

DEVELOPMENT OF DETECTION SYSTEM ON SUSPICIOUS BEHAVIOUR DURING EXAM

Ili Nadia Karim
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
ili.karim01@s.unikl.edu.my

Diyana Ab Kadir
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
diyana@unikl.edu.my

Fuead Bin Ali
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
fuead@unikl.edu.my

Abstract—Development of Detection System on Suspicious Behaviour During Exam using Image Processing (D²S²BDE) is a project that detect student suspicious behaviour during exam. Students intend to cheat during exam and the invigilator did not notice the students who cheat. This project is meant to discourage student from cheating during exam. The objectives of this project are to detect student suspicious behaviour using images processing, to analyse the suspicious behaviour and save the images as evidence. The methodology use in this project is prototype model methodology. By using prototype model, error may be detected earlier before implementing it into the real environment. This project detects suspicious behaviour such as peeking, exchanging notes, and talking during exam by capturing the real-time video of them using the webcam camera. An analysis is to be conducted on the suspicious images data that have been trained. If the success rate is high, the particular suspicious behaviour will be captured as evidence. This project used Faster-RCNN and Yolov4 models, which are going to be compared among them in term of performance. These two models are trained in two different platforms; Faster-RCNN is trained locally in laptop while Yolov4 is trained in cloud platform. The development of the system is done using Acer Aspire 5 laptop. According to result of the study on related topic, it shows that cheating during exam among student is high and it becomes a concern towards student growth. Cheating habit is an unethical habit that should be fixed or prevented. Hopefully, by having this project running, the students can be more honest in answering the exam paper.

Keywords—Faster-RCNN, Yolov4, Locally, Cloud platform

I. INTRODUCTION

Cheating during exam is unethical and might be practiced by some students. This behaviour is unfair to the students who do not cheat and work hard to study. Furthermore, it may impact the individual itself if they are caught red-handed. Some institution gives a strict punishment to students who cheat during final exam. The example of punishment is such as fail the subject or get expelled from school. The main idea of this “Development of Detection System on Suspicious Behaviour during Exam” using image processing (D²S²BDE) project is to prevent cheating and to help invigilators in supervising student during exam.

The project is using the real time video of students to recognize student suspicious behaviour. To accomplish the goal, image processing and computer vision techniques are to be used to execute the project. Computer vision is a field of computer science that enable computers to see, discover and process photos in the same manner that human vision does, and then provide suitable output. Computer vision falls under artificial intelligent (AI) technology with an example such to unlock phone by recognizing the owner's face.

The research gap of the project is that the previous projects are not saving the image of the suspicious behaviour as an evidence, in case to prove the student wrongdoing. With the proposed system, hopefully it will discourage student from cheating during exam and will assist the invigilator to monitor the students.

II. RELATED WORKS

A. Suspicious Human Activity Detection in Classroom Examination

The journal [1] is a study to detect suspicious human activity in classroom examination. The focus of in journal are the face region of the students, hand contact detection and hand signalling. Face region detection and monitoring of the students is using Haar feature Extraction. Haar can detect face only if the face orientation does not exceed above 30 in all other directions. Next, to detect hand contact detection. background subtraction is a major pre-processing step where the foreground is extracted from the static background. Hand movement based on constructing a grid for every student in an examination hall and a group vector line segmenting each rows and columns grid formation because the classroom is set as a fixed environment. Thirdly, to detect and recognize the hand signalling by skin colour detection and convex hull. A Convex hull is drawn around the hand contour that uses minimum points in the contour region to form the hull and maintains the convexity property.

B. Cheating Video Description Based on Sequence of Gestures

Based on journal [2], this project is to develop a cheating video description based on human gesture. The goal of this projects are human detection, human activity analysis, and human interaction analysis. The human detection gesture is using Mixture of Gaussin(MOG) background subtraction. OpenCV is used because it can model the pixel values of the video using multiple distributions allowing a more complex model. Gesture recognition model to predict the detected cheating gestures of a short video chunk are using 3D CNN as a feature and XGBoost as a classifier. A language model was built to generate text based by using long short-term memory (LSTM) network. For the hardware, it uses Intel i7-4700HQ 2.4GHz processor and NVidia 745M 2Gb GPU on Windows 7 64 Bit and the result shows that this type of laptop may run at real-time very well.

C. Suspicious Human Activity Detection

According to [3], the journal discusses on detecting human suspicious activity in certain place. The activities covered are such as talking in the exam hall, sleeping in classroom et cetera. The method to detect unwanted activities is by analysing the hand gestures and the head movement of the person. This project is not using a real-time video, but it is analysing the frames from the video input. At first, the video needs to be converted into frames and stored. Then the frames must be pre-processed to eliminate the noise in the frames. After that, the area of interest has to be subtracted from its background. To subtract the background, it must detect the edge of the object. After the elimination, the algorithm for the face detection used to detect the faces in the image. To proceed further, the persons in the image must be identified. This should be possible by matching the example with the database. If the activity done by the person is seen as suspicious, the concerned higher authorities will be alerted, and the subtleties of the people associated with the action must be sent to them.

D. Online Surveillance for Exam

In journal [4], the intent is to develop a system to automatically detect suspicious activity during online examination. The goal of this project is to design and create a system of video surveillance and monitoring that will provide easy access to live frames during an online analysis of institutions. This system allows us to identify the face that moves out of the candidate's online exam frame and will give the notification to the administrator. The face detection starts after the student logged in, the student face is detected, and the frame is set as per the student face positions. The background of the student will be freeze during the whole Online Examination and real-time notifications will be sent to admin and the beep sound occurs. The face detection is using Haar classifier algorithm that proposed by Viola and Jones and is applied in OpenCv. Haar like features are calculated and are determined by comparing the variance of pixel in nearby pixel classes.

E. An Automatic Method for Cheating Detection in Online Exams by Processing the Student's Webcam Images

Research by [5] is detecting cheating behaviour using image processing. The first method is by using functions from Matlab for image processing and comparing. This is comparison in detection of difference between two images by calculating subtraction between the pixels of two image. Secondly, clustering 50 images of students before an exam using clustering algorithm. Third method is using k-medoids clustering algorithm. After implementing this method, researchers found that it is not an appropriate method. Researcher makes calculation of mean data in each cluster and consider these mean values as the new centres of clusters every k-means algorithm iteration.

III. PROPOSED METHOD

The "Development of Detection System on Suspicious Behaviour During Exam" using image processing is proposed so that it is able to recognise suspicious behaviour during exam such as exchange note, peeking and talk with neighbour. The recognised actions will be captured, analysed and displayed on the monitor with a bounding box in red colour. It also saves image frames at high percentage as evidence.

A. Hardware and Software

To capture a real-time video, we need a good quality of USB webcam for better detection and wide view coverage to detect two students in one frame with space between two students. JVCU webcam has 80° view cover and has high resolutions with 1080 pixels. JVCU webcam comes with function 30 frame per second will help a lot during data collection.

This project is using Laptop Acer Aspire 5, the graphic processing unit (GPU), Nvidia MX250, which is capable to

process deep learning data. GPU is going to boost up the training of deep learning models, and it can do multiple computations simultaneously without lacking.

In the analysis stage, we compare detection between two methods which are Faster-RCNN model and Yolov4 model. Faster-RCNN is known with high accuracy, while Yolov4 is a new model, making a debut in April 2020 and claim as a faster detection. Anaconda will be used for developing Faster-RCNN and needs to install the requirement locally such as OpenCV library and Tensorflow library. OpenCV is for the computer vision purpose while Tensorflow is for deep learning purpose. Meanwhile, the Google Colab is used to execute Yolov4 method because Google Colab has zero configuration required.

B. Block Diagram

For Faster-RCNN model, the local dataset was trained through Anaconda software. The steps are as shown in Figure 1. While for Yolov4 model, the datasets were picked up from Google drive, then being trained through Google Colab as per Figure 2. If the suspicious behaviour was detected, then the image of it will be cropped from the frame.

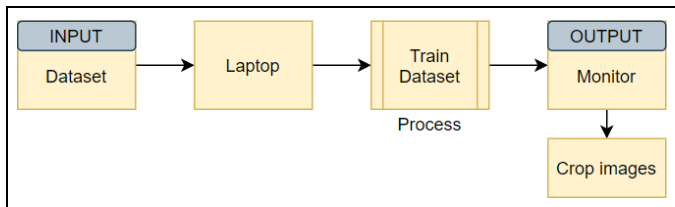


Figure 1: Faster-RCNN

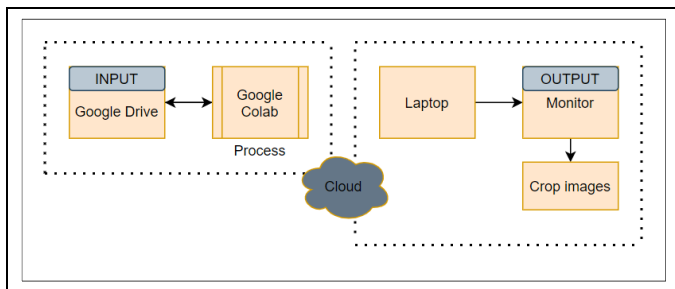


Figure 2: Yolov4

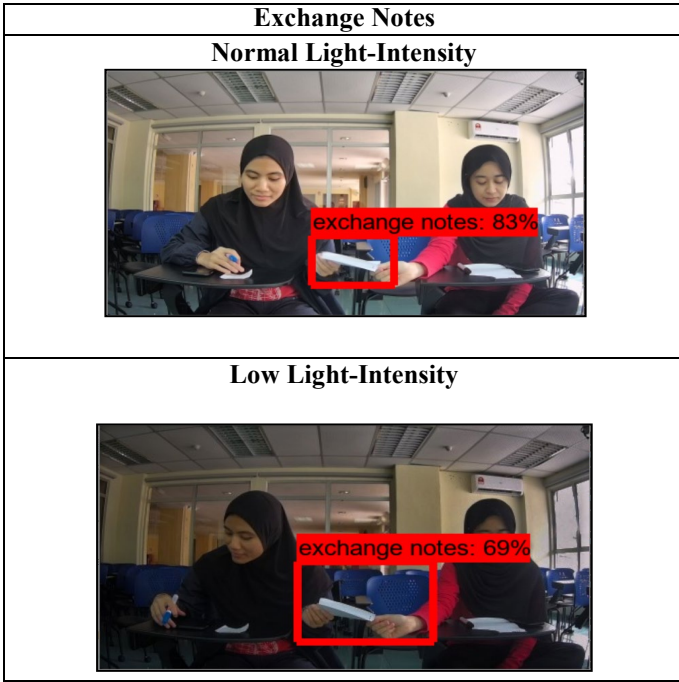
IV. RESULT

The testing phase is divided into three parts: Peeking, Talking and Exchange notes. These tests are conducted based on two criteria of image settings; first during the normal-light intensity and second test during low-light intensity. These tests are conducted using Faster-RCNN model and Yolov4 model.

A. Faster-RCNN

Table 1: Faster-RCNN results

<p>Peeking</p> <p>Normal Light-Intensity</p>
<p>Low Light-Intensity</p>
<p>Talking</p> <p>Normal Light-Intensity</p>
<p>Low Light-Intensity</p>



According to result in Table 1, it shows that in low-light intensity, we are getting a lower detection percentage rather than normal-light intensity.

B. Yolov4

Table 2: Yolov4 model results





From Table 2, all behaviour shows that in low-light intensity, they recorded a lower detection percentage compared to the normal-light intensity except for talking. Talking action recorded higher 0.02% in a low-light intensity than in normal-light intensity.

C. Compare Faster-RCNN and Yolov4 in Normal Light Intensity

Table 3: Compare in Normal Light Intensity

Peeking	
<p>Faster-RCNN</p> 	
<p>Yolov4</p> 	

Talking	
<p>Faster-RCNN</p> 	
<p>Yolov4</p> 	

Exchange Notes	
<p>Faster-RCNN</p> 	
<p>Yolov4</p> 	

According to Table 3, normal-light intensity Yolov4 have low accuracy for detecting a small object rather than Faster-RCNN but talking in Yolov4 model getting higher detection rate than Faster-RCNN model.

D. Compare Faster-RCNN and Yolov4 in Low Light Intensity

Table 4: Compare in Low Light-Intensity

Peeking	
<p>Faster-RCNN</p> 	
<p>Yolov4</p> 	



images in a folder as evidence. The high percentage is being set at more than 50%.

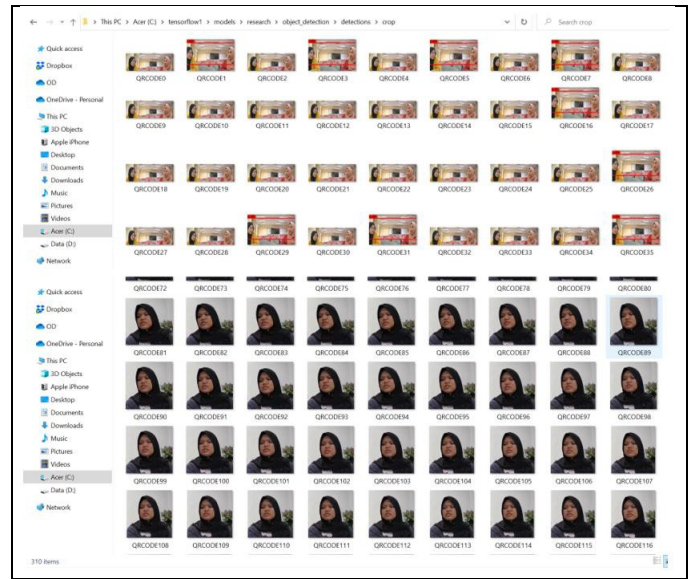


Figure 3: Suspicious Behaviour Faster-RCNN

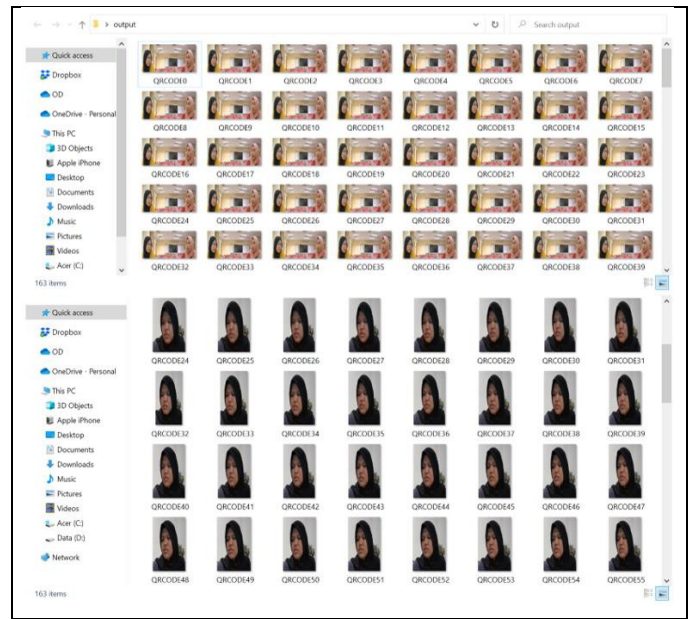
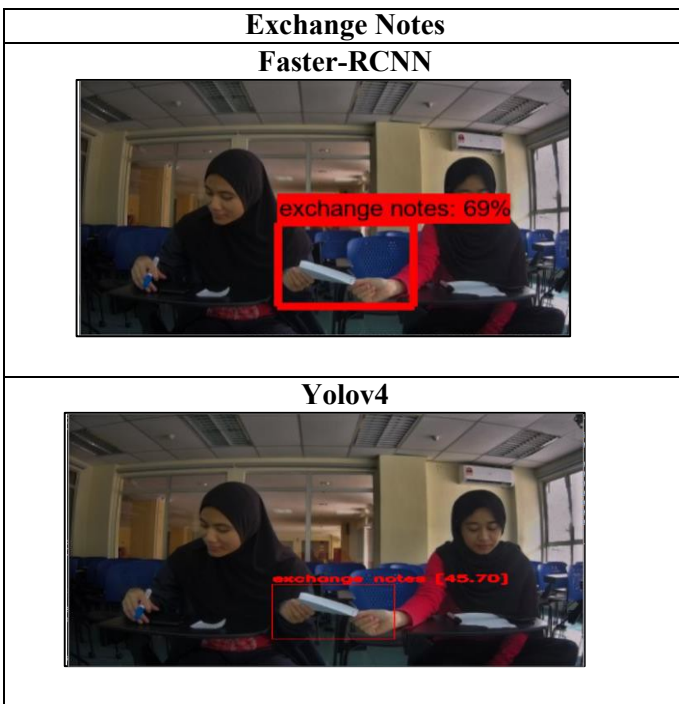


Figure 4: Suspicious Behaviour Yolov4

Based on Table 4 in low-light intensity testing, Faster-RCNN has better detection than Yolov4 except for talking, which Yolov4 has better detection.

E. Save Images of Suspicious Behaviour

From detection done in the previous testing phase, the detected suspicious behaviour at high percentage will save as

Figure 3 and Figure 4 shows that the system can successfully crop and store the suspicious images in a folder.

F. Speed Detection

The different processing speed detection between the two models were being tested.

Table 5: Speed Comparisons

	Video length	Faster-RCNN	Yolov4
1.	4 seconds	1 minutes 7 seconds	22 seconds
2.	6 seconds	1 minutes 43 seconds	17 seconds
3.	7 seconds	1 minutes 19 seconds	32 seconds
4.	8 seconds	2 minutes 21 seconds	39 seconds
5.	9 seconds	1 minutes 47 seconds	27 seconds
6.	12 seconds	3 minutes 1 seconds	54 seconds
7.	16 seconds	3 minutes 26 seconds	1 minutes 9 seconds
8.	20 seconds	3 minutes 51 seconds	1 minutes 40 seconds

Based on Table 5, it indicates that in terms of speed, Yolov4 is having a faster detection rate compared to Faster-RCNN model.

V. DISCUSSION

After training both models, the data that needs to be taken have to be in different angles to get better accuracy and the more the images trained, the better detection we can get. Upon testing, several findings are discussed. Firstly, the system detects suspicious behaviour at a higher percentage when in the normal-light intensity state. The percentage drops slightly when in low-light intensity but the percentage is still above 50%. However, there was an exception for talking behaviour using Yolov4 model, which detected a higher percentage in low-light intensity.

Next, Faster-RCNN shows that it can detect smaller things better than Yolov4. Refer to Table 3 and Table 4, they show that Faster-RCNN getting higher percentage than Yolov4 for both conditions, which in normal-light intensity and in low-light intensity. Besides that, Faster-RCNN also can detect peeking better during low-light intensity but getting the same percentage with Yolov4 for normal-light intensity.

However, in terms of speed, Faster-RCNN is a complicated model for detection using the real-time video. It is taking a lot of time even though it is a short video. The higher movement in the video, the slower Faster-RCNN will do the processing while Yolov4 has the better speed in term of processing.

Last but not least, saving images of suspicious behaviour is successfully working for both models. In order to use this functionality, Yolov4 need to be installed in laptop locally with different versions of Cuda, cuDNN and the different type of software that use by Yolov4. Those images will be saved in the folder that has been set. The images are being cropped depend on bounding box that shows up during detection. The smaller the bounding box detection, the smaller the images saved in the folder.

VI. CONCLUSION

The first objective set for this project which is to recognize a suspicious behaviour (talking, peeking and exchange notes) during an exam and second objective is to save the images of suspicious behaviour at the high percentage as evidence. From the results obtained in result section, it can be concluded that both objectives were achieved.

From this project, we recommend Yolov4 to be used for detection during the real-time video, however for a better accuracy of detection, Faster-RCNN is the right model to be used.

REFERENCE

- [1] T. Senthilkumar and G. Narmatha, "Suspicious Human Activity Detection in Classroom Examination," 2016, pp. 99–108.
- [2] A. Arinaldi and M. I. Fanany, *Cheating Video Description Based on Sequences of Gestures*. 2017.
- [3] P. P. Nandini. G, Dr. B. Mathivanan, Nantha Bala. R. S, "Suspicious human activity detection," *Int. J. Adv. Res. Dev.*, vol. Volume 3, no. Issue 4, pp. 12–14, 2018.
- [4] P. V. S. Nikhil Desai, Komal Pathari, Juice Raut, "Online Surveillance for Exam," *Int. J. Recent Trends Eng. Res.*, vol. 4, no. 3, pp. 331–336, 2018.
- [5] K. Jalali and F. Noorbehbahani, *An Automatic Method for Cheating Detection in Online Exams by Processing the Student's Webcam Images*. 2017.