision Workshops. 2017, pp. 3154–3160.

[17] Gao Huang et al. “Densely connected convolutional networks”. In: Proceedings of the IEEE conference on computer vision and pattern recognition. 2017, pp. 4700–4708.

[18] Hyeonseong Jeon, Youngoh Bang, and Simon S Woo. “FDNtNet: Facing off fake images using fake detection fine-tuning network”. In: IFIP International Conference on ICT Systems Security and Privacy Protection. Springer. 2020, pp. 416–430.

[19] Jun Jiang et al. “Practical Face Swapping Detection Based on Identity Spatial Constraints”. In: 2021 IEEE International Joint Conference on Biometrics (IJCB). IEEE. 2021, pp. 1–8.

[20] Davis E King. “Dlib-ml: A machine learning toolkit”. In: The Journal of Machine Learning Research 10 (2009), pp. 1755–1758.

[21] Diederik P Kingma and Jimmy Ba. “Adam: A method for stochastic optimization”. In: arXiv preprint arXiv:1412.6980 (2014).

[22] Diederik P Kingma and Max Welling. Auto-Encoding Variational Bayes. 2014. arXiv:1312.6114 [stat.ML].

[23] Pavel Korshunov and Sébastien Marcel. “Deepfakes: a new threat to face recognition? assessment and detection”. In: arXiv preprint arXiv:1812.08685 (2018).
[24] Haodong Li et al. “Identification of deep network generated images using disparities in color components”. In: Signal Processing 174 (2020), p. 107616.

[25] L. Li et al. “Face X-Ray for More General Face Forgery Detection”. In: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020, pp. 5000–5009. DOI: 10.1109/CVPR42600.2020.00505.

[26] Yuezun Li, Ming-Ching Chang, and Siwei Lyu. “In ictu oculi: Exposing ai generated fake face videos by detecting eye blinking”. In: arXiv preprint arXiv:1806.02877 (2018).

[27] Yuezun Li and Siwei Lyu. “Exposing deepfake videos by detecting face warping artifacts”. In: arXiv preprint arXiv:1811.00656 (2018).

[28] Yuezun Li et al. Celeb-DF: A Large-scale Challenging Dataset for DeepFake Forensics. 2020. arXiv: 1909.12962 [cs.CR].

[29] Honggu Liu et al. “Spatial-phase shallow learning: rethinking face forgery detection in frequency domain”. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2021, pp. 772–781.

[30] Francesco Marra et al. “Detection of gan-generated fake images over social networks”. In: 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR). IEEE. 2018, pp. 384–389.

[31] Francesco Marra et al. “Do gans leave artificial fingerprints?” In: 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR). IEEE. 2019, pp. 506–511.

[32] Iacopo Masi et al. “Two-branch recurrent network for isolating deepfakes in videos”. In: European Conference on Computer Vision. Springer. 2020, pp. 667–684.

[33] Falko Matern, Christian Riess, and Marc Stamminger. “Exploiting visual artifacts to expose deepfakes and face manipulations”. In: 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW). IEEE. 2019, pp. 83–92.

[34] Scott McCloskey and Michael Albright. “Detecting GAN-generated imagery using saturation cues”. In: 2019 IEEE International Conference on Image Processing (ICIP). IEEE. 2019, pp. 4584–4588.

[35] Yisroel Mirsky and Wenke Lee. “The creation and detection of deepfakes: A survey”. In: ACM Computing Surveys (CSUR) 54.1 (2021), pp. 1–41.

[36] H. H. Nguyen, J. Yamagishi, and I. Echizen. “Capsule-forensics: Using Capsule Networks to Detect Forged Images and Videos”. In: ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2019, pp. 2307–2311. DOI: 10.1109/ICASSP.2019.8682602.

[37] Yuyang Qian et al. “Thinking in frequency: Face forgery detection by mining frequency-aware clues”. In: European Conference on Computer Vision. Springer. 2020, pp. 86–103.

[38] Weize Quan et al. “Distinguishing between natural and computer-generated images using convolutional neural networks”. In: IEEE Transactions on Information Forensics and Security 13.11 (2018), pp. 2772–2787.

[39] Danilo Jimenez Rezende, Shakir Mohamed, and Daan Wierstra. “Stochastic Backpropagation and Approximate Inference in Deep Generative Models”. In: ed. by Eric P. Xing and Tony Jebara. Vol. 32. Proceedings of Machine Learning Research 2. Beijing, China: PMLR, 22–24 Jun 2014, pp. 1278–1286. URL: http://proceedings.mlr.press/v32/rezende14.html.

[40] Andreas Rossler et al. “FaceForensics++: Learning to Detect Manipulated Facial Images”. In: Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV). Oct. 2019.

[41] Yiwei Ru et al. “Bita-Net: Bi-temporal Attention Network for Facial Video Forgery Detection”. In: 2021 IEEE International Joint Conference on Biometrics (IJCB). IEEE. 2021, pp. 1–8.

[42] Ekraam Sabir et al. “Recurrent convolutional strategies for face manipulation detection in videos”. In: Interfaces (GUI) 3.1 (2019).

[43] Ke Sun et al. “Deep high-resolution representation learning for human pose estimation”. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019, pp. 5693–5703.

[44] Michail Tarasiou and Stefanos Zafeiriou. “Extracting deep local features to detect manipulated images of human faces”. In: 2020 IEEE International Conference on Image Processing (ICIP). IEEE. 2020, pp. 1821–1825.

[45] Ruben Tolosana et al. “Deepfakes evolution: Analysis of facial regions and fake detection performance”. In: International Conference on Pattern Recognition. Springer. 2021, pp. 442–456.
Cristian Vaccari and Andrew Chadwick. “Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty, and trust in news”. In: Social Media+ Society 6.1 (2020), p. 2056305120903408.

Mika Westerlund. “The emergence of deepfake technology: A review”. In: Technology Innovation Management Review 9.11 (2019).

Yuting Xu et al. “Visual-Semantic Transformer for Face Forgery Detection”. In: 2021 IEEE International Joint Conference on Biometrics (IJCB). IEEE. 2021, pp. 1–7.

Xin Yang, Yuezun Li, and Siwei Lyu. “Exposing deep fakes using inconsistent head poses”. In: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE. 2019, pp. 8261–8265.

Semih Yavuzkilic et al. “Spotting Deepfakes and Face Manipulations by Fusing Features from Multi-Stream CNNs Models”. In: Symmetry 13.8 (2021), p. 1352.

Ning Yu, Larry S Davis, and Mario Fritz. “Attributing fake images to gans: Learning and analyzing gan fingerprints”. In: Proceedings of the IEEE International Conference on Computer Vision. 2019, pp. 7556–7566.

Daichi Zhang et al. “Detecting Deepfake Videos with Temporal Dropout 3DCNN”. In: ().

Peng Zhou et al. “Learning rich features for image manipulation detection”. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018, pp. 1053–1061.

Peng Zhou et al. “Two-stream neural networks for tampered face detection”. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). IEEE. 2017, pp. 1831–1839.