Metadata of the chapter that will be visualized in SpringerLink

Book Title	Emerging Technologies in Computer Engineering: Cognitive Computing and Intelligent IoT	
Series Title		
Chapter Title	Personally Identifiable Information (PII) Detection and Obfuscation Using YOLOv3 Object Detector	
Copyright Year	2022	
Copyright HolderName	The Author(s), under exclusive license to Springer Nature Switzerland AG	
Corresponding Author	Family Name	**Soni**
	Particle	
	Given Name	**Saurabh**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Sir Padampat Singhania University
	Address	Udaipur, India
	Email	saurabh.soni18@spsu.ac.in
	ORCID	http://orcid.org/0000-0002-5893-7336
Corresponding Author	Family Name	**Hiran**
	Particle	
	Given Name	**Kamal Kant**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Sir Padampat Singhania University
	Address	Udaipur, India
	Email	kamal.hiran@spsu.ac.in
	ORCID	http://orcid.org/0000-0002-4563-1944

Abstract	We live in an era of smart phones, and the number of smart phone users is growing by the day, resulting in a rapid increase in the number of people with access to the internet and social media. According to reports, the average person spends about five hours per day on his or her mobile phone. This extensive use of phone and internet had a significant impact on the amount of data exchanged on social media platforms such as Instagram, Facebook, Whatsapp, Snapchat, and others. Images are one type of data. Every day, millions and billions of images are shared, and many of them may contain information that compromises an individual's privacy. Hackers can use such information for malicious purposes and personal gain. They can even use this person's personal information to blackmail or threaten them. Cybercriminals can also use that information to open a bank account in the victim's name, create a forged driving licence, and other forms of identification. Although many researchers have addressed this issue by using tools such as Tensorflow and OpenCV to detect and obfuscate sensitive information in images. In this paper, we will use the YOLOv3 object detector to solve this problem. First, we'll label the data that needs to be blurred, and then we'll train our object.

Keywords (separated by '-')	You Only Look Once (YOLO) - Convolutional Neural Network (CNN) - Face-detection

Personally Identifiable Information (PII) Detection and Obfuscation Using YOLOv3 Object Detector

Saurabh Soni(✉) and Kamal Kant Hiran(✉)

Sir Padampat Singhania University, Udaipur, India
{saurabh.soni18,kamal.hiran}@spsu.ac.in

Abstract. We live in an era of smart phones, and the number of smart phone users is growing by the day, resulting in a rapid increase in the number of people with access to the internet and social media. According to reports, the average person spends about five hours per day on his or her mobile phone. This extensive use of phone and internet had a significant impact on the amount of data exchanged on social media platforms such as Instagram, Facebook, Whatsapp, Snapchat, and others. Images are one type of data. Every day, millions and billions of images are shared, and many of them may contain information that compromises an individual's privacy. Hackers can use such information for malicious purposes and personal gain. They can even use this person's personal information to blackmail or threaten them. Cybercriminals can also use that information to open a bank account in the victim's name, create a forged driving licence, and other forms of identification. Although many researchers have addressed this issue by using tools such as Tensorflow and OpenCV to detect and obfuscate sensitive information in images. In this paper, we will use the YOLOv3 object detector to solve this problem. First, we'll label the data that needs to be blurred, and then we'll train our object.

AQ1

Keywords: You Only Look Once (YOLO) · Convolutional Neural Network (CNN) · Face-detection

1 Introduction

We all know that new technology related to smart phones follow a J-curve or exponential advancement. Earlier generations utilised reel cameras, but with the introduction of camera phones, the first thing people look for when purchasing a new phone is the camera and its quality. The picture quality on new phones has greatly increased, and even the tiniest elements in the environment are clearly evident in the images we take. These days, features like twin cameras are fairly prevalent. Front cameras with 32 Mega Pixels are also rather prevalent. New smart phones with such outstanding picture quality are also quite affordable, resulting in a tremendous increase in the number of individuals using social media platforms. Even if we only consider Instagram, the statistics shows that 95 million photos are submitted every day. These data demonstrate how information

V. E. Balas et al. (Eds.): ICETCE 2022, CCIS 1591, pp. 1–9, 2022.
https://doi.org/10.1007/978-3-031-07012-9_24

sharing has become ingrained in people's daily lives. Whether they are going to the bank or getting their driver's licence, new generations provide status updates on everything they do in their everyday lives. On social media, information such as a person's full name, age, and occasionally their current location or the location of their residence puts them exposed to crimes such as burglary. The Data Privacy Law is used to protect sensitive information from falling into the hands of criminals by censoring or removing it from the internet (if necessary).

Information such as a person's name, date of birth, and Social Security Number (SSN) (sometimes known as the "Holy Trinty") is sufficient for a hacker or cybercriminal to gain access to his or her personnel account. And by answering simple security questions, fraudsters can gain access to that person's financial information.

Personally Identifiable Information (PII) is information about a person that allows us to determine his or her identity. Examples of PII include name, date of birth, location, phone number, driving licence number, account number, pan id, aadhar card number, and so on. If they have a photo of the victim's pan card, aadhar card, driving licence, credit card, or debit card, they can access this information. And the amount of damage that can be done with it is limitless. There was one such case, it was March 2021, and it was discovered using a third party that there was unauthorised access to data from payment cards at one of the stores of the company Forever 21. This could be because credit card information of customers was leaked from one of their stores.

Object detection is used to address the problem of spreading personnel information about any individual via photos or videos. Object detectors are used to detect objects in images. When we look at the big picture, we can see that today's object detectors detect objects not only in images, but also in videos.

2 Problem and Objectives

To detect and obfuscate personally identifiable or other sensitive information in image.

- This Find and collect images that contain sensitive information, then use tools like labelImg to label that information (this step is known as Data Annotation).
- Secondly, that use YOLOv3 (You Only Look Once) object detector to get coordinates of bounding box around that information.
- Third finally censor it using OpenCV (Open Source Computer Vision Library) and Python.

3 Theoretical Background

3.1 Object Detection

Object detection is a type of computer technology that detects objects in images or video.

3.2 Convolutional Neural Network (CNN)

CNN is well-known for challenges requiring image processing or classification problems. CNN is a more advanced version of the Artificial Neural Network (ANN), which is used to address image-related problems by finding patterns in images that make sense. It's quite different because if you try to tackle an image-related problem with an ANN, you'll end up with a lot of computation that's wasteful in terms of time and memory usage. CNN, on the other hand, employs convolutional layers, or hidden layers. When we give CNN an image, it constructs filters to recognise features (like eyes, nose, loopy pattern, etc.). Then, based on their location in the image, those discovered features will be stacked into a feature map.

3.3 YOLOv3

You Only Look Once, or YOLO, is a state-of-the-art object recognition algorithm that is so quick that it has practically become a standard method of detecting things in the field of computer vision. Previously, people relied on sliding window object detection, although faster versions such as RCNN (Region Based Convolutional Neural Network), Fast-RCNN, and Faster-RCNN were developed. However, in 2015, YOLO emerged, outperforming all prior object identification methods. We're utilising YOLOv3, which AQ2 is the most recent and fastest version available (Fig. 1).

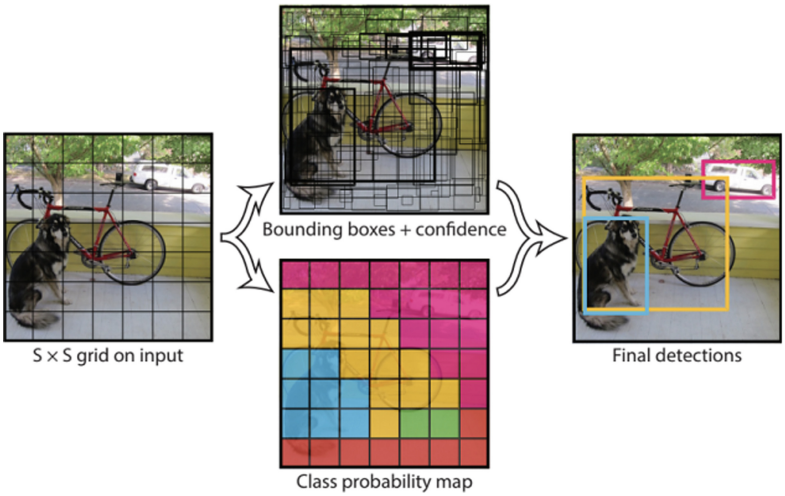

Fig. 1. YOLO (You Only Look Once)

The reasons why YOLOv3 is best suited for this project are:-

- As seen in Fig. 2, it is the quickest of all the options.

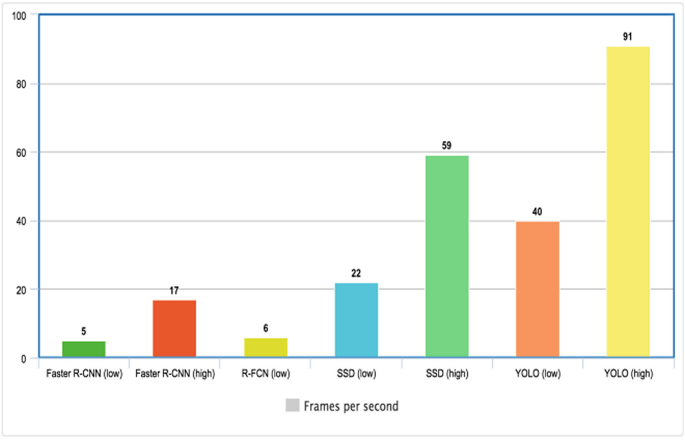

Fig. 2. Speed comparison (YOLO vs others)

- It has accuracy is good enough accuracy for our project. As shown Fig. 3.

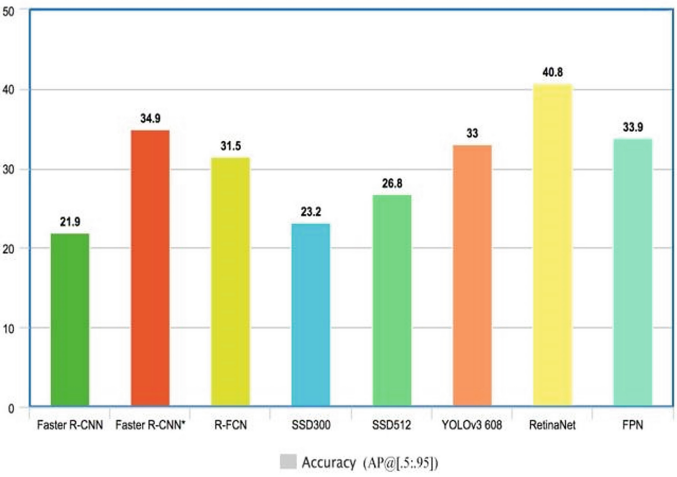

Fig. 3. Comparison of our model

- It recognizes small objects in images using the Feature Pyramid Network (FPN).

Darknet-53 is used by YOLOv3 to extract features from images. Darknet-53 is the moniker given to it since it uses 53 hidden layers or convolutional layers. It has

3X3 and 1X1 convolutional layers (hidden layers) in succession, as well as some short connections.

We'll also use the Darknet neural network framework to train our YOLO model. Multi scale training, data augmentation, and batch normalisation will all be used in this framework. It's an open source platform that's written in C and CUDA. It's also simple to set up, fast, and compatible with both CPU and GPU computing.

OpenCV
Intel Corporation developed the Open Source Computer Vision (OpenCV) library in C/C++ in the year 2000. In this project, we will use the OpenCV library to blur the sensitive information detected by our YOLO object detector.

TensorFlow
TensorFlow is an open source library developed by Google. Its main purpose is to simplify model building using neural networks and to use it for problems involving object detection.

Mean Average Precision (mAP)
Graphs are extremely useful and convenient when analysing the scope of improvement for a specific thing it was used for. However, in the case of computers, we only need a single numerical value to determine whether one value is greater than another. We calculate mean precision by calculating the average of different queries, and average precision (AP) is the average of a single rank.

The precision measured is a single threshold quantity. Average Precision examines the entire ranking and assigns a quality score based on the results. And this step is crucial because rank 1 (awarded to the person at the top) is worth twice as much as rank 2. It obtains all of its queries with average precision and obtains its average value using arithmetic average.

Intersection Over Union (IoU)
Intersection Over Union, or IoU, is a technique for detecting overlapping in a dataset, which aids in determining prediction accuracy when compared to real object boundaries.

4 Methodology

Data Gathering
Data is critical in machine learning problems. Images serve as our data in this project. We were able to collect over 50 images containing sensitive information. In future research, we will also use the Data Augmentation technique to improve the accuracy and reliability of our model, as well as to increase the volume of our dataset.

Data Annotation
Computer systems primarily use Data Annotation technology to assign keywords to image or video files. The term Annotating Image refers to the process of locating an

object in an image by box-bounding and labelling it. This is our second step, and it is required before we can train and test the object detection model. In this step, we will use an open-source tool called labeling.

Training

We will use **pre-trained darknet-53 weights** to train our model because they will help our model converge quickly.

Censoring Information with OpenCV

The most important step follows training and testing. Obfuscate sensitive information or personally identifiable information (PII) detected in an image. Our object detection model (YOLOv3) will generate a bounding-box containing the coordinates (top, left, right, and bottom) of our region of interest. Following the extraction of our region of interest, we would crop that portion and pass it as an argument to our blur function, which would replace the sensitive information portion of the original image with the blurred region, thereby censoring the information.

Integrating with Face-Detection Function

In this project, we also use a Python face detection library called "face-recognition", which was created with dlib and deep learning. It is quite accurate and can detect small

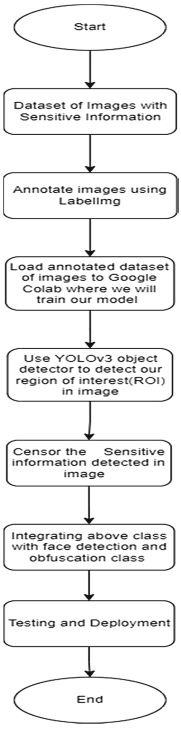

Fig. 4. Model workflow

faces in images. First, we used this library to determine whether or not there is a face in an input image. If a face is detected, we use its location (top, right, bottom, left) as an argument to our blur function, and after it is censored, the image is returned to our YOLO-based class where other sensitive information will be obfuscated.

Work Flow

AQ3 The work flow of our model is depicted in Fig. 4.

5 Result

As shown in Fig. 5, after the preceding steps, we run our class, and the output of our code is shown below in the figure, where in a PAN card image, the Date of Birth, Permanent Account Number, and face of that individual are obfuscated.

Fig. 5. Censored image of pan card

6 Conclusions

We've taken our first step and will continue to improve its performance by collecting more data that contains sensitive information and will help our model be more accurate.

Using this research, we can censor any individual's sensitive information. Furthermore, this research can serve as a foundation for moving forward with the concept of privacy in images or videos available on the internet. Many platforms, such as YouTube, where creators blur their car registration number and hide their bank details because cyber criminals can use these details for blackmailing, earning money, or even political gain. In this day and age of bio-warfare and cyber-warfare, data privacy is a major concern.

References

1. Morales, J., Huliganga, V., Pasaoa, J., Melad, N.: Detecting and blurring potentially sensitive personal information containers in images using faster R-CNN object detection model with TensorFlow and OpenCV (2019)
2. Grigorescu, S., Trasnea, B., Cocias, T., Macesanu, G.: A survey of deep learning techniques for autonomous driving. J. Field Robot. **37**, 362–387 (2019). https://doi.org/10.1002/rob.21918
3. Bochkovskiy, A., Wang, C.-Y., Liao, H.: YOLOv4: optimal speed and accuracy of object detection (2020)
4. Daoud, E., Vu Nguyen Hai, D., Nguyen, H., Gaedke, M.: Enhancing fake product detection using deep learning object detection models. **15**, 13–24 (2020). https://doi.org/10.33965/ijcsis_2020150102
5. Tautkute, I., Trzcinski, T., Skorupa, A., Brocki, L., Marasek, K.: DeepStyle: Multimodal search engine for fashion and interior design. IEEE Access. **7**, 84613–84628 (2018). https://doi.org/10.1109/ACCESS.2019.2923552
6. Chen, P.-Y., Hsieh, J.-W., Gochoo, M., Wang, C.-Y., Liao, H.: Smaller object detection for real-time embedded traffic flow estimation using fish-eye cameras, pp. 2956–2960 (2019). https://doi.org/10.1109/ICIP.2019.8803719
7. Apiparakoon, T., et al.: MaligNet: semisupervised learning for bone lesion instance segmentation using bone scintigraphy. IEEE Access 1 (2020). https://doi.org/10.1109/ACCESS.2020.2971391
8. Gallardo-Caballero, R., Orellana, C., García Manso, A., González-Velasco, H., Tormo-Molina, R., Macías, M.: Precise pollen grain detection in bright field microscopy using deep learning techniques. Sensors **19**, 3583 (2019). https://doi.org/10.3390/s19163583
9. Junayed, M.S., Jeny, A.A., Neehal, N., Ahmed, E., Hossain, S.A.: Incept-N: a convolutional neural network based classification approach for predicting nationality from facial features. In: Santosh, K.C., Hegadi, R.S. (eds.) RTIP2R 2018. CCIS, vol. 1036, pp. 466–475. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-9184-2_41
10. Kallam, S., Basha, M., Rajput, D., Patan, R., Balamurugan, B., Basha, S.; Evaluating the performance of deep learning techniques on classification using tensor flow application, pp. 331–335 (2018). https://doi.org/10.1109/ICACCE.2018.8441674
11. Shafiq, F., Yamada, T., Vilchez, A., Dasgupta, S.: Automated flow for compressing convolution neural networks for efficient edge-computation with FPGA (2017)
12. Janahiraman, T.V., Shahrul, M.S.M.: Traffic light detection using tensorflow object detection framework, pp. 108–113 (2019). https://doi.org/10.1109/ICSEngT.2019.8906486
13. Galvez, R.L., Bandala, A.A., Dadios, E.P., Vicerra, R.R.P., Maningo, J.M.Z.: Object detection using convolutional neural networks. In: TENCON 2018 - 2018 IEEE Region 10 Conference (2018)
14. Yanagisawa, H., Yamashita, T., Watanabe, H.: A study on object detection method from manga images using CNN. In: 2018 International Workshop on Advanced Image Technology (IWAIT), pp. 1–4 (2018). https://doi.org/10.1109/IWAIT.2018.8369633
15. Zhang, N., Luo, J., Gao, W.: Research on face detection technology based on MTCNN. In: 2020 International Conference on Computer Network, Electronic and Automation (ICCNEA), pp. 154–158 (2020). https://doi.org/10.1109/ICCNEA50255.2020.00040
16. Sharma, S., Shanmugasundaram, K., Ramasamy, S.K.: FAREC—CNN based efficient face recognition technique using Dlib. In: 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp. 192–195 (2016). https://doi.org/10.1109/ICACCCT.2016.7831628

17. Hiran, K.K., Doshi, R., Fagbola, T., Mahrishi, M.: Cloud Computing: Master the Concepts, Architecture and Applications with Real-World Examples and Case Studies. Bpb Publications (2019)
18. Mahrishi, M., Hiran, K.K., Doshi, R.: Selection of cloud service provider based on sampled non-functional attribute set. In: Abraham, A., Siarry, P., Ma, K., Kaklauskas, A. (eds.) ISDA 2019. AISC, vol. 1181, pp. 641–648. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-49342-4_62

Author Queries

Chapter 24

Query Refs.	Details Required	Author's response
AQ1	This is to inform you that corresponding authors have been identified as per the information available in the Copyright form.	
AQ2	Please check and confirm if the inserted citation of Fig. 1 is correct. If not, please suggest an alternate citation.	
AQ3	To maintain sequential order, figures and its citations have been renumbered. Please check and correct if necessary.	
AQ4	Reference [1–18] are given in the list but not cited in the text. Please cite this in text or delete this from the list.	
AQ5	As References [1] and [13] are same, we have deleted the duplicate reference and renumbered accordingly. Please check and confirm.	