Improved Xception with Dual Attention Mechanism and Feature Fusion for Face Forgery Detection

Hao Lin  
Guangdong Key Lab of Information Security Technology  
Sun Yat-sen University  
Guangzhou, China  
linh233@mail2.sysu.edu.cn

Kangkang Wei  
School of Computer Science and Engineering  
Sun Yat-sen University  
Guangzhou, China  
weikk5@mail2.sysu.edu.cn

Weiqi Luo  
School of Computer Science and Engineering  
Sun Yat-sen University  
Guangzhou, China  
luoweiqi@mail.sysu.edu.cn

Minglin Liu  
School of Computer Science and Engineering  
Sun Yat-sen University  
Guangzhou, China  
liumlin6@mail2.sysu.edu.cn

Abstract—With the rapid development of deep learning technology, more and more face forgeries by deepfake are widely spread on social media, causing serious social concern. Face forgery detection has become a research hotspot in recent years, and many related methods have been proposed until now. For those images with low quality and/or diverse sources, however, the detection performances of existing methods are still far from satisfactory. In this paper, we propose an improved Xception with dual attention mechanism and feature fusion for face forgery detection. Different from the middle flow in original Xception model, we try to catch different high-semantic features of face images using different levels of convolution, and introduce the convolutional block attention module and feature fusion to refine and reorganize those high-semantic features. In the exit flow, we employ the self-attention mechanism and depthwise separable convolution to learn the global information and local information of the fused features separately to improve the classification ability of the proposed model. Experimental results evaluated on three Deepfake datasets demonstrate that the proposed method outperforms Xception as well as other related methods both in effectiveness and generalization ability.

Index Terms—Deepfake, Attention Mechanism, Feature Fusion, Convolutional Neural Network

I. INTRODUCTION

With the rapid development of deep learning technology, various face forgery methods [1]–[5] based on deep learning have been proposed. Nowadays, more and more forged faces without any visual artifacts are widely spread on social media. If these forgery images are abused, it probably leads to a series of moral, ethical, and safety issues. Nowadays, face forgery detection is facing severe challenges.

Up to now, many deepfake detection methods [6]–[16] have been proposed. Most existing methods are mainly based on Convolutional Neural Network (CNN). For instance, in [10], [11], the authors make full use of physiological signal, such as the inconsistency of human blinks, to detect deepfake; in [13], the authors first introduce the capsule network for face forgery detection, and show that it can achieve very good detection performances compared with related methods; in [7], the authors try to detect those artifacts generated by GAN (Generative adversarial network) for exposing face forgery; in [16], the authors consider deepfake detection as a fine-grained classification problem, and propose a new multi-attentional detection network. Typically, the existing detection methods can achieve good detection accuracy for high-quality databases. However, the detection accuracies would drop compared with their high-quality versions. Furthermore, for those face images with more diverse contents, such as images from WildDeepfake [17], the detection performances of existing methods are still far from satisfactory.

The previous results in [18] show that Xception [19] has better sensitivity to manipulated face images created by deepfake, and it can outperform many related methods for face forgery detection. In this paper, therefore, we use the Xception as the backbone of the proposed method, and introduce dual attention mechanism and feature fusion in the middle flow and exit flow in the original Xception model for face forgery detection. In the middle flow, we firstly obtain different high-dimensional features using different levels of convolution, and refine the features via Convolutional Block Attention Module (CBAM) simultaneously. Finally, we fuse them to get a more comprehensive high-dimensional features for subsequent network analysis. In the exit flow, we employ the self-attention mechanism and depthwise separable convolution to learn the global information and local information of the fused features separately to improve the classification ability of the proposed model. Experimental results show that the proposed method outperforms the related methods both in effectiveness and generalization ability.

The rest of the paper is organized as follows. Section II describes related works. Section III introduces the proposed method in detail. Section IV shows comparative results and discussions. Finally, the concluding remarks of this paper and future works are given in Section V.
II. RELATED WORK

In this section, we will describe three related works used in the proposed method, that is, Xception [19], Convolutional Block Attention Module (CBAM) [20] and self-attention Mechanism [21].

A. Xception

As illustrated in Fig. 1, Xception [19] consists of three flows: Entry flow, Middle flow, and Exit flow. Entry flow includes a classical convolution block and 3 residual separable-Conv blocks; Middle flow includes 8 residual separableConv blocks; Exit flow includes 1 residual separableConv block and 1 separableConv block. Expect for the first block and the last block, all blocks have linear residual connections around them, which aims to prevent the gradient from disappearing during the training process of the network. Xception is a network architecture based on depthwise separable convolution, which can not only significantly reduce the number of parameters, but also independently learn channel correlation and spatial correlation separately. Note that Xception is originally used for traditional image classification. In [18], Xception is introduced to detect face forgery and achieves good detection results. Thus, Xception usually serves as a baseline network for comparative study in most recent related works.

B. Convolutional Block Attention Module

CBAM [20] is a lightweight and general module, which aims to refine features via attention mechanism. As illustrated in Fig 2 given an input feature map, CBAM infers attention maps along two separate dimensions, i.e., channel and spatial, then the attention maps are multiplied to the input feature map for adaptive feature refinement. In this way, CBAM can help the model refines the feature effectively by learning what and where to emphasize or suppress. CBAM is used in sign language recognition [23], generative model [24] and target detection [25]. To our best knowledge, however, there are no related works for deepfake detection.

C. Self-Attention Mechanism

The self-attention mechanism [26] tries to focus on key information and ignore irrelevant information via learning different weights corresponding to the feature maps. The self-attention mechanism can be described as mapping a query and a set of key-value pairs to an output, where the query (Q), keys (K) and values (V) can be obtained from the input feature map. Let \( H, W, F_{in} \) denote the height, width and number of channel of input feature map. \( d_k \) denotes the keys of dimension. Given an input feature map of shape \((H, W, F_{in})\), we firstly flatten it to a matrix \( X \in \mathbb{R}^{HW \times F_{in}} \).

The output of the single-head attention mechanism can be calculated as:

\[
Q = XW_q; K = XW_k; V = XW_v
\]

\[
output = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V
\]

where \( W_q, W_k \) and \( W_v \) represent randomly initialized coefficient matrices, which can be updated during training stage. The softmax denotes the normalization operation. Through the self-attention mechanism, we can adaptively learn the global feature information. Note that the classical convolution operation has a significant weakness in that it only operates on a local neighbourhood, thus missing global information. In some applications, self-attention mechanism can be used to enhance the convolution operation.
### III. PROPOSED METHOD

As illustrated in Fig. 3, the proposed method is an improved version of Xception, and it also includes three flows, that is, entry flow, middle flow and exit flow. We will describe the three modules in the following subsections.

#### A. Entry Flow

The entry flow in the proposed framework is exactly the same as that in original Xception model (refer to Fig. 1), which consists of a classical convolution block and 3 residual separableConv blocks.

#### B. Middle Flow Combined with Feature Fusion & CBAM

The middle flow in the original Xception is composed of 8 residual separableConv blocks within a single branch. In the proposed middle flow, however, we firstly reduce the number of residual separableConv blocks from 8 to 6, and assign them into three parallel branches. As illustrated in Fig. 3, we assign 1, 2, and 3 residual separableConv blocks in the three branches respectively. In this way, the proposed method is able to learn different high-dimensional semantic features of image by using different levels of convolution. Furthermore, we introduce the CBAM after every residual separableConv block to enhance the characterization ability of the features and refines intermediate features. Finally, we merge the reorganized high-dimensional features in the three branches, and employ a $1 \times 1$ convolution to learn the channel correlation to fully integrate these features. By doing so, we can also significantly reduce the dimension of feature map that feed to the exit flow.

#### C. Exit Flow Combined with Self Attention

The exit flow in Xception consists of a residual separableConv block and a separableConv block (including two depthwise separable convolutions). Thus, just local information of the fused features is considered here. Inspired by method [21], we introduce a self-attention module after the first depthwise separable convolution, and this module is paralleled with another depthwise separable convolution in the proposed exit flow as illustrated in Fig. 3. As described in section II-C, each attention map over the fused features are firstly computed from keys (K) and query (Q) in self-attention mechanism. These attention maps are used to compute weighted averages of the values (V). Then we concatenate the results and reshape them to match the original spatial dimensions via a pointwise convolution. In addition, we employ the depthwise separable convolution at the other branch to learn the local information of the fused features. Finally, we combine the global information (via self-attention) and local information (via depthwise separable convolution) of the fused features, and feed them to a fully connected layer for classification.

### IV. EXPERIMENTS

In our experiments, we employ three popular databases, including Deepfake-TIMIT (denoted as TIMIT for short) [31], FaceForensics++ (denoted as FF++) [18], and WildDeepfake [17]. In training stage, we use MTCNN [32] to locate and align the face regions in video frames, and then resize the face images to the size of $224 \times 224$. For a fair comparison, all detection results are evaluated on the same test dataset as existing methods.
We employ the cross-entropy loss and Adam optimizer with the batch size 64. We set the initial learning rate to be 0.0001. We train the networks in total of 20 epochs, and reduce the learning rate by a half every 5 epochs, and select the model with the best accuracy as the final model.

A. Evaluation on FF++, TIMIT and WildDeepfake

In this experiment, just the low-quality (LQ) versions of TIMIT and FF++(deepfake) databases are considered since their high-quality (HQ) versions are relatively detected by the current methods. The detection accuracies are shown in Table I. From Table I, we obtain two following observations:

- First of all, the proposed method always outperforms other test methods in all cases. Compared with the advanced method (i.e., Capsule [13]), the proposed method achieves 0.01%, 2.43%, and 5.72% improvements for TIMIT (LQ), FF++deepfake (LQ), and WildDeepfake respectively. Compared with the original Xception [18] model, the proposed method achieves 0.21%, 5.99%, and 9.00% improvements for the three databases respectively, which means that the feature fusion and dual attention mechanism introduced in the proposed model can effectively enhance the ability of the original Xception for face forgery detection.

- Compared with TIMIT and FF++, the detection accuracies for WildDeepfake are relatively lower for all detection networks. The main reason is due to the diversity of WildDeepfake. Note that those video clips of WildDeepfake are collected on the Internet, they are from different sources and may be compressed several times. Based on our experiments, the proposed method still obtain 83.32% detection accuracy for WildDeepfake. While the detection accuracies are all lower than 77.70% for other test networks.

B. Cross-dataset Evaluation on Celeb-DF

To show the generalization of the proposed method, cross-dataset evaluation on a new database - Celeb-DF [33] is considered. In this section, we first train a classifier based on the high-quality version of FF++ and WildDeepfake respectively, and then use the resulting classifier to detect those face forgeries on Celeb-DF. The comparative results are shown in Table II and Table III respectively.

The results in the two above tables show that the generalization of the proposed method is better than three other modern networks. Especially for the case of training on WildDeepfake, the proposed method achieves around 20% improvements.

C. Ablation Study

In the proposed method, we introduce dual attention mechanism (i.e., CBAM in middle flow and self-attention in exit flow) and feature fusion (in the middle flow) into original Xception model for face forgery detection. In order to verify the rationality of the proposed method, we conduct the

### Table I

| Network          | TIMIT (LQ) | FF++deepfake (LQ) | WildDeepfake |
|------------------|------------|-------------------|--------------|
| AlexNet [27]     | 94.77%     | 90.58%            | 60.37%       |
| VGG16 [28]       | 98.73%     | 90.19%            | 60.92%       |
| ResNetV2-50 [29] | 94.88%     | 90.91%            | 63.99%       |
| ResNetV2-152 [29]| 95.68%     | 88.00%            | 59.33%       |
| Inception-v2 [30]| 95.68%     | 88.00%            | 59.33%       |
| MesoNet-4 [15]   | 91.18%     | 87.75%            | 64.47%       |
| MesoNet-Inception[15]| 97.85%     | 84.82%            | 68.48%       |
| Xception [18]    | 99.65%     | 90.25%            | 74.32%       |
| ADDNet-2D [17]   | 99.54%     | 90.42%            | 76.25%       |
| Capsule [13]     | 99.85%     | 93.81%            | 77.60%       |
| Proposed Method  | 99.86%*    | 96.24%*           | 83.32%*      |

### Table II

| Network          | FF++ (HQ) | Celeb-DF |
|------------------|-----------|----------|
| MesoNet-Inception| 83.00%    | 53.60%   |
| Xception [18]    | 99.70%    | 65.30%   |
| Capsule [13]     | 90.61%    | 67.92%   |
| Proposed Method  | 98.09%    | 68.39%*  |

### Table III

| Network          | WildDeepfake | Celeb-DF |
|------------------|--------------|----------|
| MesoNet-Inception| 68.48%       | 49.11%   |
| Xception [18]    | 74.32%       | 51.87%   |
| Capsule [13]     | 77.60%       | 53.00%   |
| Proposed Method  | 83.32%       | 72.62%*  |
several ablation experiments in this section. For simplicity, WildDeepfake is used for performance evaluation.

- Analysis on Dual Attention Mechanism: In this experiment, we evaluate the the proposed model after removing the CBAM and/or self-attention. The experimental results are shown in Table [V] From Table [IV] we observe that when both CBAM and self-attention are removed from the proposed model, the detection accuracy is 78.28%. When self-attention or CBAM is removed, the corresponding detection accuracies increase to 80.09% and 82.78% respectively. When the self-attention and CBAM are preserved, the proposed method works the best, and achieves 83.32% detection accuracy. The above results show that the dual attention mechanism is useful for face forgery detection.

- Analysis on Different Setups in Middle Flow: In the proposed middle flow, we design three branches (i.e., 1, 2, and 3 residual SparavleConv Blocks and CBAM respectively) to extract different high-dimensional semantic features of face image, and then perform feature fusion on all branches for subsequent network analysis. In this experiment, we evaluate the performance on using different setups in the middle flow. Some comparative results are shown in Table [V] From Table [V] we observe that the proposed middle flow achieves the best detection performance. When adding the 4th branch (i.e., 4 residual SparavleConv Blocks and CBAM) or removing the 3rd branch in proposed middle flow, the corresponding detection accuracies will drop from 83.32% to 79.20% and 74.99% respectively, which means that setting 3 branches is reasonable in the proposed model. In addition, we compared other four setups with a single branch, that is, just using the 1st, 2nd, 3rd branch respectively, and the original middle flow in Xception. Their detection accuracies are all lower than 80.05%, which means that feature fusion is helpful to enhance the model performance.

V. Conclusion
In this paper, we first introduce dual attention mechanism (i.e., CBAM and self-attention) and feature fusion into Xception for face forgery detection, and show that the proposed method can significantly improve the detection performance of the original Xception model, and achieve state-of-the-art results both in the effectiveness and generalization ability compared with related methods. In addition, we also provide some ablation experiments to verify the rationality of introducing dual attention mechanism and feature fusion in the proposed method. In future, there are several important issues in the proposed framework worthy of in-depth study. For instance, we just consider the spatial information as network input in the proposed method. We would combine some features in the frequency domain, and construct a two stream network for further enhancing the detection performance. In addition to high-dimensional facial semantic features, we try to use multiple attention maps to explore discriminative local region (such as eyes and nose) on the face, and fuse these features in the middle flow for face forgery detection.


table

| Setups               | WildDeepfake |
|----------------------|--------------|
| Proposed Method w/o CBAM & Self-Attention | 78.28% |
| Proposed Method w/o Self-Attention | 80.09% |
| Proposed Method w/o CBAM | 82.78% |
| Proposed Method | 83.32% |

| Setups in Middle Flow | Branch Number | WildDeepfake |
|-----------------------|---------------|--------------|
| Proposed middle flow  | 3             | 83.32% *     |
| Adding the 4th branch | 4             | 79.20%       |
| Removing the 3rd branch | 2             | 74.99%       |
| Just using the 1st branch | 1             | 79.60%       |
| Just using the 2nd branch | 1             | 79.57%       |
| Just using the 3rd branch | 1             | 80.04%       |
| Original middle flow in Xception | 1 | 78.53% |


References

[1] J. Thies, M. Zollhöfer, M. Stamminger, C. Theobalt, and M. Nießner, “Face2face: Real-time face capture and reenactment of RGB videos,” in IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 2387–2395.
[2] J. Thies, M. Zollhöfer, and M. Nießner, “Deferred neural rendering: image synthesis using neural textures,” ACM Transactions on Graphics, vol. 38, pp. 66:1–66:12, 2019.
[3] T. Karras, S. Laine, and T. Aila, “A style-based generator architecture for generative adversarial networks,” in Conference on Computer Vision and Pattern Recognition, 2019, pp. 4401–4410.
[4] “Faceswap,” [Online]. Available: https://github.com/MarekKowalski/FaceSwap.
[5] “Deepfakes,” [Online]. Available: https://github.com/deepfakes/faceswap.
[6] S. McCloskey and M. Albright, “Detecting gan-generated imagery using color cues,” 2018. [Online]. Available: http://arxiv.org/abs/1812.08247.
[7] N. Yu, L. Davis, and M. Fritz, “Attributing fake images to gans: Analyzing fingerprints in generated images,” 2018. [Online]. Available: http://arxiv.org/abs/1811.08180.
[8] H. Mo, B. Chen, and W. Luo, “Fake faces identification via convolutional neural network,” in Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2018, pp. 43–47.
[9] L. Guarnera, O. Giudice, and S. Battiato, “Analyzing fingerprints in generated images,” 2018. [Online]. Available: http://arxiv.org/abs/1811.08180.
[10] “Face2face,” [Online]. Available: https://github.com/MarekKowalski/FaceSwap.
[11] T. Jung, S. Kim, and K. Kim, “Deepvision: Deepfakes detection using human eye blinking pattern,” IEEE Access, vol. 8, pp. 83 144–83 154, 2020.
[12] Y. Li, M.-C. Chang, and S. Lyu, “In icu oculi: Exposing ai created fake videos by detecting eye blinking,” in IEEE International Workshop on Information Forensics and Security, 2018, pp. 1–7.
[13] H. H. Nguyen, J. Yamagishi, and I. Echizen, “Multi-task learning for detecting and segmenting manipulated facial images and videos,” in International Conference on Biometrics Theory, Applications and Systems, 2019, pp. 1–8.
[14] H. H. Nguyen, J. Yamagishi, and I. Echizen, “Capsule-forensics: Using capsule networks to detect forged images and videos,” in International Conference on Acoustics, Speech and Signal Processing, 2019, pp. 2307–2311.
[14] L. Li, J. Bao, T. Zhang, H. Yang, D. Chen, F. Wen, and B. Guo, “Face x-ray for more general face forgery detection,” in IEEE Conference on Computer Vision and Pattern Recognition, 2020, pp. 5000–5009.

[15] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, “Mesonet: a compact facial video forgery detection network,” in International Workshop on Information Forensics and Security, 2018, pp. 1–7.

[16] H. Zhao, W. Zhou, D. Chen, T. Wei, W. Zhang, and N. Yu, “Multi-attentional deepfake detection,” 2021. [Online]. Available: https://arxiv.org/abs/2103.02406

[17] B. Zi, M. Chang, J. Chen, X. Ma, and Y. Jiang, “Wilddeepfake: A challenging real-world dataset for deepfake detection,” in The ACM International Conference on Multimedia, 2020, pp. 2382–2390.

[18] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, “Faceforensics++: Learning to detect manipulated facial images,” in International Conference on Computer Vision, 2019, pp. 1–11.

[19] F. Chollet, “Xception: Deep learning with depthwise separable convolutions,” in IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 1800–1807.

[20] B. Ma, X. Wang, H. Zhang, F. Li, and J. Dan, “CBAM-GAN: generative adversarial networks based on convolutional block attention module,” in Artificial Intelligence and Security International Conference, 2019, pp. 227–236.

[21] I. Bello, B. Zoph, Q. Le, A. Vaswani, and J. Shlens, “Attention augmented convolutional networks,” in International Conference on Computer Vision, 2019, pp. 3285–3294.

[22] S. Ioffe and C. Szegedy, “Batch normalization: Accelerating deep network training by reducing internal covariate shift,” in Proceedings of the International Conference on Machine Learning, 2015, pp. 448–456.

[23] C. Huang, F. Wang, and R. Zhang, “Sign language recognition based on cbam-resnet,” in Proceedings of the International Conference on Artificial Intelligence and Advanced Manufacturing, 2019, pp. 48:1–48:6.

[24] B. Ma, X. Wang, H. Zhang, F. Li, and J. Dan, “CBAM-GAN: generative adversarial networks based on convolutional block attention module,” in Artificial Intelligence and Security, 2019, pp. 227–236.

[25] H. Fu, G. Song, and Y. Wang, “Improved yolov4 marine target detection combined with CBAM,” Symmetry, vol. 13, p. 623, 2021.

[26] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, “Attention is all you need,” in Advances in Neural Information Processing Systems, 2017, pp. 5998–6008.

[27] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in Advances in Neural Information Processing Systems, 2012, pp. 1106–1114.

[28] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” in International Conference on Learning Representations, 2015.

[29] K. He, X. Zhang, S. Ren, and J. Sun, “Identity mappings in deep residual networks,” in Computer Vision European Conference, 2016, pp. 630–645.

[30] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, “Rethinking the inception architecture for computer vision,” in IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 2818–2826.

[31] P. Korshunov and S. Marcel, “Deepfakes: a new threat to face recognition? assessment and detection,” 2018. [Online]. Available: http://arxiv.org/abs/1812.08685

[32] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face detection and alignment using multitask cascaded convolutional networks,” IEEE Signal Processing Letters, vol. 23, pp. 1499–1503, 2016.

[33] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, “Celeb-df: A large-scale challenging dataset for deepfake forensics,” in IEEE Conference on Computer Vision and Pattern Recognition, 2020, pp. 3204–3213.