AAA534-2021S: Final Project
“Detecting multiple accounts in the darknet market using Super-classfication”

Yerim Kim Jaedeok Jo

Abstract

Darknet markets are online services behind Tor where cybercriminals trade illegal goods. Vendors in these markets often create multiple accounts, making it challenging to infer the relationship between cybercriminals and identify coordinated crimes. For sybil detection of darknet market, we will use the vendor’s photography style. In this project, we propose novel approach to link the multiple accounts of the same darknet vendors through a super-classfication model that combines super-resolution and DNN architecture.

1. Introduction

Darknet market is a website accessible through Tor that trades illegal goods and services. Due to the anonymity of the darknet, transactions such as drugs, weapons, and hacking services have increased tremendously in the darknet. One of the factors that makes tracking harder in the darknet is a vendor with multiple accounts. So far, related works that have identified multiple accounts of vendors include studies using vendors’ photography style, and studies using stylometry analysis. Among them, we will focus on the method of identifying the same vendor by analyzing the vendors’ photography style. The core idea is that darknet vendors often have to take their own product photos to prove the possession of the illegal goods, which can reveal their distinct photography styles. Since there are few studies focused on vendor photo analysis, we thought that developing the analysis tool used in previous studies would be able to more accurately detect vendors with multiple accounts.

To fingerprint vendors, we construct a deep neural networks (DNN) to model the photography styles. We apply transfer learning to the model training, which allow us to accurately fingerprint vendors with a limited number of photos. Also, darknet images have the limitation of low-resolution, so it is expected that solving this problem will show improved classification results. Therefore, we create a *‘super-classification model’* that increases the resolution of the darknet image through super-resolution (SR) and classifies vendors based on the photography style. There are three challenges we need to solve in this project. The process we solved for the following problems is detailed in section 4.

- Pre-processing of darknet web crawling data
- Designing Deep Neural Networks architecture proposed in previous study
- Applying super-resolution to the images to compare our new model to the base model

We are freshmen with a master’s degree, and since we majored in a different field with a bachelor’s degree, we have never done any research in that field before, and we started with computer vision class for the first time.

Yerim Kim: Researching and analyzing related works, Wrting, Presentation

Jaedock Jo: Data collection and pre-processing, Modeling

2. Related works

There are researches that improve the accuracy of sybil detection of darknet using various features. The SR model has also been improved by developing various models.

2.1. Darknet sybil detection

In the recent past, several research efforts have tackled drug trafficking in darknet markets. Ho and Ng (Ho & Ng, 2016) investigated the role of stylometric features that work at the character level, word level, sentence level, and paragraph level. They uncovered that writing style could be used to attribute and correlate authorship between vendors on multiple Dark Web forums with high accuracy. Apart from capturing the stylometric information, some studies have also exploited the image embedded in the vendor sites. Wang and Peng (Wang et al., 2018) utilized a deep neural network and transfer learning framework to extract distinct features from a vendor’s photos automatically. They discovered that image-based approach outperforms existing stylometry based techniques in both accuracy and coverage. Another study conducted by Zhang and Fang (Zhang et al., 2019) integrated both the stylometric and the photography styles using an attributed heterogeneous information network.

2.2. Super-resolution

There are many studies that have proposed various super-resolution models. Dong and Loy (Dong et al., 2015) proposed method that directly learns an end-to-end mapping between the low/high-resolution images. The mapping is represented as a deep convolutional neural network (CNN) that takes the low-resolution image as the input and outputs the high-resolution one. They further show that traditional sparse-coding-based SR methods can also be viewed as a deep convolutional network. But unlike traditional methods that handle each component separately, the method jointly optimizes all layers. The deep CNN has a lightweight structure, yet demonstrates state-of-the-art restoration quality, and achieves fast speed for practical on-line usage.

Ledig and Theis (Ledig et al., 2017) present SRGAN, a generative adversarial network (GAN) for image super-resolution (SR), which is the first framework capable of inferring photo-realistic natural images for 4× upscaling factors. To achieve this, they propose a perceptual loss function which consists of an adversarial loss and a content loss. The adversarial loss pushes the solution to the natural image manifold using a discriminator network that is trained to differentiate between the super-resolved images and original photo-realistic images. In addition, they use a content loss motivated by perceptual similarity instead of similarity in pixel space. The deep residual network is able to recover photo-realistic textures from heavily downsampled images on public benchmarks.

3. Dataset

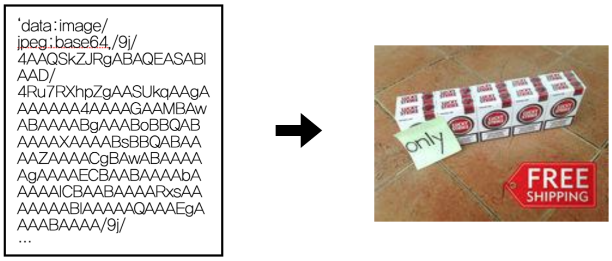
To examine the possibility of profiling darknet vendors, we use the public archive of darknet market datasets.[1] The data archive contains the daily (sometimes weekly) snapshots of the darknet markets crawled by researchers from 2013 to 2015. Each snapshot contains the raw product pages of the respective marketplace. In this paper, we select one of the largest darknet markets: SilkRoad2.

4. Super-classification model

The super-classification model consists of three process which are data pre-processing, DNN, and SR. The detailed description of each step and the structure of the model are as follows. The code and dataset for our project has been uploaded to github.[2]

4.1. Image pre-processing

Since the raw data of crawling darknet can not be used for analysis, we go through pre-processing procedure. The images in the crawled data were expressed in base64 code, so we conduct the process of converting base64 code to jpg format like Figure 1, and classifying each image by vendor. Also, there were many images in which several images were combined like Figure 2. In this case, we crop each images and used separately. We extract in total products 18,402 image listed by 582 vendors from the market, and used three-day data and only images related to drugs.



‘data : image/
jpeg ; base64,/9j/
4AAQSkZJRgABAQEASABI
AAD/
4Ru7RXhpZgAASUkqAAgA
AAAAAA4AAAAGAAMBAw
ABAAAABgAAABoBBQAB
AAAAXAAAABsBBQABAA
AAZAAAACgBAwABAAAA
AgAAAAECBAABAAAAbA
AAAAICBAABAAAARxsAA
AAAAABIAAAAAQAAAEgA
AAABAAAA/9j/
…

only
FREE
SHIPPING

Figure 1. Image data converted from base64.

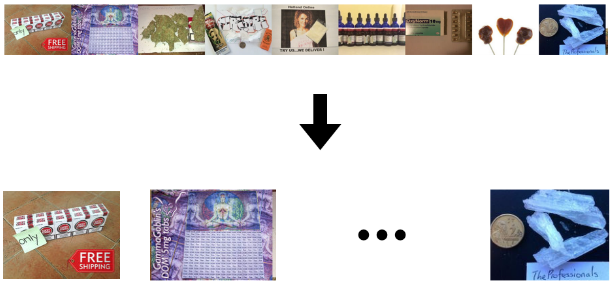


Figure 2. Image data combined with several images.

4.2. DNN architecture

To capture the unique features from a vendor’s photos, we rely on Deep Neural Networks which can extract features automatically without manually crafting the feature list. The key challenge is that DNN, in order to be accurate, requires a massive amount of training data. However, in darknet markets, the number of photos per vendor is limited. We apply transfer learning to pre-train a DNN using a large existing image dataset and then fine-tune the last few layers using the darknet dataset. The intuition is that features of the DNN are more generic in the early layers and are more dataset-specific in the later layers.

The early layers can be trained using general object photos. For our system, we use the largest annotated image dataset

[1] https://www.gwern.net/DNM-archives

[2] https://github.com/lubiksss/SR_applied_CivilDetection

Table 1. Number of vendors and images in our dataset.

VENDOR	TOTAL IMAGE	TRAIN IMAGE	TEST IMAGE
582	18,402	11,383	7,019

called ImageNet to pre-train a DNN. Then we replace the final softmax layer with a new softmax layer which handles the classes in the darknet dataset. Here, a "class" is defined as a set of photos uploaded by the same vendor. To construct the DNN, we selected ResNet-18 model.

Figure 3 shows the workflow for the ground-truth evaluation. First, for vendors that have more than 30 photos, we split their photos into two even parts. We add the first part to the training dataset and the second part to the testing dataset. Second, for the other vendors, if their image is less than 30, we add them to the training set. Once we construct the dataset as shown in Table 1, we then perform transfer learning based on a model pre-trained on ImageNet, and use our training dataset to fine-tune the last layers of the network.

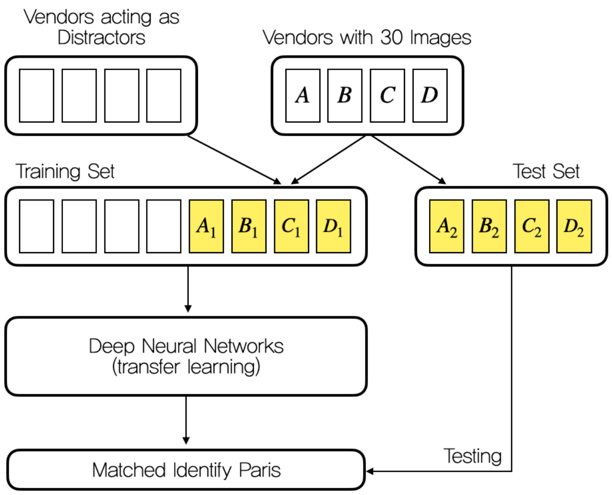


Figure 3. Work flow for the ground-truth evaluation.

4.3. SRCNN architecture

Consider a single low-resolution image, we first upscale it to the desired size using bicubic interpolation, which is the only pre-processing we perform. Let us denote the interpolated image as Y. Our goal is to recover from Y an image $F(Y)$ that is as similar as possible to the ground truth high-resolution image X. For the ease of presentation, we still call Y a "low-resolution" image, although it has the same size as X. We wish to learn a mapping F, which conceptually consists of three operations:

Table 2. Accuracy and loss of models without SR and models with SR.

	WITHOUT SR		WITH SR	
	TRAIN	TEST	TRAIN	TEST
ACCURACY	0.997	0.945	0.998	0.941
LOSS	0.062	0.287	0.064	0.289

Patch extraction and representation: this operation extracts (overlapping) patches from the low-resolution image Y and represents each patch as a high-dimensional vector. These vectors comprise a set of feature maps, of which the number equals to the dimensionality of the vectors.

Non-linear mapping: this operation nonlinearly maps each high-dimensional vector onto another high-dimensional vector. Each mapped vector is conceptually the representation of a high-resolution patch. These vectors comprise another set of feature maps.

Reconstruction: this operation aggregates the above high-resolution patch-wise representations to generate the final high-resolution image. This image is expected to be similar to the ground truth X.

We put all three operations together and form a convolutional neural network as shown in Figure 4. We apply SR-CNN to the entire darknet dataset to obtain high-resolution images, use the high-resolution darknet dataset conducting experiment using DNN, and perform the same experiment as before.

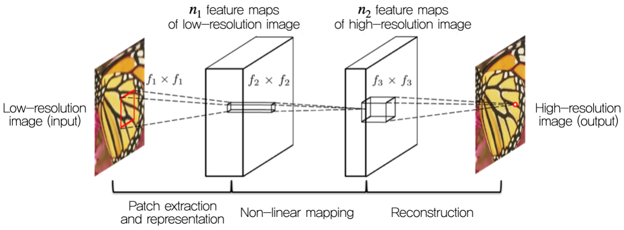

n_1 feature maps of low–resolution image
n_2 feature maps of high–resolution image
$f_1 \times f_1$
$f_2 \times f_2$
$f_3 \times f_3$
Low–resolution image (input)
High–resolution image (output)
Patch extraction and representation
Non–linear mapping
Reconstruction

Figure 4. SRCNN architecture.

5. Evaluation

In order to check whether the application of super-resolution improves the performance of detecting the same vendor, we compared the accuracy and loss of a model using basic darknet data and a model using high-resolution darknet data. The accuracy and loss results of train and test are in Table 2, and the evaluation results of the two models are visualized in Figure 5 and Figure 6.

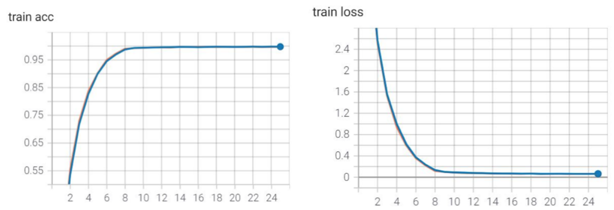


Figure 5. Train accuracy and loss(blue line: without SR, orange line: with SR).

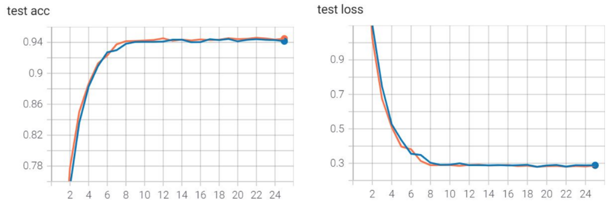


Figure 6. Test accuracy and loss(blue line: without SR, orange line: with SR).

When looking at the data and graph, it can be seen that there is no significant difference in the performance of the two models. The reason can be confirmed through Figure 7. We analyzed that the resolution of the picture area in the image was improved, but the resolution of the text area was worse. Therefore, the two results offset each other out and show the same result as the existing model.

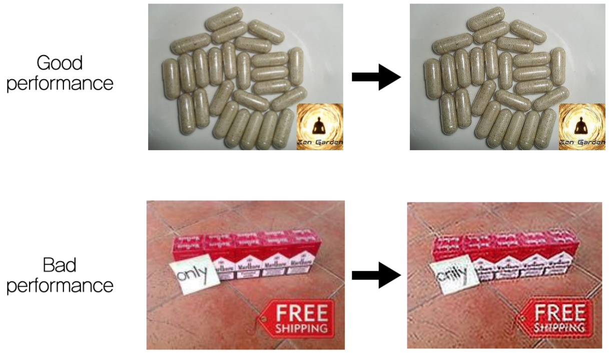


Figure 7. Good and bad performance of SR

6. Discussion

Contrary to our expectation that increasing the resolution of the darknet image would enable more accurate classification by vendor, almost similar results were obtained. The reason is considered to be that the resolution of the text area is rather poor because the data of ImageNet was used in the pre-training process. The resolution of the text area is expected to be improved if MNIST dataset is used as pre-train data. Therefore, it is likely that the results will be improved if SR is applied by separating data with a lot of picture areas and data with a lot of text areas.

Since there are various models of SR itself, it is also a good task to try other models such as SRGAN, NE, and DCSCN. Also, we consider all of vendor's product photos, but we allow different products to use the same photo. Therefore, the performance of the classification model all came out high accuracy because of the duplicated image. If we conduct the experiment with a non-duplicated image dataset, we can see a more pronounced difference.

7. Conclusion

In this study, we propose a super-classification model that improves classification performance by putting images applied with a super-resolution tool into DNN. Although the results were different than expected, there is much room that can be improved in the future to accurately detect the multiple accounts in the darnet market. There were many challenges such as the pre-processing of darknet data, building a DNN, and applying SR, however it is meaningful that we studied a lot in the process of solving these challenges and applied the models learned in the computer vision class.

References

Dong, C., Loy, C. C., He, K., and Tang, X. Image super-resolution using deep convolutional networks. *IEEE transactions on pattern analysis and machine intelligence*, 38(2):295–307, 2015.

Ho, T. N. and Ng, W. K. Application of stylometry to darkweb forum user identification. In *International Conference on Information and Communications Security*, pp. 173–183. Springer, 2016.

Ledig, C., Theis, L., Huszár, F., Caballero, J., Cunningham, A., Acosta, A., Aitken, A., Tejani, A., Totz, J., Wang, Z., et al. Photo-realistic single image super-resolution using a generative adversarial network. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 4681–4690, 2017.

Wang, X., Peng, P., Wang, C., and Wang, G. You are your photographs: Detecting multiple identities of vendors in the darknet marketplaces. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pp. 431–442, 2018.

Zhang, Y., Fan, Y., Song, W., Hou, S., Ye, Y., Li, X., Zhao, L., Shi, C., Wang, J., and Xiong, Q. Your style your identity: Leveraging writing and photography styles for drug trafficker identification in darknet markets over attributed heterogeneous information network. In *The World Wide Web Conference*, pp. 3448–3454, 2019.