





Natural & Adversarial Bokeh Rendering via Circle-of-Confusion Predictive Network

Yihao Huang , Felix Juefei-Xu , *Member, IEEE*, Qing Guo[†] , *Member, IEEE*, Geguang Pu 
and Yang Liu , *Senior Member, IEEE*,

Abstract—Bokeh effect is a natural shallow depth-of-field phenomenon that blurs the out-of-focus part in photography. In recent years, a series of works have proposed automatic and realistic bokeh rendering methods for artistic and aesthetic purposes. They usually employ cutting-edge data-driven deep generative networks with complex training strategies and network architectures. However, these works neglect that the bokeh effect, as a real phenomenon, can inevitably affect the subsequent visual intelligent tasks like recognition, and their data-driven nature prevents them from studying the influence of bokeh-related physical parameters (*i.e.*, depth-of-the-field) on the intelligent tasks. To fill this gap, we study a totally new problem, *i.e.*, *natural & adversarial bokeh rendering*, which consists of two objectives: rendering realistic and natural bokeh and fooling the visual perception models (*i.e.*, bokeh-based adversarial attack). To this end, beyond the pure data-driven solution, we propose a hybrid alternative by taking the respective advantages of data-driven and physical-aware methods. Specifically, we propose the *circle-of-confusion predictive network (CoCNet)* by taking the all-in-focus image and depth image as inputs to estimate circle-of-confusion parameters for each pixel, which are employed to render the final image through a well-known physical model of bokeh. With the hybrid solution, our method could achieve more realistic rendering results with the naive training strategy and a much lighter network. Moreover, we propose the adversarial bokeh attack by fixing the CoCNet while optimizing the depth map w.r.t. the visual perception tasks. Then, we are able to study the vulnerability of deep neural networks according to the depth variations in the real world. The extensive experiments show that our method produces more realistic bokeh than the state-of-the-art methods while fooling the powerful deep neural networks with a high accuracy drop.

Index Terms—Bokeh Rendering, Circle-of-Confusion, Adversarial Attack

Geguang Pu is supported by National Key Research and Development Program (2020AAA0107800), and Shanghai Collaborative Innovation Center of Trusted Industry Internet Software. This research is supported by the National Research Foundation, Singapore, and DSO National Laboratories under the AI Singapore Programme (AISG Award No: AISG2-GC-2023-008), the A*STAR Centre for Frontier AI Research, the National Research Foundation, Singapore, and the Cyber Security Agency under its National Cybersecurity R&D Programme (NCRP25-P04-TAICeN), and NRF Investigatorship NRF-NRFI06-2020-0001. This work is also supported by NTU-DESAY SV Research Program under Grant 2018-0980. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore and Cyber Security Agency of Singapore.

Yihao Huang and Yang Liu are with Nanyang Technological University, Singapore. Felix Juefei-Xu is with New York University, USA. Qing Guo is with the Institute of High Performance Computing (IHPC) and Centre for Frontier AI Research (CFAR), Agency for Science, Technology and Research (A*STAR), Singapore. Geguang Pu is with 1) East China Normal University and 2) Shanghai Industrial Control Safety Innovation Technology Co., LTD, China. [†] Qing Guo is the corresponding author (tsingguo@ieee.org).

I. INTRODUCTION

In photography, the shallow depth-of-field (DoF) effect or the bokeh effect is an important technique to generate aesthetically pleasing photographs. The images with the bokeh effect draw the attention of the viewers by primarily blurring the out-of-focus parts of the images while keeping the focused parts sharp. This effect can wash out unnecessary image details such as cluttered backgrounds, which can save the viewers from the messy information of the images and emphasize the salient themes such as the foreground person or object of the images. There are mainly two ways to produce a bokeh effect, which is either generated optically or through computational photography methods. To physically and optically produce the bokeh effect, usually fast lenses with large apertures in tandem with high-end digital single-lens reflex (DSLR) cameras or the latest digital single-lens mirrorless (DSLM) cameras are needed. The high barrier of entry has limited this option largely to professionals. To benefit more people, the latest smartphone manufacturers have tried to enable a computational photography way of generating a realistic bokeh effect on consumer-level cell phone products, which strongly drives research in this direction.

In recent years, a lot of works [1]–[9] have been proposed and “AIM 2019 Challenge on Bokeh Effect Synthesis” competitions [10] have been organized to promote the development of computational photography-based bokeh effect synthesis. These methods usually employ data-driven deep generative networks with complex training strategies and network architectures. The state-of-the-art methods (*e.g.*, PyNET [1] and DMSHN [7]) are typical examples.

However, as a kind of common image style, the bokeh effect inevitably influences the subsequent visual tasks. To further study the relationship between the physical parameters of the bokeh effect with the visual intelligence tasks, we raise a new problem (*i.e.*, *natural & adversarial bokeh rendering*) which aims to generate natural and realistic bokeh effect and fool the visual perception model. It is obvious that pure data-driven methods can hardly support such research due to their physical-independent property. Thus we propose a hybrid bokeh synthesis network that is guided by the advantages of data and physical principles.

We first analyze the bokeh generation process of the camera and summarize the physical model of the bokeh. Then, by imitating the operation form as priori, we propose a novel *circle-of-confusion predictive network (CoCNet)* that takes the all-in-focus image and depth image as inputs to estimate



Fig. 1. In the left part shows the comparison between CoCNet (ours) and state-of-the-art method PyNET [1]. CoCNet has a smaller model size and needs less inference time based on a single Tesla V100 GPU. The right part shows the adversarial bokeh example generated by CoCNet. CoCNet-AdvBokeh successfully fools the ResNet50 model with the adversarial bokeh effect.

circle-of-confusion (CoC) parameters. The method is able to realistically synthesize the bokeh effect, with a simple training strategy and lightweight design. Specifically, the way of synthesis is implemented by fusing the all-in-focus image with learned templates. The templates are generated by filtering the all-in-focus image with specialized kernels predicted in the network, which simulates the physical rendering process by implicitly predicting the CoC for each pixel. Through experiments, we verify that our proposed method can adaptively estimate the kernels according to the image content and achieve comparable performance to the state-of-the-art methods with fewer model parameters (*i.e.*, less than $\frac{3}{4}$). In the case of simplifying the convolution channels of the model, CoCNet can achieve on-par performance to the state-of-the-art methods with fewer than merely $\frac{1}{5}$ parameters.

Due to the natural advantage and universality of bokeh in photos, as well as potential adverse effects on multifarious visual tasks, in this work, we also aim to reveal the vulnerabilities in various visual image understanding tasks with the help of CoCNet, with a newly proposed task termed **adversarial bokeh attack (AdvBokeh)**. The method embeds deceptive information into the bokeh generation procedure and produces a natural bokeh-like adversarial example without any human-noticeable noise artifacts by fixing the parameters of CoCNet while optimizing the depth map. Adversarial bokeh examples are shown in Fig. 1 on the rightmost panel. We validate the proposed method on a popular adversarial image classification dataset, *i.e.*, NeurIPS-2017 DEV, and show that the proposed method can penetrate four state-of-the-art (SOTA) image classification networks, *i.e.*, ResNet50, VGG, DenseNet, and MobileNetV2 with high success rates as well as high image quality. Moreover, the adversarially generated defocus blur images from the AdvBokeh can actually be exploited to enhance the performance of downstream tasks (*e.g.*, defocus deblurring system), which shows the versatility of the adversarial bokeh samples.

The contributions are summarized as follows:

- ❶ We raise a new computer vision problem (*i.e.*, natural & adversarial bokeh rendering) for investigation and propose *circle-of-confusion predictive network (CoCNet)* by combining the advantages of data-driven and physical-aware methods. It achieves on-par SOTA performance with a more lightweight design and a much simpler training strategy.
- ❷ We propose the depth-guided attack, *i.e.*, AdvBokeh for image classification tasks by tapping into the bokeh generation process via the proposed CoCNet. The generated adversarial bokeh images can be used to improve the performance of the SOTA defocus deblurring systems, *i.e.*, IFAN [11], demonstrating that the adversarial bokeh examples can further enhance downstream visual tasks.
- ❸ We compare the performance of CoCNet with the state-of-the-art methods (*i.e.*, PyNET, DMSHN, MPFNet, BRViT) on the popular EBB! bokeh generation dataset. The adversarial attack experiments are carried out on a popular adversarial image classification dataset (*i.e.*, NeurIPS-2017 DEV), showing that the proposed method can penetrate four classical image classification networks with high success rates as well as maintain high image quality. The adversarial examples obtained by AdvBokeh also exhibit a certain degree of transferability under black-box settings.

We introduce related works in Sec. II. In Sec. III, we use a lot of figures and formulas to illustrate the design of CoCNet and the implementation architecture. In Sec. IV, we propose how to generate a natural & adversarial bokeh effect with CoCNet. In Sec. V, we conduct quantitative and qualitative experiments to verify the effectiveness of our method. The conclusion of the paper is in Sec. VI.

Scope. Our research belongs to the image synthesis task in the multimedia domain. We raise a new image synthesis problem (*i.e.*, natural & adversarial bokeh rendering) for investigation. The research can help to reveal the vulnerabilities in various visual multimedia understanding tasks under bokeh rendering.

II. RELATED WORK

A. DoF Rendering

DoF rendering plays an important role in realistic image synthesis [12]–[15]. A number of works [16]–[20] have tried using ray tracing or light field rendering to synthesize realistic bokeh effect images. Most of these methods need accurate 3D scene information and are time-consuming.

To achieve a realistic bokeh effect, early works [21]–[23] first take a portrait as the target of bokeh effect rendering. However, the previous methods put emphasis on portrait photos, which neglects the bokeh effect generation for images in the wild. To expand the application domain of DoF rendering, recently researchers proposed a lot of works [1]–[9], [24]. Some of them [2], [3], [5], [6], [24] are starved of fine depth maps collected by the additional sensors or calculated by pretrained depth estimation network. Wang *et al.* [3] propose a neural network with a depth estimation module, a lens blur module, and a guided upsampling module to render the bokeh effect on high-resolution images.

Since depth estimation is runtime-intensive and not suitable for consumer-level phones. Thus the “AIM 2019 Challenge on Bokeh Effect Synthesis” competition [10] asks the participants to generate bokeh images with only one single frame. The recent works [1], [4], [7]–[9], [25]–[28] have tried to directly render the bokeh effect by a well-designed network without the help of the depth map. Dutta *et al.* [4] propose to fuse the all-in-focus image with a Gaussian-blurred version of it. However, Gaussian blur is physically different from the blur effect of bokeh and preparing the Gaussian-blurred version of an all-in-focus image is time-consuming. PyNET [1], DMSHN [7], MPFNet [25], and BRViT [29] achieve the state-of-the-art performance. Ignatov *et al.* [1] present a large-scale bokeh dataset named “Everything is Better with Bokeh!” (EBB!), which contains 5K shallow DoF image pairs captured using the Canon 7D DSLR. They propose PyNET-based architecture with multi-stage training to render the bokeh effect. Dutta *et al.* [7] proposes an end-to-end deep multi-scale hierarchical network (DMSHN) for the bokeh effect rendering of images captured from the monocular camera, also with multi-stage training. BRViT [29] uses an end-to-end pyramid ViT as the backbone for Bokeh rendering of images from a monocular camera. MPFNet [25] uses a self-supervised multi-scale pyramid fusion network to generate bokeh images. The pyramid architecture used by BRViT and MPFNet is complex and unwieldy. In summary, these bokeh rendering methods design complicated networks and need a time-consuming multi-stage training strategy to render the bokeh effect, which is not physically aware and efficient.

B. Unrestricted Attack

Adversarial attacks [30], [31] that generate L_p -norm perturbations have obvious noises and are now considered unrealistic. Recent works [32]–[35] have tried to put emphasis on generating unrestricted adversarial images, which will not raise the suspicion of the people. From this point of view, unrestricted adversarial images make more sense in practice. The attacks mainly focus on three categories: geometric transformation,

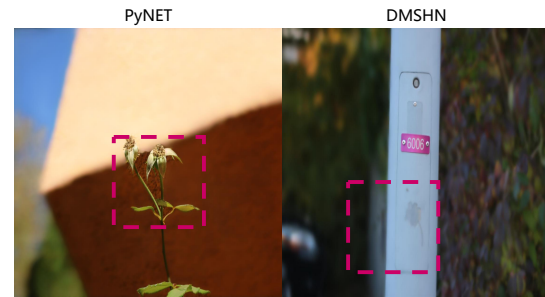


Fig. 2. There are noticeable artifacts from the bokeh rendering methods PyNET [1] and DMSHN [7].

color modification and photography effect. For geometric transformation, a few works exploit image deformations to construct adversarial attacks [33]. The images do not contain unnatural noise. However, image distortion is not natural when applied to images with straight edges. For color modification, some works have tried to do semantic adversarial attacks by modifying the color of the object in the image [32], [36]. However, the colors of some objects in the adversarial attacked images defy common sense and look very fake (*e.g.*, yellow river, purple tree, *etc.*). For photography effect, Guo *et al.* [34] propose an adversarial attack method that can generate visually motion-blurred adversarial examples, which mimics a type of photographic effect with high fidelity. However, the method cannot be extended to generate defocus blur.

III. BOKEH SYNTHESIS METHOD

In Sec. III-A, we introduce the motivation for designing a hybrid bokeh rendering network. To achieve this, in Sec. III-B, we infer the realistic bokeh imaging model based on the optical principle of a normal sensor. However, rendering that strictly adheres to the physical model is time-consuming, thus in Sec. III-C, we propose two time-efficient approximation strategies and design a lightweight bokeh synthesis network.

A. Motivation

Although existing bokeh effect rendering methods have achieved impressive photographic effects, the SOTA methods mainly adopt data-driven end-to-end networks with cumbersome architecture and complicated training strategies. For example, PyNET [1] designs a seven-level UNet-like network and replaces the skip-connection with diversified convolution modules. They need to go through seven stages of progressive training, confirming model parameters layer by layer, to get the final rendering model. With respect to DMSHN [7], the authors first design a three-level network with the encoder-decoder module on each level. Then they stack multiple three-level networks together to achieve the complete model. The training is a two-stage procedure with different losses (*i.e.*, L_1 and SSIM loss in the first stage, MS-SSIM loss in the second stage). Even with such a complex design, the rendered bokeh images still exhibit errors somehow (see Fig. 2).

Beyond the pure data-driven rendering methods, we think the hybrid schema which takes both the advantage of data-driven and physical-related priori is a more reasonable and

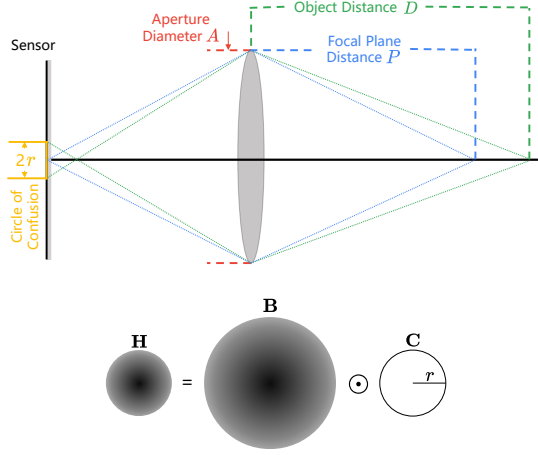


Fig. 3. Thin lens model and point spread function of Eq. (1) and (2).

promising approach. To this end, we refer to the physical process of bokeh rendering in normal sensors and try approximately simulating the process. We hope that the hybrid network design can help reduce the learning difficulty of the network, leading to a much lighter network and faster inference speed. With this hybrid solution, we are able to study the influence of bokeh-related physical parameters (*i.e.*, depth-of-the-field) on the downstream visual intelligence tasks. In the following sections, we first introduce the physical model of bokeh rendering (Sec. III-B) and then describe how we design the network to simulate it (Sec. III-C).

B. Bokeh Modeling with Sensors

1) *Preliminary knowledge:* Currently, the bokeh datasets are mainly captured by normal cameras. To simplify the optical calculation, we assume that the thickness of the lens is negligible. With the thin lens model, when a light source passes through the lens, it converges to a focal point on the image plane. If the light does not converge to a perfect focus, it will form a disk (*i.e.*, circle of confusion (CoC)). The radius of CoC can be approximated by the following formula

$$r = \frac{A}{2} \times \frac{f}{D} \times \frac{|D - P|}{P - f}, \quad (1)$$

which involves camera parameters focal length (f), distance of focal plane (P), aperture diameter (A), and object distance (D), *etc.* For a given dataset captured by a certain type of camera, the camera parameters are fixed when taking the bokeh images, and only the object distance D changes. Please see Fig. 3 for a pictorial illustration of Eq. (1)

The point spread function (PSF) \mathbf{H} of the view can be modeled as Hadamard product (*i.e.*, element-wise multiplication) ' \odot ' of a 2D Butterworth filter \mathbf{B} and a circular disk \mathbf{C} [37] with CoC's radius r ,

$$\mathbf{H} = \mathbf{B} \odot \mathbf{C}. \quad (2)$$

Here \mathbf{H} , \mathbf{B} , and \mathbf{C} are all related to the object distance D . Please see Fig. 3 for a pictorial illustration of Eq. (2). For each sublayer \mathbf{I}_m that contains pixels from the same depth of



Fig. 4. The pictorial illustration of Eq. (4).

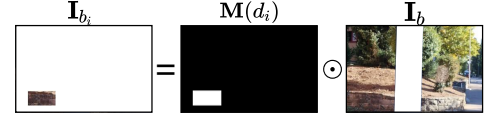


Fig. 5. The pictorial illustration of Eq. (5).

depth map w.r.t. the all-in-focus image \mathbf{I} , the blurred sublayer \mathbf{I}'_m can be modeled as the convolution ' $*$ ' of \mathbf{I}_m and its PSF,

$$\mathbf{I}'_m = \mathbf{I}_m * \mathbf{H}_m. \quad (3)$$

The bokeh image $\hat{\mathbf{I}}$ is the fusion of the blurred sublayers.

2) *Modeling:* Given an all-in-focus image $\mathbf{I} \in \mathbb{R}^{H \times W \times 3}$, the target is to obtain the bokeh image $\hat{\mathbf{I}} \in \mathbb{R}^{H \times W \times 3}$ corresponding to the all-in-focus image \mathbf{I} . Assume that the camera focuses on the foreground area and the all-in-focus image \mathbf{I} consists of the foreground image \mathbf{I}_f and background image \mathbf{I}_b (*i.e.*, $\mathbf{I} = \mathbf{I}_f + \mathbf{I}_b$). According to the property of bokeh (*i.e.*, the foreground remains the same), the bokeh image $\hat{\mathbf{I}}$ consists of the foreground image \mathbf{I}_f and the blurred background image \mathbf{I}'_b (*i.e.*, $\hat{\mathbf{I}} = \mathbf{I}_f + \mathbf{I}'_b$). Then we replace the \mathbf{I}_f with $\mathbf{I} - \mathbf{I}_b$ and get

$$\hat{\mathbf{I}} = \mathbf{I} + \mathbf{I}'_b - \mathbf{I}_b, \quad (4)$$

impelling the model to learn the residual between \mathbf{I} and $\hat{\mathbf{I}}$. Please see Fig. 4 for a pictorial illustration of Eq. (4). For a sublayer \mathbf{I}_{b_i} that contains pixels from the same depth (*i.e.*, d_i ($1 \leq i \leq N$, N represents the number of the discrete depth layers in the depth map w.r.t. background image)) of the depth map w.r.t. background image \mathbf{I}_b . Set $\mathbf{M}(d_i)$ as a binary mask in which describes whether the pixels of depth d_i are selected. \mathbf{I}_{b_i} is the Hadamard product of $\mathbf{M}(d_i) \in \mathbb{R}^{H \times W}$ and \mathbf{I}_b ,

$$\mathbf{I}_{b_i} = \mathbf{M}(d_i) \odot \mathbf{I}_b. \quad (5)$$

That is, $\mathbf{I}_b = \sum_{i=1}^N \mathbf{M}(d_i) \odot \mathbf{I}_b$. Please see Fig. 5 for a pictorial illustration of Eq. (5). The blurred background image \mathbf{I}'_b can be represented by blending (*i.e.*, $\mathcal{B}(\cdot)$) the blurred sublayers \mathbf{I}'_{b_i} (\mathbf{I}'_{b_i} is the blurred version of \mathbf{I}_{b_i}) together. Then Eq. (4) can be rewritten as

$$\hat{\mathbf{I}} = \mathbf{I} + \mathcal{B}(\mathbf{I}'_{b_i}) - \sum_{i=1}^N \mathbf{I}_{b_i}. \quad (6)$$

According to Eq. (2), \mathbf{I}'_{b_i} can be represented as the convolution of \mathbf{I}_{b_i} and its corresponding PSF (*i.e.*, $\mathbf{H}(d_i)$). Please see Fig. 6 for a pictorial illustration of Eq. (7).

$$\hat{\mathbf{I}} = \mathbf{I} + \mathcal{B}(\mathbf{I}_{b_i} * \mathbf{H}(d_i)) - \sum_{i=1}^N \mathbf{I}_{b_i}. \quad (7)$$

The function $\mathcal{B}(\cdot)$ depends on the processed masks $\mathbf{M}'(d_i)$ as the weight to fuse the blurred sublayers. The processed masks

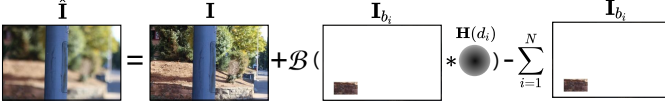


Fig. 6. The pictorial illustration of Eq. (7).

$M'(d_i)$ are generated by the convolution of mask and its PSF (i.e., $M(d_i) * H(d_i)$) [37]. Therefore,

$$\hat{\mathbf{I}} = \mathbf{I} + \sum_{i=1}^N (M(d_i) * H(d_i)) \odot (\mathbf{I}_{b_i} * H(d_i)) - \mathbf{I}_{b_i}. \quad (8)$$

In terms of a single pixel \mathbf{I}_{x_0, y_0} (of which the depth is d_0) in the location $[x_0, y_0]$ of \mathbf{I}_{b_i} , according to Eq. (8),

$$\hat{\mathbf{I}}_{x_0, y_0} = \mathbf{I}_{x_0, y_0} + u(d_0) \times \mathbf{I}_{x_0, y_0} * \mathbf{H}(d_0) - \mathbf{I}_{x_0, y_0}, \quad (9)$$

where $u(d_0)$ represents the value in the location $[x_0, y_0]$ of the processed mask $M'(d_0)$. \mathbf{I}_{x_0, y_0} can be replaced by $u(d_0) \times \mathbf{I}_{x_0, y_0} * \frac{\mathbf{R}}{u(d_0)}$, where \mathbf{R} is a kind of kernel which does not change the value of the pixel \mathbf{I}_{x_0, y_0} and has the same size as $\mathbf{H}(d_0)$. Then we can rewrite the Eq. (9) into

$$\hat{\mathbf{I}}_{x_0, y_0} = \mathbf{I}_{x_0, y_0} + u(d_0) \times \mathbf{I}_{x_0, y_0} * \mathbf{J}(d_0), \quad (10)$$

where $\mathbf{J}(d_0) = \mathbf{H}(d_0) - \frac{\mathbf{R}}{u(d_0)}$. Intuitively, we can find that for each pixel in the background image, its bokeh version is composed of its own value and a residual. The form of residual can be regarded as $a \times b \times c$. Obviously, the residual of pixels in the foreground image can also be written in this form (by simply setting a to 0). Therefore, the bokeh rendering model can be summarized as the general format

$$\hat{\mathbf{I}} = \mathbf{I} + \sum_{i=1}^N \mathbf{v}(d_i) \odot \mathbf{I} * \mathbf{L}(d_i), \quad (11)$$

where $\mathbf{v}(d_i) \in \mathbb{R}^{H \times W}$ is a weight map and $\mathbf{L}(d_i)$ means kernels (the number of $\mathbf{L}(d_i)$ is $H \times W$). The size of the kernels depends on the depth d_i .

If directly rendering the all-in-focus image with Eq. (11), there are two factors that lead to a huge computation problem, which is not convenient. ❶ The method needs to split the pixels into many sublayers (maybe up to several hundred) according to their depth. For each sublayer, a dedicated rendering operation is needed, which is time-consuming. ❷ For the pixels at deep depth, the size of the kernels is large, which makes convolution operation time-consuming.

To simplify the bokeh rendering, we solve the huge computation problem and improve the efficiency through approximation strategies with respect to the two factors. The details of the approximation and the architecture of our network are introduced in the next subsection.

C. Circle-of-confusion Predictive Network

1) *Approximation strategy.*: In pursuit of operating efficiency, we approximate the physical principle of bokeh rendering by simplifications.

For the problem of having too many sub-layers and large convolution kernel size, we propose the following solutions

respectively. To reduce the number of sublayers in the calculation, we propose to use finite templates to approximate the effect, as shown in Eq. (12). Here we utilize the idea of sparse coding to simulate a complex image by weighted fusion of a few templates. Please note that the formula form is the same as the Eq. (11), which guarantees the physical correlation of the approximation formula.

$$\hat{\mathbf{I}} = \mathbf{I} + \sum_{j=1}^Q \mathbf{w}'_j \odot \mathbf{I} * \mathbf{K}'_j. \quad (12)$$

The $\mathbf{w}'_j \in \mathbb{R}^{H \times W}$ is a weight map and \mathbf{K}'_j is a group of kernels. Q is the number of templates. In this paper, it is 5.

With regard to large kernel size, it is apparent that we inevitably need large convolution kernels to simulate the blur effect of distant objects. Thus we use the following formula to approximate Eq. (12). The $\mathbf{w}_j \in \mathbb{R}^{H \times W}$ is a weight map and \mathbf{K}_j is a group of kernels.

$$\hat{\mathbf{I}} = \mathbf{I} + \sum_{j=1}^Q \mathbf{w}_j \odot \mathcal{U}_j(\mathcal{D}_j(\mathbf{I}) * \mathbf{K}_j), \quad (13)$$

where $\mathcal{U}_j(\cdot)$ and $\mathcal{D}_j(\cdot)$ are upsampling/downsampling method. They will upsample/downsample the width/height of an image by 2^j . The main idea is to apply convolution kernels of the same size on images of different scales. Then, by scaling the images back to a uniform size with different ratios, the blur effect of different convolution kernel sizes can be simulated.

2) *Architecture of CoCNet*: To implement Eq. (13), we design a network (i.e., $\mathcal{T}(\cdot)$) which is based on an encoder-decoder architecture, as shown in Fig. 8. Since the Eq. (13) implicitly predicts circle-of-fusion for each pixel, thus we call the network circle-of-confusion predictive network (CoCNet).

$$\hat{\mathbf{I}} = \mathcal{T}(\tilde{\mathbf{I}}), \quad (14)$$

where $\tilde{\mathbf{I}}$ is the input of the network. It includes the all-in-focus image $\mathbf{I} \in \mathbb{R}^{H \times W \times 3}$ and the depth map $\mathbf{D}_{[0,1]} \in \mathbb{R}^{H \times W}$ of \mathbf{I} . Please note that the depth map is optional. As shown in Table I, the network without the depth map can also achieve state-of-the-art performance. The reason why we take it as the input is to maintain the formula consistency of natural/adversarial bokeh rendering methods. The encoder-decoder network consists of $2Q - 1$ basic module layers, in which the encoder has $Q - 1$ layers (from Enc_1 to Enc_{Q-1}) and the decoder has Q layers (from Dec_Q to Dec_1). The encoder layers are connected by downsampling and the decoder layers are connected by upsampling. There are skip connections between the encoder layer j and decoder layer j ($1 \leq j \leq Q - 1$). We assume that the feature map outputs of decoder layers are $\text{Dec}_j(\tilde{\mathbf{I}})$. The template $\mathbf{T}_j \in \mathbb{R}^{H \times W \times 3}$ is

$$\mathbf{T}_j = \mathcal{U}_j(\mathcal{D}_j(\mathbf{I}) * \varphi(\text{Dec}_{Q-j+1}(\tilde{\mathbf{I}}))), \quad (15)$$

where $\varphi(\cdot)$ represents the kernel prediction module. It will output $\frac{H}{2^j} \times \frac{W}{2^j}$ kernels, the width/height of each kernel is k . Please note that here we assume the number $\frac{H}{2^j}$ and $\frac{W}{2^j}$ are integers. For decimals, we can adjust the scaling flexibly.

We can achieve the weight map of each template by

$$\mathbf{w}_j = \mathcal{W}([\mathbf{I}, \mathbf{T}_1, \mathbf{T}_2, \dots, \mathbf{T}_Q, \text{Dec}_1(\tilde{\mathbf{I}})]), \quad (16)$$

$$\hat{\mathbf{I}} = \mathbf{I} + \sum_{i=1}^N \left(\left(\mathbf{M}(d_i) * \mathbf{H}(d_i) \right) \odot \left(\mathbf{I}_{b_i} * \mathbf{H}(d_i) \right) - \mathbf{I}_{b_i} \right)$$

Fig. 7. The pictorial illustration of Eq. (8).

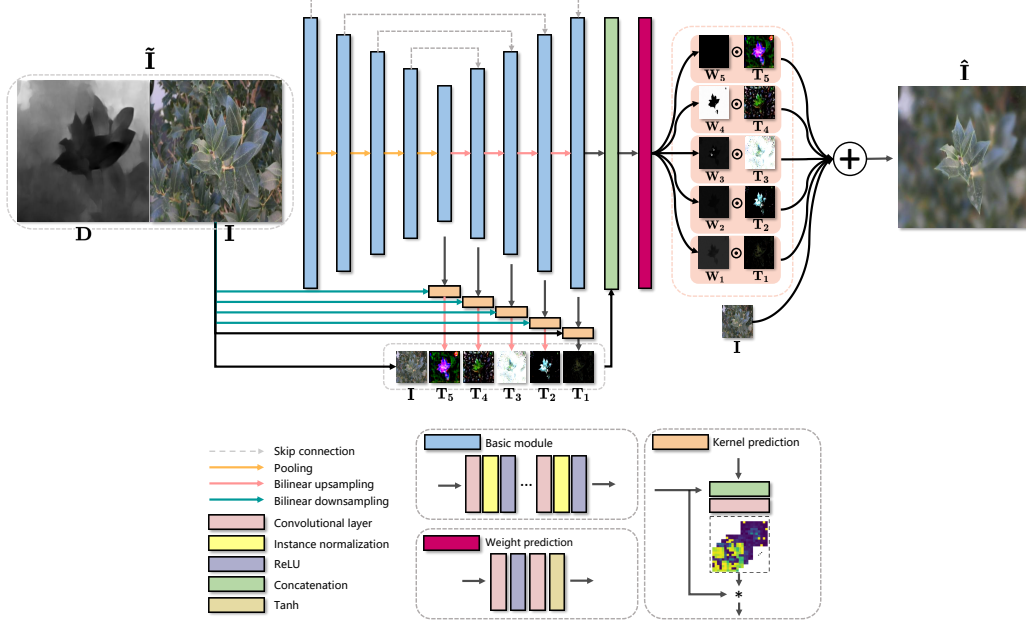


Fig. 8. Architectures and training pipeline of *circle-of-confusion predictive network (CoCNet)*. Please note the depth map \mathbf{D} is optional.

where $\mathcal{W}(\cdot)$ is the weight prediction module. Finally, the bokeh image $\hat{\mathbf{I}}$ can be achieved by

$$\hat{\mathbf{I}} = \mathbf{I} + \sum_{j=1}^Q \mathbf{w}_j \odot \mathbf{T}_j. \quad (17)$$

DBSI [4] may look similar to our method since it also fuses the all-in-focus image with templates (*i.e.*, Gaussian-blurred versions of the all-in-focus image). However, our method is fundamentally different from their approach since they do not follow the physical model. The Gaussian blur is physically different from the bokeh effect and they prepare the Gaussian-blurred version of the all-in-focus image manually. To be specific, they generate several Gaussian-blurred images of an all-in-focus image as templates. The kernel sizes of the Gaussian blur are manually set, which is cumbersome and lacks generality. Furthermore, the preparation procedure for the templates is time-consuming since they have to generate these Gaussian-blurred templates for each all-in-focus image. In contrast, the templates in our method are physical-aware and generated by the network automatically.

Limitation. Since our method generates templates to simulate the bokeh effect, the network may inevitably generate the bokeh effect, even for objects that are located close to the all-in-focus physical range. This is a potential limitation of our method.

IV. NATURAL & ADVERSARIAL BOKEH ON VISUAL TASK

Since the CoCNet follows the physical priori, it gives us the ability to study the influence of the natural bokeh effect on visual tasks. In Sec. IV-A, we study the influence of bokeh on image classification as an example. Furthermore, the bokeh effect may be maliciously exploited to attack visual tasks and cause harm to society. Thus in Sec. IV-B, we further propose three kinds of depth-guided adversarial bokeh attack methods as unrestricted attacks to reveal the extent of the harm.

A. Influence of Natural Bokeh

Image degradations may drop the performance of neural networks on the visual tasks [38]–[40]. Although the bokeh effect aims to produce aesthetically pleasing photos, it may come with some unexpected bad influences on visual tasks. Whether and how much it drops the performance of neural networks is an interesting and meaningful problem. Here we take the classical visual task (*i.e.*, image classification) as the target to show the influence of the natural bokeh effect.

To study the influence of the natural bokeh effect, there are two challenges. First, there are not enough all-in-focus and bokeh image pairs (*i.e.*, enough data) to support the study. Second, the existing bokeh datasets are not designed for classification tasks, thus leading to the lack of classification labels. To solve these two problems, we need a bokeh rendering method that can generate an unlimited number of natural

bokeh images from the labeled all-in-focus images. Since the CoCNet follows the physical priori and the generated bokeh images reflect the characteristics of natural bokeh, it is obvious that the proposed CoCNet is the rescue.

We conduct the experiments on the NeurIPS-2017 DEV dataset (*i.e.*, an ImageNet-like dataset) and on four classical CNNs (*i.e.*, ResNet50, VGG, DenseNet, and MobileNetV2). As shown in Table II, “aif” and “bokeh” in each group mean the all-in-focus images and corresponding bokeh images. We can find that the bokeh effect drops the classification performance of all four CNNs by an average of 7%. This demonstrates the minor aggressiveness of the bokeh effect.

B. Depth-guided Adversarial Bokeh Attack

Although natural bokeh has minor adverse effects on neural networks, some people may maliciously generate natural adversarial examples without any human-noticeable noise artifacts to attack the perception model. To fully study the influence of adversarial bokeh rendering, We further propose three kinds of depth-guided adversarial bokeh attacks with CoCNet and reveal the vulnerability of neural networks.

① In traditional restricted adversarial attacks, the methods usually add attack noise to the image. However, directly adding noise to the bokeh image violates the smoothness feature of the bokeh, which may arouse suspicion and raise the defense of the detection mechanism. It is better to apply unrestricted and non-suspicious attacks on the bokeh image by modifying the input of CoCNet (*i.e.*, $\tilde{\mathbf{I}}$). Then the calculated deceptive information is embedded into the aesthetical bokeh effect generation procedure, which is more dangerous to neural networks and more worthy of attention. In our attack method, we choose to modify the physical factors (*i.e.*, depth map) rather than the all-in-focus image to simulate the adversarial bokeh attack, which can better construct the relationship between the real-world physical factors and bokeh aggression.

Given a pretrained CNN (*i.e.*, $\phi(\cdot)$) for image classification task, an all-in-focus image \mathbf{I} and its depth map \mathbf{D} . We first propose to simply apply gradient-based attack (*i.e.*, “gda”) to achieve attacked depth map $\mathbf{D}^* = \mathbf{D} + \delta$ by optimizing the objective function

$$\delta = \arg \max_{\delta^*} \mathcal{J}(\phi(\mathcal{T}(\mathbf{I}, \mathbf{D} + \delta^*)), y),$$

$$\text{subject to } \|\delta^*\|_p \leq \epsilon, \quad (18)$$

where $\mathcal{J}(\cdot)$ denotes the cross-entropy loss function with y being the annotation of the all-in-focus image \mathbf{I} . By directly applying a gradient-based attack on the depth map, although the depth map is with noise, the rendered bokeh image looks natural. The method avoids adding suspicious noise to the bokeh image by transforming the noise in the depth map into the inconspicuous bokeh effect.

② Although the noise in the depth map is hidden and imperceptible during the bokeh generation process, we propose a smooth gradient-based attack method (*i.e.*, “sm-gda”) to further maintain the smoothness property of the depth map, which will lead to a more natural bokeh effect, as shown in Table II. In specific, we change the value of gradient $\nabla_{\mathbf{D}_{i,j}}$

($1 \leq i \leq H, 1 \leq j \leq W$) of depth map $\mathbf{D} \in \mathbb{R}^{H \times W}$ according to its neighbors. The number of neighbors used for reference is dependent on l , where l is the kernel size of the smooth function $\mathcal{S}(\cdot)$. In detail, the value $\nabla_{\mathbf{D}_{i,j}}$ is changed according to $\nabla_{\mathbf{D}_{i \pm (l/2), j \pm (l/2)}}$. We obtain the attacked depth map $\mathbf{D}^* = \mathbf{D} + \mathcal{S}(\delta, l)$ with the Eq. (18).

③ Furthermore, applying a gradient-based attack on the depth map ignores an important characteristic of the bokeh image (*i.e.*, the object in the focus region is clear). With an intuitive idea that the variation in the focus region attracts more attention than variation in a blurred region, we aim to remove the variation in the focus region and only apply a gradient-based attack on the background. We call this background-guided gradient-based attack (*i.e.*, “bg-gda”). We obtain the attacked depth map $\mathbf{D}^* = \mathbf{D} + \delta^* \odot \mathbf{BR}$ with the same objective as in Eq. (18). \mathbf{BR} is the background region (represented by a binary map) obtained by applying threshold on the depth map.

V. EXPERIMENTS

We verify the effectiveness of the method from three aspects: the bokeh effect and efficiency (Sec. V-C), the attack success rate (Sec. V-E), and the improvement to downstream tasks (Sec. V-F).

A. Target Model

We take four SOTA bokeh effect rendering methods (*i.e.*, DMSHN [7], PyNET [1], MPFNet [25], and BRViT [29]) as the baseline for bokeh effect comparison. The advantage of DMSHN is that the model is small enough to run on consumer-level phones (*e.g.*, Qualcomm Snapdragon 855+ processor, Adreno 640 GPU and 8GB RAM) with several seconds for an image. Though the DMSHN model is small, our model is smaller, which is introduced in Sec. V-C. To evaluate the influence of adversarial bokeh examples on CNNs, we take ResNet50, VGG, MobileNetV2, and DenseNet as the target model. For downstream tasks, we aim to improve the performance of the SOTA defocus deblurring method [11] with the adversarial bokeh examples.

B. Experimental Setup

a) *Datasets.*: There are several datasets involved in our experiment. Ignatov *et al.* [1] open-source the “Everything is Better with Bokeh!” (EBB!) dataset which was used in AIM 2020 Bokeh Effect Synthesis Challenge. The dataset contains 4,694 pairs of bokeh and bokeh-free images captured using a narrow aperture (f/16) and a high aperture (f/1.8). The resolution of images is around 1024×1536 pixels. We resized the images to 1024×1024 in our experiment. This dataset is used in the training (4,400) and testing (294) of the bokeh effect rendering network. We use the NeurIPS-2017 DEV dataset [41] as the testing dataset for the classification task, which contains 1,000 ImageNet-like images and is used by NIPS 2017 adversarial attacks and defenses competition. For downstream tasks, we use the dual-pixel defocus deblurring (DPDD) [42] dataset. The DPDD dataset provides 500 dual-pixel images captured by a Canon EOS 5D Mark IV.

TABLE I
COMPARISON BETWEEN CoCNet AND OTHER SOTA BOKEH EFFECT RENDERING METHODS. THE ABLATION STUDY RESULTS ARE ON THE RIGHT.

	MPFNet	BRViT	PyNET	DMSHN	DMSHN-os	CoCNet-b3	CoCNet-b2	CoCNet-b3-less	CoCNet-b2-less	CoCNet-b3- L_2	CoCNet-b3-dir	CoCNet-b3-depth
PSNR \uparrow	24.74	24.76	24.21	24.73	24.57	24.78	24.70	24.72	24.62	24.63	24.24	24.81
SSIM \uparrow	0.8806	0.8904	0.8593	0.8619	0.8558	0.8604	0.8603	0.8597	0.8579	0.8611	0.8507	0.8607
LPIPS \downarrow	0.0596	0.0509	0.0693	0.0601	0.0631	0.0625	0.0632	0.0635	0.0630	0.0639	0.0686	0.0624
Para.(M) \downarrow	6.12	123.14	47.5	10.84	10.84	7.34	5.18	1.91	1.37	7.34	7.07	7.61

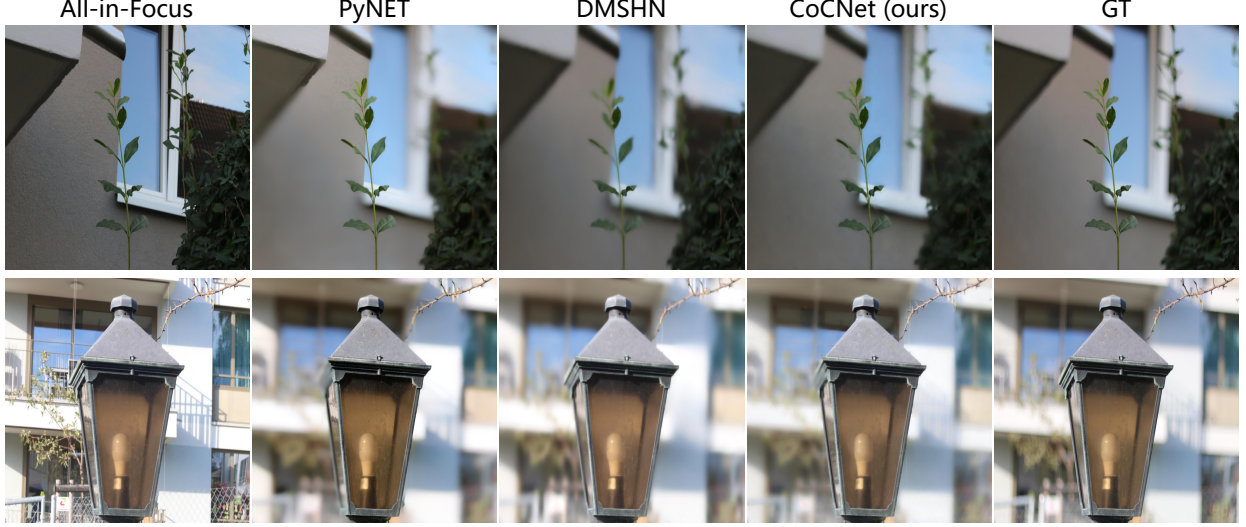


Fig. 9. Bokeh effect comparison. Our method has comparable results with the state-of-the-art bokeh rendering methods PyNET [1] and DMSHN [7].

b) Metrics.: To measure the similarity between prediction and ground truth bokeh images, we use peak signal-to-noise ratio (PSNR) [43], structural similarity (SSIM) [44] and learned perceptual image patch similarity (LPIPS) [45] as the metric. PSNR is the most commonly used measurement for the reconstruction quality of lossy compression. SSIM is used for measuring the similarity between two images. LPIPS is a metric that uses the features of neural networks to judge the similarity of images. Higher means more different and lower means more similar. We also use model parameters (Para.(M), M means million) as the metric to evaluate the model size.

c) Implementation details.: In CoCNet, as shown in Fig. 8, we set the layer numbers of the encoder-decoder to be 9 and the conv kernels in the encoder-decoder of CoCNet are of size 3 with striding 1 and padding 1. The group (*i.e.*, convolutional layer, instance normalization, ReLU) numbers in the basic module are 3 and the kernel size of the kernels in the kernel prediction module is (11,11). We use the Adam optimizer with $2e^{-4}$ learning rate and the batch size is 2. We also use Xavier initialization [46] on the weight of the network. The loss function used by us is L_1 and $SSIM$ loss, $L = L_1 + (1 - L_{SSIM})$. All the experiments were run on an Ubuntu 16.04 system with an Intel(R) Xeon(R) CPU E5-2699 with 196 GB of RAM, with an NVIDIA Tesla V100 GPU of 32G RAM.

C. Bokeh Effect

a) Quantitative and qualitative evaluation.: In this section, we compare our method to the current four state-of-the-art bokeh rendering methods (*i.e.*, PyNET [1], DMSHN [7], MPFNet [25] and BRViT [29]) that were tuned specifically

for the bokeh rendering. The quantitative results on comparing with state-of-the-art results and the ablation study are shown in Table I. In the first row, the “PyNET”, “DMSHN”, “MPFNet” and “BRViT” represent the official best-pretrained models respectively. “DMSHN-os” means using our training strategy, that is, training the DMSHN model with L_1 and L_{SSIM} loss in one stage. Because the models are trained without a depth map as input, we train “CoCNet-b3”, a model only using the all-in-focus image as input to keep the input information consistent with them. We find that “CoCNet-b3” has already achieved comparable performance with the state-of-the-art methods. From the table, we can find that the performance of CoCNet and DMSHN are significantly better than PyNET (higher similarity and fewer parameters). Compared with “DMSHN-os”, our model is better on all four metrics. Compared with the official model “DMSHN”, our model has comparable performance with fewer parameters. From the paper of DMSHN [7], we can find that the PSNR result of PyNET evaluated by them is 24.93. However, we have to claim that, there is a nonrigorous setting in the DMSHN paper that makes the PSNR result of PyNET in the DMSHN paper to be higher than it actually should be. The problem is from the dataset setting. The EBB! dataset has 4694, 200, and 200 pairs of images in its training, validation and test set. Since the ground truth images of validation and test set are not available yet, DMSHN uses part of the image pairs (294 pairs) of the training set as the test set. This means, in the setting of DMSHN, the training set has 4400 (4694-294=4400) pairs of images and the test set has 294 pairs of images. However, in the setting of PyNET paper, they use all the 4694 pairs of images as the training set. Thus testing the PyNET on the test

TABLE II

PERFORMANCE OF THE ATTACK METHOD ON FOUR MODELS AND THE NEURIPS-2017 DEV DATASET. THE SIMILARITY BETWEEN THE ATTACKED BOKEH IMAGES AND THE ALL-IN-FOCUS IMAGES. "AIF" MEANS ALL-IN-FOCUS IMAGE. "BOKEH" MEANS BOKEH IMAGE GENERATED BY CoCNet. "SM-GDA", "GDA" AND "BG-GDA" MEAN SMOOTH GRADIENT-BASED ATTACKED BOKEH IMAGE, GRADIENT-BASED ATTACKED BOKEH IMAGE AND BACKGROUND-GUIDED GRADIENT-BASED ATTACKED BOKEH IMAGE, RESPECTIVELY. THE **TOP-1** VALUE OF EACH METRIC IN EACH MODEL IS BOLDED.

	<i>ResNet50</i>					<i>VGG</i>					<i>DenseNet</i>					<i>MobileNetV2</i>				
	aif	bokeh	gda	sm-gda	bg-gda	aif	bokeh	gda	sm-gda	bg-gda	aif	bokeh	gda	sm-gda	bg-gda	aif	bokeh	gda	sm-gda	bg-gda
Acc. ↓	0.923	0.864	0.046	0.054	0.038	0.890	0.807	0.045	0.048	0.041	0.946	0.885	0.048	0.060	0.038	0.885	0.797	0.024	0.038	0.020
PSNR ↑	\	\	26.560	26.597	26.505	\	\	26.482	26.556	26.378	\	\	26.547	26.582	26.472	\	\	26.550	26.573	26.484
SSIM ↑	\	\	0.8846	0.8842	0.8832	\	\	0.8830	0.8850	0.8813	\	\	0.8842	0.8848	0.8828	\	\	0.8847	0.8846	0.8832
LPIPS ↓	\	\	0.0307	0.0302	0.0313	\	\	0.0318	0.0302	0.0327	\	\	0.0314	0.0303	0.0322	\	\	0.0305	0.0300	0.0311

TABLE III

ATTACK TRANSFERABILITY EVALUATION. THE IMAGES ARE OBTAINED BY ATTACKING ONE OF THE FOUR MODELS (*i.e.*, ResNet50, VGG, DenseNet AND MOBILENetV2) AND TESTING ON THE OTHER THREE. A LOWER VALUE MEANS BETTER TRANSFERABILITY.

	<i>ResNet50</i>			<i>VGG</i>			<i>DenseNet</i>			<i>MobileNetV2</i>		
	VGG	DenseNet	MobileNetV2	ResNet50	DenseNet	MobileNetV2	ResNet50	VGG	MobileNetV2	ResNet50	VGG	DenseNet
Acc. ↓	0.890	0.946	0.885	0.923	0.946	0.885	0.923	0.890	0.885	0.923	0.890	0.946
aif	0.807	0.885	0.797	0.864	0.885	0.797	0.864	0.807	0.797	0.864	0.807	0.885
bokeh	0.695	0.771	0.675	0.754	0.796	0.664	0.712	0.691	0.675	0.766	0.676	0.803
gda	0.714	0.798	0.717	0.789	0.832	0.711	0.759	0.714	0.720	0.786	0.704	0.831
sm-gda	0.684	0.744	0.669	0.731	0.789	0.648	0.684	0.684	0.668	0.758	0.665	0.800
bg-gda												

set of DMSHN is not fair since the PyNET has seen the test set of DMSHN in its training set. This is the reason why the PSNR result claimed in the DMSHN paper (they use the model pretrained by PyNET) is higher than the official value claimed by PyNET itself. In contrast, we additionally train the PyNET by ourselves and avoid the above unfair setting. For MPFNet, our CoCNet has similar metric values to it. For BRViT, our method is a bit worse in image quality but much smaller in model size. Please note that since MPFNet and BRViT do not provide pretrained model and codes respectively, the results are referred to their paper.

Ablation study. To study whether the model can be more lightweight, we adjust the optional variables of CoCNet to comprehensively demonstrate the model. ❶ The "CoCNet-b3" uses 3 groups in the basic module, thus we reduce it to 2 to see the influence on performance (*i.e.*, "CoCNet-b2"). We can find that it has a close performance to "DMSHN" with half of the model size. ❷ We also try to reduce the kernel number in the convolutional layers of the basic module to half, obtaining "CoCNet-b3-less" and "CoCNet-b2-less". We can find that the "CoCNet-b3-less" model has a close performance to "DMSHN" with only $\frac{1}{5}$ model size, which is extremely small. With respect to "CoCNet-b2-less", though its model size is the smallest in the table, its performance has an obvious gap to "DMSHN". According to this discovery, we plan to improve the model which has less than 2M parameters in future work.

We also try different loss functions, network architecture and input. ❸ For loss function, we try $L_2 + (1 - L_{SSIM})$ loss, named "CoCNet-b3- L_2 ". It is not as good as using $L_1 + (1 - L_{SSIM})$ loss. ❹ Furthermore, to verify the function of the kernel prediction module (used to simulate the priori of convolution operation in Eq. (13)), we directly concatenate the feature outputs of each decoder layer and the corresponding downsampled all-in-focus image, adding convolution layer to process them and obtain templates. This operation takes the same input as the kernel prediction module and also output templates. The main difference is the way processing input.



Fig. 10. Failure samples of CoCNet, DMSHN and PyNET.

That is, the kernel prediction module applies convolution on the downsampled all-in-focus image with the predicted kernel while this operation (similar to the operation in "PyNET" and "DMSHN") only takes the downsampled all-in-focus image as information and hopes the network can learn the bokeh effect by itself. The model is named "CoCNet-b3-dir". We can find that the performance is far away from using the priori-based architecture, which points out the effectiveness of priori. ❺ Although our network can learn the depth-related weight map and templates by itself, adding depth maps as input provides information more directly. This is why we add the depth map as input when introducing the network architecture in Sec. III-C. Furthermore, the adversarial bokeh attack method also needs to change the depth map. Thus we train the model with an estimated depth map as the complete model. The depth map is generated by Deeplens [3] and the corresponding model is "CoCNet-b3-depth". We achieve the same conclusion as [7], that is, the depth map boosts minimal to the performance. Considering the time decay in generating depth maps, it is not suitable for consumer-level phones.

D. Failure Samples

We carefully observe the bokeh image generated by CoCNet and find it is poor at generating the bokeh effect of spots. Please see Fig. 10, we can find that the CoCNet, DMSHN and PyNET are all poor at generating the bokeh effect of small spots, which needs further research.

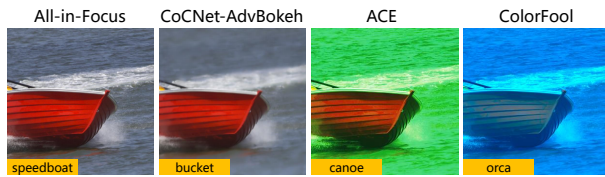


Fig. 11. Comparison of adversarial examples towards ResNet50 generated by our attack method with other state-of-the-art unrestricted attack methods (*i.e.*, ColorFool [32] and ACE [36]).

E. Adversarial Attack Accuracy

We apply gradient-based attack, smooth gradient-based attack and background-guided gradient-based attack on four pretrained models (ResNet50, VGG, MobileNetV2 and DenseNet). As shown in Table II, we demonstrate the accuracy of each model to the all-in-focus images (*i.e.*, “aif” for short), bokeh image generated by CoCNet (*i.e.*, “bokeh”), gradient-based attacked bokeh image (*i.e.*, “gda”), smooth gradient-based attacked bokeh image (*i.e.*, “sm-gda”), background-guided gradient-based attacked bokeh image (*i.e.*, “bg-gda”). Here we use the projected gradient descent [47] (PGD) to implement the gradient-based attack method in the bokeh rendering. For gradient-based attacked bokeh image, smooth gradient-based attacked bokeh image and background-guided gradient-based attacked bokeh image, the maximum perturbation for each pixel (*i.e.*, ϵ) is 0.0003, 0.008 and 0.0006, respectively. The number of attack iterations is 50. Compared with the natural degradation, our method significantly decreases the accuracy to less than 10% on all four models. With a similar decrease, we further calculate the image similarity between bokeh images and attacked bokeh images. We can find that “sm-gda” always achieves more similar results than “gda”. “bg-gda” is a little worse than them.

Transferability. To fully demonstrate the attack methods, we evaluate their transferability. As shown in Table III, the first row shows our attack methods (*i.e.*, gda, bg-gda, sm-gda). They all attack one of the four models (*i.e.*, ResNet50, VGG, DenseNet and MobileNetV2) and test on the other three models. The values are the test accuracy and the lower value means better transferability of the attack method. We can find that “bg-gda” has the best attack transferability. To summarize, the “sm-gda” and “bg-gda” have better attack performance and attack transferability than “gda” respectively, which shows the improvement on “gda” proposed by us is effective.

Comparison to other unrestricted attacks. There are some unrestricted attacks proposed to modify the semantics of the image. However, most of them lead to unnatural and absurd adversarial examples. As shown in Fig. 11, we can find that the adversarial bokeh examples proposed by “gda” look far more natural than the other two unrestricted attacks (*i.e.*, ColorFool and ACE) and less likely to arouse suspicion.

F. Defocus Deblurring Task Improvement

Every coin has two sides. Although the adversarial bokeh examples have a bad influence on visual tasks, they can be used to improve downstream tasks. Here we take the state-of-the-art defocus deblurring method IFAN [11] as an

TABLE IV
COMPARISON OF THE DEFOCUS DEBLURRING PERFORMANCE BETWEEN IFAN [11] AND OUR FINETUNED IFAN (*i.e.*, F-IFAN).

	PSNR \uparrow	SSIM \uparrow	LPIPS \downarrow
IFAN	25.36620	0.78885	0.21739
F-IFAN (ours)	25.38111	0.78887	0.21836

example. The training dataset used by them is DPDD. We use our method to generate adversarial attacked bokeh images according to the training images of DPDD. Then we collect the attacked images and original training images together as a kind of data augmentation to fine-tune the IFAN model. As shown in Table IV, we compare the IFAN model with our fine-tuned model (*i.e.*, “F-IFAN”) on the test dataset of DPDD. We can find that the deblurred images generated by our model achieve higher similarity with the ground truth all-in-focus images than IFAN, which shows the effectiveness of our attack method in improving the defocus deblurring task.

VI. CONCLUSIONS.

In this paper, we propose a circle-of-confusion predictive network (CoCNet) that follows the physical priori. Based on CoCNet, we are able to research the influence of natural & adversarial bokeh effects by revealing the vulnerability of the neural networks in visual understanding tasks. Furthermore, we demonstrate the positive usage of the attacked images as data augmentation to improve the downstream tasks. In the future, we aim to introduce GAN [48]–[50] into the framework for more realistic bokeh rendering.

REFERENCES

- [1] A. Ignatov, J. Patel, and R. Timofte, “Rendering natural camera bokeh effect with deep learning,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 2020, pp. 418–419.
- [2] L. Xiao, A. Kaplanyan, A. Fix, M. Chapman, and D. Lanman, “Deep-focus: Learned image synthesis for computational display,” in *ACM SIGGRAPH 2018 Talks*, 2018, pp. 1–2.
- [3] L. Wang, X. Shen, J. Zhang, O. Wang, Z. Lin, C.-Y. Hsieh, S. Kong, and H. Lu, “DeepLens: Shallow depth of field from a single image,” *arXiv preprint arXiv:1810.08100*, 2018.
- [4] S. Dutta, “Depth-aware blending of smoothed images for bokeh effect generation,” *Journal of Visual Communication and Image Representation*, vol. 77, p. 103089, 2021.
- [5] B. Busam, M. Hog, S. McDonagh, and G. Slabaugh, “Sterefo: Efficient image refocusing with stereo vision,” in *Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops*, 2019, pp. 0–0.
- [6] N. Wadhwa, R. Garg, D. E. Jacobs, B. E. Feldman, N. Kanazawa, R. Carroll, Y. Movshovitz-Attias, J. T. Barron, Y. Pritch, and M. Levoy, “Synthetic depth-of-field with a single-camera mobile phone,” *ACM Transactions on Graphics (ToG)*, vol. 37, no. 4, pp. 1–13, 2018.
- [7] S. Dutta, S. D. Das, N. A. Shah, and A. K. Tiwari, “Stacked deep multi-scale hierarchical network for fast bokeh effect rendering from a single image,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 2398–2407.
- [8] M. Qian, C. Qiao, J. Lin, Z. Guo, C. Li, C. Leng, and J. Cheng, “Bg-gan: Bokeh-glass generative adversarial network for rendering realistic bokeh,” in *European Conference on Computer Vision*. Springer, 2020, pp. 229–244.
- [9] X. Luo, J. Peng, K. Xian, Z. Wu, and Z. Cao, “Bokeh rendering from defocus estimation,” in *European Conference on Computer Vision*. Springer, 2020, pp. 245–261.

- [10] A. Ignatov, J. Patel, R. Timofte, B. Zheng, X. Ye, L. Huang, X. Tian, S. Dutta, K. Purohit, P. Kandula *et al.*, "Aim 2019 challenge on bokeh effect synthesis: Methods and results," in *2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)*. IEEE, 2019, pp. 3591–3598.
- [11] J. Lee, H. Son, J. Rim, S. Cho, and S. Lee, "Iterative filter adaptive network for single image defocus deblurring," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2021.
- [12] J. Xu, Y. Pu, R. Nie, D. Xu, Z. Zhao, and W. Qian, "Virtual try-on network with attribute transformation and local rendering," *IEEE Transactions on Multimedia*, vol. 23, pp. 2222–2234, 2021.
- [13] X. Zhang, Y. Song, Z. Li, and J. Jiang, "Pr-rl: Portrait relighting via deep reinforcement learning," *IEEE Transactions on Multimedia*, vol. 24, pp. 3240–3255, 2021.
- [14] Q. Meng, S. Zhang, Z. Li, C. Wang, W. Zhang, and Q. Huang, "Automatic shadow generation via exposure fusion," *IEEE Transactions on Multimedia*, 2023.
- [15] R. Wan, B. Shi, H. Li, Y. Hong, L.-Y. Duan, and A. C. Kot, "Benchmarking single-image reflection removal algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 2, pp. 1424–1441, 2022.
- [16] P. Haeblerli and K. Akeley, "The accumulation buffer: Hardware support for high-quality rendering," *ACM SIGGRAPH computer graphics*, vol. 24, no. 4, pp. 309–318, 1990.
- [17] S. Lee, E. Eisemann, and H.-P. Seidel, "Real-time lens blur effects and focus control," *ACM Transactions on Graphics (TOG)*, vol. 29, no. 4, pp. 1–7, 2010.
- [18] C. Soler, K. Subr, F. Durand, N. Holzschuch, and F. Sillion, "Fourier depth of field," *ACM Transactions on Graphics (TOG)*, vol. 28, no. 2, pp. 1–12, 2009.
- [19] J. Wu, C. Zheng, X. Hu, Y. Wang, and L. Zhang, "Realistic rendering of bokeh effect based on optical aberrations," *The Visual Computer*, vol. 26, no. 6, pp. 555–563, 2010.
- [20] X. Yu, R. Wang, and J. Yu, "Real-time depth of field rendering via dynamic light field generation and filtering," *Computer Graphics Forum*, vol. 29, no. 7, pp. 2099–2107, 2010.
- [21] X. Shen, X. Tao, H. Gao, C. Zhou, and J. Jia, "Deep automatic portrait matting," in *European conference on computer vision*. Springer, 2016, pp. 92–107.
- [22] X. Shen, A. Hertzmann, J. Jia, S. Paris, B. Price, E. Shechtman, and I. Sachs, "Automatic portrait segmentation for image stylization," *Computer Graphics Forum*, vol. 35, no. 2, pp. 93–102, 2016.
- [23] X. Xu, D. Sun, S. Liu, W. Ren, Y.-J. Zhang, M.-H. Yang, and J. Sun, "Rendering portraits from monocular camera and beyond," in *Proceedings of the European Conference on Computer Vision (ECCV)*, 2018, pp. 35–50.
- [24] K. Purohit, M. Suin, P. Kandula, and R. Ambasamudram, "Depth-guided dense dynamic filtering network for bokeh effect rendering," in *2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)*. IEEE, 2019, pp. 3417–3426.
- [25] Z. Wang, A. Jiang, C. Zhang, H. Li, and B. Liu, "Self-supervised multi-scale pyramid fusion networks for realistic bokeh effect rendering," *Journal of Visual Communication and Image Representation*, vol. 87, p. 103580, 2022.
- [26] T. Seizinger, M. V. Conde, M. Kolmet, T. E. Bishop, and R. Timofte, "Efficient multi-lens bokeh effect rendering and transformation," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 1633–1642.
- [27] Z. Yang, W. Lian, and S. Lai, "Bokehormot: Transforming bokeh effect with image transformer and lens metadata embedding," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 1542–1550.
- [28] Y. Jeong, S. Y. Baek, Y. Seok, G. B. Lee, and S. Lee, "Real-time dynamic bokeh rendering with efficient look-up table sampling," *IEEE Transactions on Visualization and Computer Graphics*, vol. 28, no. 2, pp. 1373–1384, 2020.
- [29] H. Nagasubramaniam and R. Younes, "Bokeh effect rendering with vision transformers," 2022.
- [30] S. Zhang, D. Zuo, Y. Yang, and X. Zhang, "A transferable adversarial belief attack with salient region perturbation restriction," *IEEE Transactions on Multimedia*, 2022.
- [31] C. Wan, F. Huang, and X. Zhao, "Average gradient-based adversarial attack," *IEEE Transactions on Multimedia*, 2023.
- [32] A. S. Shamsabadi, R. Sanchez-Matilla, and A. Cavallaro, "Colorfool: Semantic adversarial colorization," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 1151–1160.
- [33] L. Engstrom, B. Tran, D. Tsipras, L. Schmidt, and A. Madry, "Exploring the landscape of spatial robustness," in *International Conference on Machine Learning*. PMLR, 2019, pp. 1802–1811.
- [34] Q. Guo, F. Juefei-Xu, X. Xie, L. Ma, J. Wang, B. Yu, W. Feng, and Y. Liu, "Watch out! motion is blurring the vision of your deep neural networks," *arXiv preprint arXiv:2002.03500*, 2020.
- [35] Y. Cheng, Q. Guo, F. Juefei-Xu, S.-W. Lin, W. Feng, W. Lin, and Y. Liu, "Pasadena: Perceptually aware and stealthy adversarial denoise attack," *IEEE Transactions on Multimedia*, vol. 24, pp. 3807–3822, 2021.
- [36] Z. Zhao, Z. Liu, and M. Larson, "Adversarial color enhancement: Generating unrestricted adversarial images by optimizing a color filter," *arXiv preprint arXiv:2002.01008*, 2020.
- [37] A. Abuolaim, M. Delbracio, D. Kelly, M. S. Brown, and P. Milanfar, "Learning to reduce defocus blur by realistically modeling dual-pixel data," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2021, pp. 2289–2298.
- [38] K. Endo, M. Tanaka, and M. Okutomi, "Classifying degraded images over various levels of degradation," in *2020 IEEE International Conference on Image Processing (ICIP)*. IEEE, 2020, pp. 1691–1695.
- [39] N. H. Thao, O. Soloviev, J. Noom, and M. Verhaegen, "Nonuniform defocus removal for image classification," *arXiv preprint arXiv:2106.13864*, 2021.
- [40] Y. Pei, Y. Huang, Q. Zou, X. Zhang, and S. Wang, "Effects of image degradation and degradation removal to cnn-based image classification," *IEEE transactions on pattern analysis and machine intelligence*, 2019.
- [41] A. Kurakin, I. Goodfellow, S. Bengio, Y. Dong, F. Liao, M. Liang, T. Pang, J. Zhu, X. Hu, C. Xie *et al.*, "Adversarial attacks and defences competition," in *The NIPS'17 Competition: Building Intelligent Systems*. Springer, 2018, pp. 195–231.
- [42] A. Abuolaim and M. S. Brown, "Defocus deblurring using dual-pixel data," in *Computer Vision—ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part X 16*. Springer, 2020, pp. 111–126.
- [43] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, no. 4, pp. 600–612, 2004.
- [44] A. Hore and D. Ziou, "Image quality metrics: Psnr vs. ssim," in *2010 20th international conference on pattern recognition*. IEEE, 2010, pp. 2366–2369.
- [45] R. Zhang, P. Isola, A. A. Efros, E. Shechtman, and O. Wang, "The unreasonable effectiveness of deep features as a perceptual metric," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 586–595.
- [46] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proceedings of the thirteenth international conference on artificial intelligence and statistics*. JMLR Workshop and Conference Proceedings, 2010, pp. 249–256.
- [47] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," *arXiv preprint arXiv:1706.06083*, 2017.
- [48] H. Emami, M. M. Aliabadi, M. Dong, and R. B. Chinnam, "Spa-gan: Spatial attention gan for image-to-image translation," *IEEE Transactions on Multimedia*, vol. 23, pp. 391–401, 2020.
- [49] H. Tan, B. Yin, K. Wei, X. Liu, and X. Li, "Alr-gan: Adaptive layout refinement for text-to-image synthesis," *IEEE Transactions on Multimedia*, 2023.
- [50] J. Zhang, L. Jiao, W. Ma, F. Liu, X. Liu, L. Li, P. Chen, and S. Yang, "Transformer based conditional gan for multimodal image fusion," *IEEE Transactions on Multimedia*, 2023.



Yihao Huang received the B.S. degree and Ph.D. degree in Software Engineering Institute, East China Normal University, China in 2017 and 2022. He is currently a research fellow with Nanyang Technological University, where he works on robust 3D perception. He is the recipient of the Best Paper Award in the ECCV 2022 AROW workshop. His research interests include computer vision and AI security, especially adversarial attacks and generative AI.



Felix Juefei-Xu (Member, IEEE) received the Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University (CMU), Pittsburgh, PA, USA. Prior to that, he received the M.S. degree in Electrical and Computer Engineering and the M.S. degree in Machine Learning from CMU, and the B.S. degree in Electronic Engineering from Shanghai Jiao Tong University (SJTU), Shanghai, China. Currently, he is a Research Scientist with GenAI at Meta, based in New York City, where he works on robust perception and efficient learning

problems in the domain of generative AI. He is also affiliated with New York University as an Adjunct Professor. Previously, he was a Research Scientist with Alibaba Group, based in Sunnyvale, CA. He was the recipient of multiple best/distinguished paper awards, including IJCB 2011, BTAS 2015 and 2016, ASE 2018, and ACCV 2018.



Qing Guo received his Ph.D. degree in computer application technology from the School of Computer Science and Technology, Tianjin University, China. He is currently a senior research scientist and principal investigator (PI) at the Center for Frontier AI Research (CFAR), A*STAR in Singapore. He is also an adjunct assistant professor at the National University of Singapore (NUS), and senior PC member of AAAI. Before that, he was a Wallenberg-NTU Presidential Postdoctoral Fellow with the Nanyang Technological University, Singapore. His research

interests include computer vision, AI security, and image processing. He is a member of IEEE.



Geguang Pu is a Professor in Software Engineering Institute, East China Normal University. His research interests include program testing and reliable AI system. He served as PC member for more than 20 international conference committees. He has published over 100 publications on the topics of software engineering and system verification (including ICSE, FSE, ASE, CAV, etc). He completed his Ph.D. in Mathematics at Peking University in 2005, and received a B.S. in Mathematics from Wuhan University in 2000.



Yang Liu graduated in 2005 with a Bachelor of Computing (Honours) in the National University of Singapore (NUS). In 2010, he obtained his Ph.D. and started his post-doctoral work in NUS and MIT. In 2012, he joined Nanyang Technological University (NTU), and currently is a full professor and Director of the cybersecurity lab in NTU. Dr. Liu specializes in software engineering, cybersecurity and artificial intelligence. His research has bridged the gap between the theory and practical usage of program analysis, data analysis and AI to evaluate the design

and implementation of software for high assurance and security. By now, he has more than 400 publications in top tier conferences and journals. He has received a number of prestigious awards including MSRA Fellowship, TRF Fellowship, Nanyang Assistant Professor, Tan Chin Tuan Fellowship, Nanyang Research Award 2019, ACM Distinguished Speaker, NRF Investigatorship, and 15 best paper awards and one most influence system award in top software engineering conferences like ASE, FSE and ICSE.