UCF: Uncovering Common Features for Generalizable Deepfake Detection

Zhiyuan Yan
Yong Zhang
Yanbo Fan
Baoyuan Wu

1 The School of Data Science, The Chinese University of Hong Kong, Shenzhen (CUHK-Shenzhen), China
2 Tencent AI Lab

{yanzhiyuan1114, zhangyong201303, fanyanbo0124}@gmail.com, wubaoyuan@cuhk.edu.cn

Abstract

Deepfake detection remains a challenging task due to the difficulty of generalizing to new types of forgeries. This problem primarily stems from the overfitting of existing detection methods to forgery-irrelevant features and method-specific patterns. The latter has been rarely studied and not well addressed by previous works. This paper presents a novel approach to address the two types of overfitting issues by uncovering common forgery features. Specifically, we first propose a disentanglement framework that decomposes image information into three distinct components: forgery-irrelevant, method-specific forgery, and common forgery features. To ensure the decoupling of method-specific and common forgery features, a multi-task learning strategy is employed, including a multi-class classification that predicts the category of the forgery method and a binary classification that distinguishes the real from the fake. Additionally, a conditional decoder is designed to utilize forgery features as a condition along with forgery-irrelevant features to generate reconstructed images. Furthermore, a contrastive regularization technique is proposed to encourage the disentanglement of the common and specific forgery features. Ultimately, we only utilize the common forgery features for the purpose of generalizable deepfake detection. Extensive evaluations demonstrate that our framework can perform superior generalization than current state-of-the-art methods.

1. Introduction

Deepfake technology has gained significant attention in recent years due to its ability to generate highly realistic videos. While deepfake has the potential to be used for various purposes, including entertainment and marketing, it has also been misused for illegal purposes. The use of deepfake to create false content can compromise people’s privacy, spread misinformation, and erode trust in digital media, resulting in severe outcomes like reputational harm, incitement of violence, and political instability.

As a result, developing a reliable and effective deepfake detection algorithm is vitally essential. Recently, a large number of detectors [58, 25, 37, 52, 36, 55, 8] have been proposed for deepfake. Existing detectors generally perform well when the training and testing data are created using the same forgery techniques. However, in real-world applications, the testing data may be created using unknown procedures, leading to differences between the training and testing data and resulting in poor detection performance. This phenomenon, known as the generalization problem in deepfake detection, presents a significant challenge to the
practical use of current detection methods.

Currently, an increasing number of studies are dedicated to tackling the issue of generalization in deepfake detection. These works typically utilize blending artifacts [23, 41] or frequency artifacts [28, 30], and some employ adversarial training to synthesize challenging forgeries [7]. However, these approaches are limited in their reliance on predefined forgery patterns. For instance, Face X-ray [23] assumes the presence of a blending region in the forged image, which could potentially curtail the effectiveness of the approach when generalized to novel and unseen forgeries. In addition, these methods consider the entire feature space when addressing the problem, which could be disrupted by irrelevant factors such as background [27] and identity [13].

To address the above challenges, we adopt the perspective of content and style [20] and formulate the problem of deepfake as an integration of two distinct components: content and fingerprint. The content in deepfake refers to elements, e.g., the background, identity, and facial appearance, which are not directly related to the forgery. In contrast, the fingerprint represents the traits that are related to the forgery. The challenge, then, becomes how to effectively disentangle these two components and use only the forgery-related fingerprint for detection.

Several recent studies [51, 18, 27] attempt to address the generalization problem through disentanglement techniques. However, limited generalization capability remains a challenge in many cases. One main reason is the over-reliance on method-specific patterns in most disentanglement methods, which only aim to eliminate the influence of content. However, these methods may still learn patterns that are unique to a specific forgery method, thereby limiting their generalization performance.

To address this issue, we propose a novel disentanglement framework that differs from existing approaches (See Fig. 1). Our framework prevents overfitting to both content and specific forgery patterns. To achieve this, we employ a multi-task disentanglement framework and a conditional decoder to disentangle the input into content and fingerprint components. Moreover, we introduce a contrastive regularization technique to disentangle the fingerprint features into specific and common features. The specific features represent method-specific forgeries, while the common features are shared across different forgery methods. In our approach, only the common features are utilized for detection, which improves the generalization ability of the model. To validate our idea, we conduct a t-SNE visualization [46] in Fig. 2, demonstrating that the baseline and our specific components actually learn method-specific texture, while our common components are able to capture the common features across forgeries. Furthermore, the content does not differentiate between real and fake images, as expected.

Our contributions are summarized as follows:

- We propose a novel multi-task disentanglement framework to address two main challenges that contribute to the generalization problem in deepfake detection: overfitting to irrelevant features and overfitting to method-specific textures. By uncovering common features, our framework aims to enhance the generalization ability of the model.

- We propose a conditional decoder that helps disentangle forgery-irrelevant and forgery features, as well as a contrastive regularization technique that facilitates the disentanglement of common and specific forgery features. By utilizing these technologies, we aim to achieve improved disentanglement.

- Extensive experiments show that our framework can outperform the performance of current state-of-the-art methods in unseen testing datasets, demonstrating its effectiveness in generalization.

2. Related Work

To date, deepfake detection can be broadly categorized into two types of tasks: image forgery detection [37, 23, 7] and video forgery detection [38, 16, 57]. This paper specifically focuses on detecting image forgery.

Classical Detection Methods. Conventional deepfake detectors [3, 34, 37] typically focus on developing optimal CNN architectures. However, these methods often overlook the details present in the frequency domain of fake images, such as compression artifacts. To this end, several works [36, 14, 22, 15] utilize frequency information to improve the performance of detectors. Other notable directions are focusing on some specific representations, i.e., forgery region location [33], neuron behaviors [49], optical flow [4], landmark geometric features [42], 3D decomposition [59], erasing technology [47], and attentional networks [10, 55, 48]. However, the generalization ability towards unseen forgery technologies of these conventional deepfake detectors is still limited.

Detection Methods toward Generalization. Deepfake detection poses a significant challenge in terms of generalization, where detectors perform poorly when training and testing on different data distributions. Despite this challenge, there is a limited amount of research in this area. One early method, FWA [25], leverages differences in resolution between forgery faces and backgrounds to detect deepfake. Recent works make significant progress in improving the generalization ability. Face X-ray [23] detects blending boundary artifacts, SPSL [28] proposes a frequency-based method by phase spectrum analysis, Lip-Forensics [16] leverages spatial-temporal networks to identify unnatural mouth movements, SRM [30] utilizes the
In the visualization, images generated by the four methods locate separately in the latent space, which reveals that the baseline Xception actually learns method-specific features, consistent with our forgery-specific module. This observation explains that Xception can mainly recognize specific types of forgeries and thus fail to generalize well to a broader range of forgeries. Additionally, as expected, the common module of our method captures the common forgery features across different methods, while the content module captures only forgery-irrelevant features.

Disentanglement Learning for Deepfake Detection. Disentanglement learning is a method that decomposes complex features into simpler, more narrowly defined variables and encodes them as separate dimensions with high discriminative power \cite{27}. In the field of deepfake detection, there are relatively few papers that are based on disentanglement learning. These works aim to separate forgery-irrelated and forgery-related features to extract forgery information from variations present in facial images. Hu et al. \cite{18} propose a disentanglement framework that separates features, only using the manipulation-related features for detection. Zhang et al. \cite{54} go further step by adding additional supervision to improve generalization ability. To ensure the independence of the disentangled features, Liang et al. \cite{27} ensure feature independence through content consistency and global representation contrastive constraints.

Despite these efforts to tackle the generalization problem through disentanglement learning, this challenge still exists because these methods only remove the influence of content. In some cases, these methods may still fail to achieve complete disentanglement of forgery features, resulting in overfitting to method-specific textures and thereby limiting their ability to generalize to other unseen forgeries.

3. Methods

3.1. Motivation

There are two main factors that contribute to the generalization problem in deepfake detection. Firstly, many detectors are prone to focus too much on content information that is not directly related to the forgery, i.e., the background, identity, and facial appearance. Secondly, different forgery techniques produce distinct forgery artifacts. These artifacts can be easily detected by a detector that is trained on a specific set of artifacts. However, detectors may be overfitted to one or more specific forgery technologies, leading to a lack of generalization to unseen forgeries. The second problem is often overlooked in previous works.

To address these issues, we propose a multi-task disentanglement learning framework to uncover common features for generalizable deepfake detection. Our framework aims to disentangle the input into the content, specific, and common forgery features. By only utilizing the common forgery features for detection, our framework can help improve the generalization ability of deepfake detectors and avoid the overfitting of both forgery-irrelated and method-specific features. Additionally, we introduce a conditional decoder and a contrastive regularization loss to further aid in disentanglement and enhance the generalization ability of the framework.
Decoder
Training Phase

Inference Phase

Decoder

Figure 3: The overview framework of our proposed method. 1) For the encoder (E), we utilize it to obtain three distinct components: content, specific fingerprint, and common fingerprint. 2) For the recombination module, we recombine the fingerprints and contents from different input images. 3) For the decoder (D), we take the fingerprint and content as inputs to generate corresponding reconstruction images. 4) For the classification, we obtain the prediction results of specific and common fingerprints by two different heads (H_s and H_c) to classify the forgery method and determine whether the image is real or fake, respectively.

Figure 4: The architecture of our decoder D, involves combining the fingerprint and content through AdaIN layers, which are then processed through multiple convolutional blocks along with upsampling layers (indicated as “Conv-Block” in the figure). The AdaIN layers are utilized twice during this process to fuse the fingerprint as a condition along with the content. Ultimately, the output of the final “Conv-Block” layer is decoded to reconstruct the image.

3.2. Disentanglement Framework

Our disentanglement framework, depicted in Fig. 3, consists of an encoder, a decoder, and two classification heads. The encoder comprises a content encoder and a fingerprint encoder that extract content and fingerprint features, respectively. While the two encoders share the same structure, they do not share parameters. The decoder includes multiple convolutional and upsampling layers that reconstruct the image by utilizing fingerprint features as a condition along with content features. The classifier consists of two different heads, one for learning method-specific textures and the other for learning generalizable features across different forgeries. More details about our encoder can be found in the supplementary material.

3.3. Architecture

Encoders. Our encoder processes a pair of images (x_0, x_1), where x_0 represents the fake image and x_1 represents the real image. The encoder E comprises a content encoder E_c and a fingerprint encoder E_f, extracting the content and forgery features, respectively. We apply the encoder to each pair to obtain the corresponding fingerprint and content features as follows:

\[ f^s_i, f^c_i, c_i = E(x_i), \]  

where \( i \in \{0, 1\} \) is the index of the image. Also, \( f^s_0, f^c_0, c_0 \) and \( f^s_1, f^c_1, c_1 \) are denoted by the specific fingerprint, common fingerprint, and content corresponding to each input image pair, respectively.
Decoders. Our decoder (See Fig. 4) reconstructs an image by utilizing its content and fingerprint through a series of upsampling and convolutional layers. Unlike other disentanglement-based deepfake detection frameworks [54, 51, 27] that linearly add forgery and content features for recombination, our decoder applies Adaptive Instance Normalization (AdaIN) [19] for improved reconstruction and decoding, inspired by stylization techniques [20]. The AdaIN aligns the mean and variance of the content code to match those of the fingerprint. The formula is written as:

$$\text{AdaIN}(c, f) = \sigma(f) \left( \frac{c - \mu(c)}{\sigma(c)} \right) + \mu(f),$$  

(2)

where $c$ and $f$ are the content and the style vectors of the image pair, respectively. The functions $\mu(\cdot)$ and $\sigma(\cdot)$ compute the mean and variance of the input.

3.4. Objective Function

To attain disentangled feature representation for detection, we design three distinct loss functions: two classification losses for common and specific forgery features, a contrastive regularization loss for similar and dissimilar image embeddings, and a reconstruction loss to ensure consistency between original and reconstructed images at the pixel level. These losses are combined in a weighted sum to create the overall loss function for training the framework.

Multi-Task Classification Loss. For classification loss, we propose two different losses of classification. First, we propose a binary classification loss $\mathcal{L}_{ce}$ computed by the cross-entropy for supervising the model to learn the common feature of different forgery methods:

$$\mathcal{L}_{ce}^s = \mathcal{L}_{ce}(H_s(f_i^s), y_i),$$  

(3)

where $\mathcal{L}_{ce}$ denotes the cross-entropy loss, $H_c$ is the head for the common forgery feature, which is implemented by several MLP layers. $y_i \in \{\text{fake}, \text{real}\}$ is the binary classification label. In addition, $\mathcal{L}_{ce}^s$ is proposed to learn the method-specific patterns by guiding the model to identify which forgery method is applied to the fake image:

$$\mathcal{L}_{ce}^s = \mathcal{L}_{ce}(H_s(f_i^s), y_i'),$$  

(4)

where $H_s$ is the head for specific forgery feature and $y_i' \in \{\text{real}, GAN_1, GAN_2, \cdots \}$ donates the label for identifying which instance belong to the image. Note that $H_c$ and $H_s$ share the same architecture but not share the parameters.

The multi-task classification loss enables the model to learn both method-specific textures and common features in different forgeries, enhancing the generalization ability of the model.

Contrastive Regularization Loss. The objective of contrastive regularization loss is to optimize the similarity and dissimilarity measurements between images. The contrastive regulation loss is formulated mathematically as:

$$\mathcal{L}_{con} = \max \left( |x_A - x_P|^2 - |x_A - x_N|^2 + \alpha, 0 \right),$$  

(5)

where $\alpha$ serves as a margin hyper-parameter. This method minimizes the Euclidean distance between an anchor image ($x_A$) and its similar counterpart ($x_P$), while simultaneously maximizing the gap between the anchor image and its dissimilar counterpart ($x_N$). For instance, if $x_A$ denotes common features of a genuine image, $x_P$ would represent common attributes of another real image, while $x_N$ signifies the attributes of a manipulated image.

For the common features, we compute the loss between real and fake images to encourage the model to learn a generalizable representation that across different forgeries. For the specific features, we compute the loss between images of the same forgery to encourage the model to learn method-specific textures for each forgery.

Reconstruction Loss. In general, there are two types of reconstruction in our framework: self-reconstruction and cross-reconstruction. For the self-reconstruction, the decoder $D$ is applied to the content and fingerprint encoded from the same image to reconstruct the corresponding image, and the formula is written as:

$$\mathcal{L}_{rec}^s = \|x_0 - D(f_0, c_0)\|_1 + \|x_1 - D(f_1, c_1)\|_1.$$  

(6)

For the cross-reconstruction, we consider the different combinations of fingerprint and content features encoded from the different images. Similarly, the formula of the cross-reconstruction loss is written as:

$$\mathcal{L}_{rec}^c = \|x_0 - D(f_0, c_0)\|_1 + \|x_1 - D(f_1, c_1)\|_1.$$  

(7)

Considering both the self-reconstruction and cross-reconstruction loss, the overall image reconstruction loss can be computed as follows:

$$\mathcal{L}_{rec} = \mathcal{L}_{rec}^s + \mathcal{L}_{rec}^c.$$  

(8)

The image reconstruction loss ensures that the reconstructed image and the original image are consistent at the pixel level. In addition, the two reconstruction losses enhance the disentanglement of features. The self-reconstruction loss penalizes the reconstruction errors by leveraging the latent features of the input image, while the cross-reconstruction loss penalizes the reconstruction errors using the forgery feature and the swapped content features.
Overall Loss. The final loss function of the training process is the weighted sum of the above loss functions.

\[
\mathcal{L} = \mathcal{L}_{cc} + \lambda_1 \mathcal{L}_{ce}^{s} + \lambda_2 \mathcal{L}_{rec} + \lambda_3 \mathcal{L}_{con},
\]

where \(\lambda_1, \lambda_2, \lambda_3\) are hyper-parameters for balancing the overall loss.

4. Experiments

4.1. Settings

Datasets. To evaluate the generalization ability of the proposed framework, our experiments are conducted on four large-scale benchmark databases: FaceForensics++ (FF++) [37], DeepFakeDetection (DFD) [11], Deepfake Detection Challenge (DFDC) [12], and CelebDF [26]. FF++ [37] is a large-scale database comprising more than 1.8 million forged images from 1000 pristine videos. Forged images are generated by four face manipulation algorithms using the same set of pristine videos, i.e., DeepFakes (DF) [1], Face2Face (F2F) [45], FaceSwap (FS) [2], and NeuralTexture (NT) [44]. To evaluate the generalization ability of our framework, we follow prior research works [23, 7] and conduct experiments on three widely used face-manipulated datasets, i.e., DFDC [12], CelebDF [26], and DFD [11]. Note that there are three versions of FF++ in terms of compression level, i.e., raw, lightly compressed (HQ), and heavily compressed (LQ). Since realistic forgeries often have a limited quality, the HQ and LQ versions are used in experiments. Following previous works [23, 7], the HQ version of FF++ is adopted by default. If any deviation from this default, it will be explicitly stated.

Implementation. We use a modified version of Xception [37] as the backbone network, with model parameters initialized by pre-training on ImageNet. Face extraction and alignment are performed using DLIB [39]. Following previous works [7], the aligned faces are resized to 256 × 256 for both the training and testing. We use the Adam [21] for optimization with the learning rate of 0.0002, and the batch size is fixed as 32. In the overall loss function in Eq. (9), we set \(\lambda_1\) to \(\lambda_3\) as 0.1, 0.3, 0.05 empirically. The margin \(\alpha\) in Eq. (5) is set to 3. We also apply some widely used data augmentations, i.e., image compression, horizontal flip, and random brightness contrast.

Evaluation Metrics. We report the Area Under Curve (AUC) metric to compare our proposed method with prior works, which is consistent with the evaluation approach adopted in many previous works [23, 36, 37, 30, 7]. The default evaluation metric employed is the AUC. We also report other metrics such as Accuracy (ACC), Average Precision (AP), and Equal Error Rate (EER) for a more comprehensive evaluation of our method. Please refer to our supplementary for more details.

4.2. Generalization Ability Evaluation

Comparison with competing methods. To assess the generalization capacity of our framework, we reproduce ten competing methods under consistent conditions for a comprehensive comparison: Xception [37], Face X-ray [23], F3Net [36], SRM [30], SPSL [28], RECCE [6], CORE [35], SLADD [7], and Liang et al. [27]. We use the provided codes of Xception, RECCE, SLADD, CORE, FWA, and SRM from the authors. We reimplement Face X-ray, F3Net, SPSL, and Liang et al. [27] rigorously following the companion paper’s instructions and train these models under the same settings.

We conduct this experiment by training the models on the FF++ [37] and then evaluate these models in DFD [11], DFDC [12], and CelebDF [26], respectively. This setting is challenging in generalization ability evaluation since the testing sets are collected from different sources and share much less similarity with the training set.

The results of the comparison between different methods are presented in Tab. 1, which shows the performance in terms of the AUC metric. It is evident that the proposed disentanglement framework and multi-task learning strategy lead to superior performance compared to other models in most cases, achieving the overall best results.

Liang et al. [27] proposes a disentanglement framework for content information removal, but their model is still prone to overfitting to method-specific patterns, leading to the limitation of the generalization. On the contrary, the disentanglement framework we proposed is designed to learn generalizable features across different forgeries by the multi-task learning strategy, thereby achieving improved generalization performance.

Face X-ray [23] and FWA [25] use blended artifacts in forgeries to achieve generalization. However, these two methods have limited generalization ability when the patterns in the training and testing datasets differ. This is because Face X-ray learns to identify the boundary patterns that are sensitive to the post-processing operations varying in different datasets. On the contrary, our proposed framework learns common representations that are not dependent on specific post-processing operations.

SRM [30], SPSL [28], and F3Net [36] utilize frequency components of images to distinguish between forgeries and pristine images. However, the experimental results show that their generalization performance is inferior to the proposed approach. This could be due to the fact that these frequency cues that are effective on the FF++ may not generalize to other datasets with different post-processing steps.

CORE [35], RECCE [6], SLADD [7] are recent detectors that focus on different detection algorithms: loss design, reconstruction learning, and adversarial training. However, these detectors could still be disrupted by unrelated factors such as race, gender, or identity because they
Table 1: Comparisons of generalization ability with competing methods implemented by ourselves. We use two different data configurations: “FF-ALL”, which includes all data generated by four forgeries, and “FF-wo-DF”, “FF-wo-F2F”, “FF-wo-FS”, and “FF-wo-NT”, which use the FF++ dataset but drop DF, F2F, FS, and NT, respectively. The best results are highlighted in bold font, while the second-best results are underlined.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DFDC</td>
<td>CelebDF</td>
<td>DFDC</td>
<td>CelebDF</td>
<td>DFDC</td>
<td>CelebDF</td>
<td>DFDC</td>
</tr>
<tr>
<td>Xception [37]</td>
<td>0.651</td>
<td>0.672</td>
<td>0.727</td>
<td>0.651</td>
<td>0.660</td>
<td>0.633</td>
<td>0.664</td>
</tr>
<tr>
<td>Liang et al. [27]</td>
<td>0.700</td>
<td>0.706</td>
<td>0.829</td>
<td>0.707</td>
<td>0.699</td>
<td>0.794</td>
<td>0.705</td>
</tr>
<tr>
<td>CORE [35]</td>
<td>0.658</td>
<td>0.708</td>
<td>0.917</td>
<td>0.630</td>
<td>0.644</td>
<td>0.807</td>
<td>0.671</td>
</tr>
<tr>
<td>RECC [6]</td>
<td>0.635</td>
<td>0.756</td>
<td>0.933</td>
<td>0.636</td>
<td>0.604</td>
<td>0.821</td>
<td>0.661</td>
</tr>
<tr>
<td>Face X-ray [3]</td>
<td>0.710</td>
<td>0.740</td>
<td>0.890</td>
<td>0.726</td>
<td>0.668</td>
<td>0.838</td>
<td>0.734</td>
</tr>
<tr>
<td>SLADD [7]</td>
<td>0.751</td>
<td>0.753</td>
<td>0.900</td>
<td>0.738</td>
<td>0.705</td>
<td>0.841</td>
<td>0.757</td>
</tr>
<tr>
<td>F3Net [36]</td>
<td>0.743</td>
<td>0.668</td>
<td>0.926</td>
<td>0.748</td>
<td>0.648</td>
<td>0.872</td>
<td>0.765</td>
</tr>
<tr>
<td>SRM [30]</td>
<td>0.771</td>
<td>0.770</td>
<td>0.915</td>
<td>0.743</td>
<td>0.746</td>
<td>0.874</td>
<td>0.745</td>
</tr>
<tr>
<td>SPSL [38]</td>
<td>0.742</td>
<td>0.787</td>
<td>0.927</td>
<td>0.749</td>
<td>0.753</td>
<td>0.898</td>
<td>0.759</td>
</tr>
<tr>
<td>Ours</td>
<td>0.850</td>
<td>0.824</td>
<td>0.945</td>
<td>0.767</td>
<td>0.749</td>
<td>0.870</td>
<td>0.765</td>
</tr>
</tbody>
</table>

Table 2: Comparison with state-of-the-art methods on CelebDF and DFDC. The results of other works are mainly cited from [7, 53, 50].

<table>
<thead>
<tr>
<th>Model</th>
<th>Training Set</th>
<th>CelebDF</th>
<th>DFDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-stream [58]</td>
<td>FF++</td>
<td>0.538</td>
<td>-</td>
</tr>
<tr>
<td>Meso4 [3]</td>
<td>Self-made</td>
<td>0.548</td>
<td>0.497</td>
</tr>
<tr>
<td>MesoInception [3]</td>
<td>Self-made</td>
<td>0.536</td>
<td>0.499</td>
</tr>
<tr>
<td>DSP-FWA [25]</td>
<td>FF++</td>
<td>0.646</td>
<td>0.646</td>
</tr>
<tr>
<td>VA-MLP [32]</td>
<td>FF++</td>
<td>0.550</td>
<td>-</td>
</tr>
<tr>
<td>Multi-task [53]</td>
<td>FF++</td>
<td>0.543</td>
<td>-</td>
</tr>
<tr>
<td>Headpose [32]</td>
<td>UADFV</td>
<td>0.546</td>
<td>-</td>
</tr>
<tr>
<td>Capsule [34]</td>
<td>FF++</td>
<td>0.575</td>
<td>0.575</td>
</tr>
<tr>
<td>SMIL [24]</td>
<td>FF++</td>
<td>0.563</td>
<td>0.563</td>
</tr>
<tr>
<td>Two-branch [31]</td>
<td>FF++</td>
<td>0.734</td>
<td>0.734</td>
</tr>
<tr>
<td>Schwarz et al. [40]</td>
<td>FF++</td>
<td>0.667</td>
<td>0.673</td>
</tr>
<tr>
<td>PEL [15]</td>
<td>FF++</td>
<td>0.692</td>
<td>0.633</td>
</tr>
<tr>
<td>MADD [55]</td>
<td>FF++</td>
<td>0.674</td>
<td>-</td>
</tr>
<tr>
<td>Local-relation [9]</td>
<td>FF++</td>
<td>0.783</td>
<td>0.765</td>
</tr>
<tr>
<td>CFFs [53]</td>
<td>FF++</td>
<td>0.742</td>
<td>0.721</td>
</tr>
<tr>
<td>Zhuang et al. [60]</td>
<td>FF++</td>
<td>0.728</td>
<td>-</td>
</tr>
<tr>
<td>SFDG [50]</td>
<td>FF++</td>
<td>0.758</td>
<td>0.736</td>
</tr>
<tr>
<td>Ours</td>
<td>FF++</td>
<td>0.824</td>
<td>0.805</td>
</tr>
</tbody>
</table>

Table 3: Comparison on FF++ with methods using disentanglement learning.

<table>
<thead>
<tr>
<th>Training</th>
<th>Method</th>
<th>CelebDF</th>
<th>DFDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF++</td>
<td>Xception [37]</td>
<td>0.683</td>
<td>0.672</td>
</tr>
<tr>
<td></td>
<td>Liang et al. [27]</td>
<td>0.714</td>
<td>0.706</td>
</tr>
<tr>
<td></td>
<td>Ours</td>
<td>0.833</td>
<td>0.824</td>
</tr>
</tbody>
</table>

Comparison with state-of-the-art methods. For disentanglement-based detection frameworks, we identify one prior work, Liang et al. [27], that shares similarities with our approach. Their framework aims to remove content information and introduces two modules to enhance the independence of disentangled features. To ensure a fair comparison, we carefully implement their framework by following the settings of the original paper, as it is not available as an open-source resource. We train the baseline Xception, Liang et al. [27], and ours on the FF++ and evaluate them on FF++ (LQ), CelebDF, DFDC, and DFDC. As reported in Tab. 3, we observe that Liang et al. [27] improve upon the baseline largely, demonstrating the essential of removing content information. Additionally, UCF outperforms Liang et al. [27] on all testing datasets, showing the efficacy of uncovering common features.

Comparison with state-of-the-art methods. We further evaluate our method against other state-of-the-art models. The results, as shown in Tab. 2, demonstrate the effective generalization ability of our framework as it outperforms other methods, achieving the best performance in terms of the AUC metric on both CelebDF and DFDC. The results of some methods are directly cited from [7, 53, 50]. Following a comprehensive evaluation against 27 state-of-the-art detectors (10 implemented in this study and 17 referenced), we demonstrate the robust generalization capability of our proposed framework. It is worth noting that both UCF and Zhuang et al. [60] aim to tackle the challenging issue of overfitting to method-specific artifacts. However, their technical methodologies are totally different (disentangle vs. adversarial learning). Actually, we offer a fresh and distinct solution to this problem. Moreover,
Table 4: Ablation study regarding the effectiveness of our disentanglement framework, multi-task learning strategy, and contrastive regularization loss. “D” and “M” represent our basic disentanglement framework and the multi-task learning module, respectively. “C” represents the contrastive learning module. Results in gray indicate the within-dataset performance.

<table>
<thead>
<tr>
<th>Training</th>
<th>Method</th>
<th>Testing AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FF++</td>
<td>CelebDF</td>
</tr>
<tr>
<td></td>
<td>Xception [37]</td>
<td>0.986</td>
</tr>
<tr>
<td></td>
<td>Xception + D</td>
<td>0.995</td>
</tr>
<tr>
<td></td>
<td>Xception + D + M</td>
<td>0.995</td>
</tr>
<tr>
<td></td>
<td>Xception + D + M + C</td>
<td>0.996</td>
</tr>
</tbody>
</table>

UCF (82.4%) significantly outperforms Zhuang et al. [60] (72.8%) on CelebDF in terms of AUC.

4.3. Ablation Study

Effects of our disentanglement framework and multi-task learning strategy. To evaluate the impact of the proposed disentanglement framework and multi-task learning strategy on generalization ability, we conduct an ablation study on several datasets. Specifically, we train all models on FF++ and evaluate their performance on FF++ [37], DFD [11], DFDC [12], and CelebDF [26]. The results are reported in Tab. 4 using the AUC metric. The evaluated variants include the baseline Xception, Xception with the proposed disentanglement framework (Xception + D), the proposed disentanglement framework with the multi-task learning strategy (Xception + D + M), and the multi-task disentanglement framework with the contrastive regularization (Xception + D + M + C).

Regarding the ablation study, we observed the following. Firstly, the four variants achieve relatively similar results on FF++ (within-dataset evaluation). Secondly, implementing the basic disentanglement framework leads to a significant improvement in DFD, DFDC, and CelebDF (cross-dataset evaluation), indicating the generalization ability is improved largely when applying the proposed disentanglement framework for the content information removal. Thirdly, the multi-task disentanglement outperforms the basic disentanglement, indicating that the multi-task learning strategy is effective in improving the generalization ability of the model. Finally, combining the proposed multi-task disentanglement with the contrastive regularization loss achieves the best results in both within-dataset and cross-dataset evaluations, supporting the effectiveness of each module.

Effects of our conditional decoder. In contrast to other disentanglement-based detection frameworks [54, 51, 27] that use linear addition to combine fingerprint and content features for recombination, our proposed decoder utilizes AdaIN [19] to incorporate the fingerprint as a condition with the content for improved reconstruction and decoding. To evaluate the impact of the conditional decoder on the generalization ability, we conduct an ablation study on the proposed framework with and without the conditional decoder. Results in Tab. 5 demonstrate that our proposed conditional decoder can achieve improved performance on both within- and cross-datasets, highlighting the importance of using AdaIN layers for reconstruction and decoding.

Comparison with binary classification results of different forgery features. To evaluate the effectiveness of the proposed multi-task learning strategy, binary classification results are compared based on the common, specific, and whole forgery features. Tab. 6 shows that the common features exhibit superior generalization performance compared to the specific features. The comparison of the common and whole forgery features reveals that the whole forgery features are not as effective as the common features, mainly due to the presence of specific features, which may lead to overfitting to method-specific textures.

Table 5: Ablation study regarding the effectiveness of the conditional decoder. “CD” represents that we use the conditional decoder for image reconstruction. Otherwise, we use the linearly add for combining the fingerprint and content. Results in gray indicate the within-dataset performance.

<table>
<thead>
<tr>
<th>Training</th>
<th>Method</th>
<th>Testing AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FF++</td>
<td>CelebDF</td>
</tr>
<tr>
<td></td>
<td>Ours</td>
<td>0.995</td>
</tr>
<tr>
<td></td>
<td>Ours + CD</td>
<td>0.996</td>
</tr>
</tbody>
</table>

Table 6: Comparison with binary classification results of different forgery features.

<table>
<thead>
<tr>
<th>Training</th>
<th>Method</th>
<th>Testing AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FF++(LQ)</td>
<td>CelebDF</td>
</tr>
<tr>
<td></td>
<td>Xception [37]</td>
<td>0.986</td>
</tr>
<tr>
<td></td>
<td>Specific Forgery</td>
<td>0.987</td>
</tr>
<tr>
<td></td>
<td>Whole Forgery</td>
<td>0.995</td>
</tr>
<tr>
<td></td>
<td>Common Forgery</td>
<td>0.996</td>
</tr>
</tbody>
</table>

Table 7: Comparing the performance of the baseline and our proposed framework using different backbones. The best result is highlighted in bold font. “Avg.” represents the average AUC for cross-datasets.

<table>
<thead>
<tr>
<th>Training</th>
<th>Method</th>
<th>Testing AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FF++(LQ)</td>
<td>CelebDF</td>
</tr>
<tr>
<td></td>
<td>Xception [37]</td>
<td>0.683</td>
</tr>
<tr>
<td></td>
<td>Ours (Xception)</td>
<td>0.833</td>
</tr>
<tr>
<td></td>
<td>ConvNext [29]</td>
<td>0.779</td>
</tr>
<tr>
<td></td>
<td>Ours (ConvNext)</td>
<td>0.845</td>
</tr>
</tbody>
</table>
Figure 5: Visualization of the reconstruction images during the training process.

Exploring Generalization performance of different backbone choices. In this section, we investigate the choice of backbone on the generalization ability of our proposed framework. We use Xception as the backbone in our previous experiments to align with other related works, but our multi-task framework is not limited to this choice. To evaluate the effectiveness of our framework with different backbones, we adopt a recent SOTA backbone ConvNeXt [29] and conduct an ablation study. The results of the ablation study, shown in Tab. 7, demonstrate that our proposed framework can largely improve the generalization performance of both Xception and ConvNeXt backbones. This suggests that our framework is effective and applicable to different backbone choices. Additionally, to further highlight the plug-and-play nature of our proposed framework, we extend its application to ResNet [17] and EfficientNet [43] backbones. More details can be accessed in our supplementary materials.

4.4. Visualization

Visual examples of reconstructed images. Within the framework we propose, the generation of reconstruction images occurs during the recombination phase of training. These images serve a pivotal role in ensuring the effective disentanglement of content and fingerprint features, as depicted in Fig. 5.

The content features within our framework are specifically designed to capture appearance, identity, gender, and other forgery-related features. In the visual examples of the reconstructed images (see Fig. 5), it is evident that the images sharing the same content code exhibit a marked similarity. This resemblance persists even when the fingerprint features, which represent unique identifiers separate from the content, are derived from other individuals. The observed similarity in the reconstructed images with identical content codes substantiates the efficacy of our framework in accurately isolating content features from other elements of the image. Contrary to the content features, the fingerprint features do not alter the content information of the original inputs. However, a close examination of the reconstructed images with the same content code but different fingerprint codes reveals subtle differences.

5. Conclusion

In this paper, we propose a novel disentanglement framework that can generalize well in unseen deepfake datasets. Our approach is grounded in the idea that a generalizable deepfake detector should be able to capture the generalizable features across different types of forgeries. To this end, we introduce a multi-task disentanglement framework to uncover the common features. Additionally, we also introduce a conditional decoder and a contrastive regularization loss to enhance the disentanglement process. In this manner, the model can avoid overfitting to forgery-irrelevant and method-specific forgery textures, leading to a more generalizable detector. To evaluate the effectiveness of our proposed method, we conduct extensive experiments on several benchmark datasets and compare our results against existing state-of-the-art methods. Overall, our proposed framework represents a promising step toward the development of more generalizable deepfake detectors.

Ethics Statement. All facial images utilized in this work are sourced from publicly available datasets and are appropriately attributed through proper citations. Our research adheres to strict ethical guidelines throughout the experimental process. There is no compromise on personal privacy during the experiments conducted in this work.

Acknowledgment. Baoyuan Wu was supported by the National Natural Science Foundation of China under grant No. 62076213, Shenzhen Science and Technology Program under the grants: No. RCYX20210609103057050, No. ZDSYS20211021111415025, No. GXWD20201231105722002-20200901175001001.
References


[54] Ke-Yue Zhang, Taiping Yao, Jian Zhang, Ying Tai, Shouhong Ding, Jilin Li, Feiyue Huang, Haichuan Song, and


