ENHANCING TEXT RECOGNITION ON TOR DARKNET IMAGES

Pablo Blanco-Medina\textsuperscript{1,2}, Eduardo Fidalgo\textsuperscript{1,2}, Enrique Alegre\textsuperscript{1,2}, Mhd Wesam Al-Nabki\textsuperscript{1} and Deisy Chaves\textsuperscript{1}

\textsuperscript{1} Universidad de León, España
\textsuperscript{2} Researcher at INCIBE (Spanish National Cybersecurity Institute), León, Spain
\{pblanm, efidf, ealeg, mnab, dchas\}@unileon.es

Abstract

Text Spotting can be used as an approach to retrieve information found in images that cannot be obtained otherwise, by performing text detection first and then recognizing the located text. Examples of images to apply this task on can be found in Tor network images, which contain information that may not be found in plain text. When comparing both stages, the latter performs worse due to the low resolution of the cropped areas among other problems. Focusing on the recognition part of the pipeline, we study the performance of five recognition approaches, based on state-of-the-art neural network models, standalone OCR, and OCR enhancements. We complement them using string-matching techniques with two lexicons and compare computational time on five different datasets, including Tor network images. Our final proposal achieved 39.70% precision of text recognition in a custom dataset of images taken from Tor domains.

Keywords: Text Spotting, Text Recognition, OCR, Cybersecurity, Tor darknet.

1 Introduction

Text spotting is a pipeline of two consecutive tasks: accurate detection of text regions inside an image or video and recognition of the detected text to obtain a readable string \cite{3, 7}. Automatizing the process of text retrieval from visual media allows to obtain a high volume of information otherwise ignored in content-based search engines \cite{4}.

The importance of text spotting is significantly evident in the Darknet network, with the onion domains of The Onion Router (Tor) network being a relevant source of illegal content. Thanks to the high level of privacy and anonymity of the Tor network, it has attracted illegal services traders to promote for their products safely, far from the monitoring tools of the authorities.

A recent study by Al-Nabki et al. (2019) \cite{1} showed that more than 29\% of the onion domains involve suspicious activities such as weapon selling, drugs trading, and counterfeiting personal identification documents \cite{10, 11}.

The recent advance in Machine Learning and Deep Learning algorithms allowed researchers to develop intelligent tools to detect suspicious activities. In Al-Nabki et al. (2019) \cite{1}, the authors proposed an algorithm to rank the onion domains and to detect the most influential ones, while in Al-Nabki et al. (2017) \cite{2}, graph analysis is used to detect the emerging products. Other approaches have proposed image classification system to detect these activities \cite{4}.

Consequently, onion domain hosts have sorted to hiding the descriptive text of their products or services inside images. The text spotting technique comes to fill in this gap to detect and recognize this type of hidden text.

As far as we know, only one work has tackled text spotting in the onion domains \cite{5}. However, the proposed method obtained 57\% F-Measure in text detection and 0\% precision in recognition. This can be attributed to issues such as partial occlusion, text orientation or the presence of multiple languages in the same image. Furthermore, several types of text can be found in the images hosted in onion domains of the Tor network, varying from hand-written based text to custom fonts and machine printed text, such as watermarks (Fig. 1).

Due to the difference in the results of each task, we split our original pipeline in order to improve their separate performance. In this paper, we focus on the text recognition phase only, in order to find the best methods suited for this task and how they can be improved.
The text recognition task can be divided into two steps, segmentation and transcription. The segmentation task consists on applying techniques that allow to extract the bounded characters from an image, separating the individual characters before their transcription. Some of the most relevant techniques in segmentation include text binarization, text line segmentation and character segmentation [23].

After the characters have been segmented, they can be transcribed into readable character sequences, by using single character or word level recognition. Words analysis is more common than sentences due to the fact that they are easier to track and transcribe.

When applied to natural-scene images, text recognizers obtain lower scores than document-based transcription. This is due to the differences in how text appears in real images when compared to the clean backgrounds and structure of document text, which may not contain multiple fonts, orientation or the noise found in regular images [21].

We benchmark five text recognition approaches in five different state-of-the-art datasets in order to test the performance of this task. We select three neural network based approaches; ASTER [21], FOTS [17] and CRNN [20], due to their state-of-the-art results, as well as one standalone Optical Character Recognition (OCR) approach and an enhanced OCR approach.

Two text corpora; general and Tor context-specific, as well as string-matching algorithms are used when comparing the result to the original ground truth in order to obtain better results. We also analyze the most relevant problems when recognizing text from different sources.

The rest of the paper is organized as follows. Section 2 presents a review of relevant text recognition approaches. Section 3 reports the methodology followed for comparing the text recognition methods. Section 4 details our experiments and result discussion. Finally, we present our conclusions and future lines of work in the field of text spotting.

## 2 Related Works

Several approaches have been proposed in the past few years to improve text recognition in natural images. Tencent-PRC & USTB-PRIR achieved the highest result of 43.58% precision in the ICDAR (International Conference on Document Analysis and Recognition) 2017 competition of Robust Reading Challenge on COCO-Text [12], using specific lexicons to improve word recognition.

Shi et al. [21] introduced a neural network model that combines rectification and recognition networks, based on sequence-to-sequence learning models. The first network is used to fix the orientation of the input image and the irregularities of the text, while the second performs a character sequence prediction using the newly corrected image.

Liu et al. [17] proposed a Text Spotting system that combines detection and recognition on a joint trainable system. This approach uses Convolutional Neural Networks (CNNs) shared between detection and recognition in order to perform feature extraction on a single network.

Shi et al. [20] combined Deep Convolutional Neural Networks (DCNN) and Recurrent Neural Networks (RNN) architectures to create a method that can process images of varying dimensions and predict characters or words of different lengths. The method trains both structures simultaneously with only one loss function.

Bartz et al. [3] proposed a method that uses a single neural network in order to both detect and recognize text in a semi-supervised way training both tasks jointly.

Finally, Busta et al. [7] developed a Fully Convolutional Net (FCN) based detector, combined with a Connectionist Temporal Classification (CTC) recognizer in a single, trainable framework.

## 3 Methodology

We selected five text recognition approaches, three of which are based on neural networks and two OCR approaches, in order to study their performance. For neural networks, we selected ASTER [21], FOTS [17] and CRNN [20]. For Optical Character Recognition, we chose Pytesseract4, a python wrapper for Google’s Tesseract technology. We used this OCR approach under two different configurations.

We selected the neural network based models due to their state-of-the-art results. In particular, we selected ASTER as a relevant text recognizer due to its rectification feature, which can correct oriented text making the transcription more accurate.

ASTER [21] is a model that combines this rectification network alongside recognition. It predicts a character sequence from the corrected image using a bidirectional decoder, which combines the results of each decoder. Using these features,
ASTER can complement text detectors improving their accuracy by correcting text orientation. The recognition network is trained on two synthetic datasets [13], while the rectification network is trained by the gradients obtained at the end of the recognition, lacking the need for annotations.

CRNN [20] consists of three main components integrated into a single framework. The convolutional layers, which extract feature maps from an image, the recurrent layers that predict a label for the extracted frames and the final transcription layer, which transcribes the predictions into a readable character sequence. The model is trained on synthetic datasets [13] and based on the VGG-Very Deep Architecture.

The FOTS method [17] focuses on retrieving and recognizing text regions with incidental text simultaneously. This approach shares features among the two tasks, reducing computational time and resulting in a single end-to-end trainable network. It uses synthetic datasets [13] before training the network and fine-tuning the model.

We also placed a strong emphasis on OCR approaches due to the high presence of watermarks and machine-printed text in our custom dataset. In our Tor based images, machine-printed text often appears in images with clear backgrounds and big font sizes. Copyright disclaimers are also often found in customized borders, separate from the rest of the image’s content. OCR approaches perform well in these environments [23].

The chosen OCR approach can be executed with the default parameters, which performs automatic page segmentation using the legacy engine but no orientation and script detection.

This algorithm can also be adapted for the treatment of the images (as a single line, word or character) and the type of engine used to recognize the character (LSTM neural networks or the legacy engine). We set these parameters so that we treat each image as a single line of text, due to the fact that each cropped image only contains one word in the used datasets. We also used LSTM as the engine mode, creating a setup different from the default algorithm execution.

In order to test all methods, we used five different datasets. The SVT dataset [22], which contains 647 text regions, the ICDAR 2013 [15] and 2015 [14] datasets, which hold 1093 and 2096 images respectively, and the IIIT5K-Words dataset [18], with a total of 3000 images, were chosen as relevant datasets for the text recognition task. Additionally, we used a small subset of our own custom dataset [5], named “Custom TOIC”, consisting of 100 images gathered from the Tor Darknet with a total of 1112 text regions. We only chose the regions labelled as "legible", reducing the quantity of images to 675 for these experiments. Fig. 2 illustrates some of the most relevant images.

Figure 2: Image examples from the used datasets

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Tor-specific</th>
<th>Generic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison</td>
<td>Ratcliff</td>
<td>Levenshtein</td>
</tr>
<tr>
<td>Default</td>
<td>13.40%</td>
<td><strong>16.50%</strong></td>
</tr>
<tr>
<td>Set-up</td>
<td>22.20%</td>
<td><strong>25.50%</strong></td>
</tr>
<tr>
<td>Speed (s)</td>
<td>0.42</td>
<td>2.44</td>
</tr>
</tbody>
</table>

Table 2: OCR precision results using lexicons on Custom TOIC

https://doi.org/10.17979/spudc.9788497497169.828
ness with a different scoring system, resulting in an ordered list with the most similar words per method. We selected them based on these different resulting values, in order to measure their performance in a Tor-specific lexicon.

The Levenstein distance measures closeness as the minimum amount of string operations such as substitutions or additions needed to turn the first string into the second, meaning a lower number indicates a higher match.

The Ratcliff / Obershelp approach compares strings by doubling the length of matched character groups and dividing it by the summed length of both words.

Finally, the Jaro-Winkler word similarity matches characters if they are found in the compared string at a distance less than half of its length. This approach penalizes less errors at the end of the string.

We tested each approach using two dictionaries, one Tor-specific and one English-based, containing 5,570 and 471,376 words respectively and measuring the average time taken by each word match.

Afterwards, we applied ASTER’s text rectification feature in all the datasets in order to enhance the performance of the algorithm, initially with no dictionaries attached. Finally, we merge this approach with the use of the Tor-specific dictionary in our custom dataset, in order to identify and analyze the hardest images and conditions to properly transcribe.

4 Experimental Results and Discussion

4.1 Experimental setup

We evaluated the methods on an Intel Xeon E5 v3 computer with 128GB of RAM using an NVIDIA Titan Xp GPU. We measured text recognition performance using the precision metric, which is the percentage of fully-matched recognition results to the documented labels of each image.

4.2 Initial experiment

The precision results for the recognition methods, without using any dictionaries, are shown in Table 1. The obtained results show that ASTER outperforms the other methods in the state-of-the-art datasets. CRNN comes as second with slightly lower performance. For FOTS, we implemented a publicly available version at https://github.com/WangXiaoCao/FOTS_two_stage that is unrelated to the original authors, which is the reason for the result variation in the datasets used.

The chosen OCR approach, Pytesseract4, scored higher than FOTS under custom configurations on the ICDAR 2015 dataset and higher than CRNN on the Custom TOIC dataset, validating our initial hypothesis of OCR focused methods being relevant in these particular environments.

Our custom TOIC dataset contains multiple level annotations from character to words and sentences levels, which can cause lower results when recognizing text inside cropped images.

In contrast, the other datasets are labeled following word-based strategy only, such as SVT and IIT5K-Words.

4.3 OCR and lexicons

As we observed a high volume of images containing watermarks and machine-printed text, we decided to only use OCR in order to analyze the improvements of string matching using dictionaries.

When using dictionaries, we compare the 10 highest scoring words against the transcribed sequence, trying to locate a word match. The results of applying these techniques on our own custom dataset are detailed in Table 2. The Levenshtein method obtained the best results with a 25.0% precision using the Tor-specific corpus on the setup version and a 21.10% on the generic dictionary, but with a very high computational cost. The Jaro-Winkler approach was the most computationally efficient, but scored lower than Levenshtein’s. However, when large dictionaries are being used, the Jaro distance could be considered as the most relevant approach.

Using lexicons with the Levenshtein string-matching method, we improved the OCR results. The default OCR improved from a precision result of 10.90% to 16.50%, while the custom setup achieved a precision 25.50% from the original 18.83%. However, the results remain lower than ASTER’s, which did not use any lexicon.

4.4 Rectification network experiments

Using ASTER’s rectification network, we tested all the datasets once more using a different number of iterations. This network corrects an input image, predicting a set of control points from the original image and then performing a Thin-Plate-Spline [6] transformation before generating the rectified image. The new image contains a lower degree of orientation which increases the performance of the recognizers.
Table 3: ASTER precision improvements using the rectification network

<table>
<thead>
<tr>
<th>Rectifications</th>
<th>SVT</th>
<th>Custom TOIC</th>
<th>IIT5K-Words</th>
<th>ICDAR 2013</th>
<th>ICDAR 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>88.25%</td>
<td>28.30%</td>
<td>84.13%</td>
<td>88.29%</td>
<td>72.35%</td>
</tr>
<tr>
<td>1</td>
<td>90.11%</td>
<td>30.52%</td>
<td>85.40%</td>
<td>89.84%</td>
<td>74.24%</td>
</tr>
<tr>
<td>2</td>
<td>90.42%</td>
<td>31.70%</td>
<td>86.07%</td>
<td>90.30%</td>
<td>75.25%</td>
</tr>
<tr>
<td>5</td>
<td>90.88%</td>
<td><strong>32.74%</strong></td>
<td>87.00%</td>
<td>90.94%</td>
<td>76.37%</td>
</tr>
<tr>
<td>10</td>
<td>91.19%</td>
<td>32.74%</td>
<td>88.53%</td>
<td><strong>91.03%</strong></td>
<td><strong>76.80%</strong></td>
</tr>
<tr>
<td>20</td>
<td>91.19%</td>
<td>32.74%</td>
<td><strong>88.93%</strong></td>
<td><strong>91.13%</strong></td>
<td><strong>76.80%</strong></td>
</tr>
</tbody>
</table>

If the recognition was not the same as the documented label, the image would be rectified and transcribed again as many times as the iterations specified. Table 3 shows our results applying this network to five images, while the visual rectification effect in the images is shown in Fig. 3.

We improved the results up to 4% on each of the datasets before the improvements converged above 10 iterations, with subsequent rectifications not significantly altering the scores. Adding a single correction improved the results 2%.

We found that 5 iterations achieved the best results in our custom TOIC, enhancing the original results of 28.30% to 32.74%.

Figure 3: Resulting images (right) of applying ASTER’s rectification network

### 4.5 Rectification network and lexicons

Lastly, we combined our selection of the Levenshtein distance, our Tor-specific lexicon, and the correction approach to improve the results in our custom dataset, as illustrated in Table 4.

When using the Tor-specific lexicon, the 10 highest-score matching words are checked against the transcribed text for string comparison. Combining all approaches, we obtain an improvement of 11.40% when recognizing text from Tor-related images using the ASTER method, with each configuration increasing processing time.

#### 4.6 Image analysis

After finishing the enhancements on the text recognition task, we take the images that were not correctly recognized and analyze them. We identify five main problems in the text recognition task: similar characters, incorrect labelling, orientation, resolution and other factors. We found no influence due to the color of the cropped words. Similar characters encapsulates text regions that are close to other sequences, such as common “g” and “9” mistakes. Other examples include the letter “U” being incorrectly detected as “LI”, due to their analogous form. Certain font type and size deviated problems can also be associated to this category, as they can make differentiating certain characters a complex task. In most cases, the problems caused by this issue can be reduced with the use of lexicons.

Incorrect labelling refers to the wrong assignment of labels to text regions where the given sequence differs from the documented text. It is a common occurrence that the label does not include certain characters that may be difficult to appreciate at first, only to be properly recognized but not obtain a full match due to the original label not contain-

Table 4: ASTER results on Custom TOIC Subset using a Tor-specific lexicon

<table>
<thead>
<tr>
<th>Lexicon</th>
<th>Rectifications</th>
<th>Precision</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>None</td>
<td>28.30%</td>
<td>75.72</td>
</tr>
<tr>
<td>No</td>
<td>1</td>
<td>30.52%</td>
<td>106.56</td>
</tr>
<tr>
<td>Yes</td>
<td>None</td>
<td>34.81%</td>
<td>330.72</td>
</tr>
<tr>
<td>Yes</td>
<td>1</td>
<td>37.04%</td>
<td>559.50</td>
</tr>
<tr>
<td>Yes</td>
<td>2</td>
<td>38.22%</td>
<td>753.30</td>
</tr>
<tr>
<td>Yes</td>
<td>5</td>
<td>39.26%</td>
<td>1.257.79</td>
</tr>
<tr>
<td>Yes</td>
<td>10</td>
<td><strong>39.70%</strong></td>
<td>1.912.09</td>
</tr>
</tbody>
</table>
ing them. Other labelling mistakes, such as writing "Brazil" as "Brasil" or "Name" as "Nam", can also be found in most of the datasets used. While some of these errors can be solved using dictionaries, wrong labelling can reduce scores significantly if left ignored.

Orientation is one of the most relevant problems when performing text recognition. From slightly distorted text due to a particular camera angle, to curved fonts or vertically aligned text, images that contain this type of information are often incorrectly recognized. Although ASTER's rectification network can improve transcription on slightly oriented character sequences, vertical or curved text is still an issue that the proposed network fails to recognize properly. In recent years, this type of text has become more relevant, [8] as it is often missing from common datasets and competitions.

The resolution of the cropped regions is a problem of strong relevance especially in our custom dataset. As we have multiple text regions that can be found in a single image, it is a common occurrence that some of these regions are of lower dimensions than 30 × 30 pixels. As most of the methods often re-scale the images to a custom size before processing, text recognition is likely to fail in such images. For this purpose, superresolution techniques can be used for image enhancement.

The last category encapsulates different problems that are common in real-scene images. We found that ASTER did not perform as well in big standalone characters, long words or sentences in images that contained a significant font size difference. Other common problems were found in blurry words, high levels of brightness and certain occluded characters as well as machine printed texts, which was our main reason for using OCR approaches.

5 Conclusions

In this paper, we have selected five text-recognition based approaches using three neural network approaches and two OCR configurations, comparing their performance in five datasets with the goal of extracting text found inside images taken from the Tor Darknet.

We have improved the results in the OCR approach by using dictionaries and string-matching methods to enhance text recognition. We obtained a precision of 25.5% in our custom dataset using Pytesseract4, concluding that the use of OCR approaches can be useful in Tor images that contain machine printed text.

In order to enhance recognition results, we used ASTER's rectification network, concluding that five iterations is the most efficient approach when considering computational efficiency. We obtained an increase of 4% precision with this configuration, which is further increased to 10.96% when combining the approach with a Tor-specific lexicon and the Levenshtein distance, which takes a high computational cost.

Combining ASTER's rectification and recognition network with the use of a Tor-based lexicon and the Levenshtein distance, we obtained a recognition precision in our custom dataset of 39.70%. When using using OCR approaches and the same lexicon, we obtained a 25.50%.

As a result of our work, we have identified the best OCR configurations for our Tor-based text recognition goal. We have also analyzed the best string matching methods efficiency and cost-wise, being the Levenshtein and Jaro-Winkler approaches respectively.

Furthermore, we determined oriented text, character similarity and low image resolution as the most challenging conditions for text recognition. We also discovered errors in the documented labels of the dataset, which reduces the algorithm’s precision results.

Our future work will be focused on vertical text recognition and low resolution images, as well as more efficient string comparison methods to improve the computational cost of using large lexicons. We will also focus on the detection section of the pipeline and how these areas can be corrected using the rectification network.

Acknowledgements

This research is supported by the framework agreement between Universidad de León and INCIBE (Spanish National Cybersecurity Institute) under Addendum 01. We acknowledge NVIDIA Corporation with the donation of the Titan Xp GPU used for this research. This research has also been funded with support from the European Commission under the 4NSEEK project with Grant Agreement 821966. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

References


IEEE transactions on pattern analysis and machine intelligence, 37(7):1480–1500.

© 2019 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution CC BY-NC-SA 4.0 license (https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es).