ABCNet: Real-time Scene Text Spotting with Adaptive Bezier-Curve Network*

Yuliang Liu[‡†], Hao Chen[†], Chunhua Shen[†], Tong He[†], Lianwen Jin[‡], Liangwei Wang[◇]
[‡]South China University of Technology [†]University of Adelaide, Australia [◇]Huawei Noah's Ark Lab

Abstract

Scene text detection and recognition has received increasing research attention. Existing methods can be roughly categorized into two groups: character-based and segmentation-based. These methods either are costly for character annotation or need to maintain a complex pipeline, which is often not suitable for real-time applications. Here we address the problem by proposing the Adaptive Bezier-Curve Network (ABCNet). Our contributions are three-fold: 1) For the first time, we adaptively fit arbitrarily-shaped text by a parameterized Bezier curve. 2) We design a novel BezierAlign layer for extracting accurate convolution features of a text instance with arbitrary shapes, significantly improving the precision compared with previous methods. 3) Compared with standard bounding box detection, our Bezier curve detection introduces negligible computation overhead, resulting in superiority of our method in both efficiency and accuracy.

Experiments on arbitrarily-shaped benchmark datasets, namely Total-Text and CTW1500, demonstrate that ABCNet achieves state-of-the-art accuracy, meanwhile significantly improving the speed. In particular, on Total-Text, our real-time version is over 10 times faster than recent state-of-the-art methods with a competitive recognition accuracy.

Code is available in the package AdelaiDet.

(a) Segmentation-based method. (b) Our proposed ABCNet.

Figure 1. Segmentation-based results are easily affected by nearby text. The nonparametric non-structured segmentation results make them very difficult to align features for the subsequent recognition branch. Segmentation-based results usually need complex post-processing, hampering efficiency. Benefiting from the parameterized Bezier curve representation, our ABCNet can produce structured detection regions and thus the BezierAlign sampling process can be used for naturally connecting the recognition branch.

1. Introduction

Scene text detection and recognition has received increasing attention due to its numerous applications in computer vision. Despite tremendous progress has been made recently [10, 41, 27, 35, 26, 42], detecting and recognizing text in the wild remains largely unsolved due to its diversity patterns in sizes, aspect ratios, font styles, perspective distortion, and shapes. Although the emergence of deep learning has significantly improved the performance of the task of scene text spotting, current methods still exist a considerable gap for real-world applications, especially in terms of efficiency.

Recently, many end-to-end methods [30, 36, 33, 23, 43, 20] have significantly improved the performance of arbitrarily-shaped scene text spotting. However, these methods either use segmentation-based approaches that maintain a complex pipeline or require a large amount of expensive character-level annotations. In addition, almost all of these methods are slow in inference, hampering the deployment to real-time applications. Thus, our motivation is to design a *simple yet effective* end-to-end framework for spotting oriented or curved scene text in images [5, 26], which ensures fast inference time while achieving an *on par* or even better performance compared with state-of-the-art

*YL and HC contributed equally to this work. YL's contribution was made when visiting The University of Adelaide. CS is the corresponding author, e-mail: chunhua.shen@adelaide.edu.au

The Evolution of Offensive Cyberattacks and Defensive Cybersecurity Operations

2

Innovation in offensive and defensive military technologies and tactics has been a constant, especially during the past two centuries. Wars put these innovations to new tests. While the "fog of war" makes it more difficult to assess the relative strength of offensive and defensive capabilities, it also creates greater urgency for doing so. The war in Ukraine is no exception, including for cyberattacks and cybersecurity protection.

It's perhaps helpful to start with a historical analogy that is well understood. The Battle of Britain in 1940 pitted the use of an offensive technology—the bomber—against the defensive use of two other technologies, more advanced fighters, and the use of radar. The radar waves were invisible to the naked eye, and their widespread use was unknown to the public during the battle itself. But radar was indispensable in enabling the Royal Air Force to detect the oncoming bombers and direct fighters to combat them. While bombers succeeded in dropping bombs on England, they failed strategically in establishing the air supremacy needed to support an invasion.

This history shares some important similarities with the current day. The war in Ukraine has pitted offensive cyberattacks that are invisible to the naked eye against advances in cybersecurity technologies and operations. Like the bombers of 1940, some of the cyberattacks have succeeded in reaching and disabling their targets. But at a broader level, so far these attacks have failed strategically in disabling Ukraine's defenses. While part of the reason lies in the disbursement of Ukrainian digital operations into the cloud, discussed above, another reason has been the overall ability of cyber defenses to successfully defeat these attacks.

It's important to take note of the destructive cyber tactics the Russian military has deployed in Ukraine. These have three facets. The first aspect, which is also common to ransomware and nation-state cyber espionage, involves targeted phishing and similar efforts to enter a computer network. This tactic reflects the determination, sophistication, and persistence long observed across the cyber activities of Russia's intelligence community and military. The second involves the planting of "wiper" malware designed to "wipe" computer hard disks and destroy all their data. And the third has involved software architecture that is designed to replicate or spread this malware to other computers across a network domain, such as the network of an entire government ministry.