Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Real Time Snatch Theft Detection using Deep Learning Networks

Nurul Farhana Mohamad Zamri[1], Nooritawati Md Tahir[1,2,*], Megat Syahirul Megat Ali[1,3], Nur Dalila Khirul Ashar[4], Ali Abd Almisreb[5]

[1] School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Selangor, Malaysia
[2] Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA, Selangor, Malaysia
[3] Microwave Research Institute (MRI), Universiti Teknologi MARA, Selangor, Malaysia
[4] School of Electrical Engineering, Universiti Teknologi MARA, Johor, Malaysia
[5] Department of Computer Science and Engineering, Faculty of Engineering and Natural Sciences, International University of Sarajevo, Sarajevo, Bosnia and Herzegovina

ARTICLE INFO

Article history:
Received 15 January 2023
Received in revised form 17 May 2023
Accepted 26 May 2023
Available online 13 June 2023

Keywords:
Real-time detection; snatch theft; deep learning; image classification

ABSTRACT

Snatch theft is a common crime in urban areas that poses a serious threat to public safety. It involves forcefully grabbing a victim's personal belongings, such as purses or mobile phones, before quickly fleeing the scene. Detecting snatch theft incidents in real-time is a challenging task due to the speed at which they occur. The current methods used to detect snatch theft incidents rely heavily on human intervention, which can lead to significant delays and potential errors. Therefore, there is a need for an automated technique that can accurately and efficiently detect these incidents in real-time. Hence, the study aims to detect snatch theft using a transfer learning approach based on eight pre-trained convolutional neural networks (CNNs) as classifiers: AlexNet, VGG16, VGG19, GoogleNet, InceptionV3, ResNet-18, ResNet-50, and ResNet-101. The modified pre-trained CNN models are evaluated in both offline and real-time modes. Based on the offline mode, VGG19 achieved 100% training accuracy, and ResNet50 had the highest testing accuracy of 98.9%. In the offline mode, all models accurately classified normal scenes, with ResNet-10 having the lowest false negative rate and ResNet-50 achieving the lowest false positive rate with only 44 misclassified anomaly frames related to snatch theft. The study further evaluated and validated the eight models in real-time mode, and the results showed that AlexNet and ResNet-18 were the only models capable of categorizing snatch theft scenarios with promising findings.

1. Introduction

Murder, shooting, drug trafficking, concealment, fraud, black marketing, and other crimes occur worldwide. Investigating the overall trends of the crimes that occur in any country is necessary to better understand the most prevalent crimes and their rates in particular places. Crimes usually happen when the offender's activity space overlaps with the victims' spaces. It should be noted that

* *Corresponding author.*
E-mail address: nooritawati@ieee.org

https://doi.org/10.37934/araset.31.1.7989

a person's activity space includes places such as their workplace or office, school, home, shopping mall, or recreational areas.

In contrast, street crimes such as mugging, pickpocketing, and snatch theft occur in public places [1]. Although authorities have implemented numerous action plans to reduce crime rates and raise awareness about street crime, the crime index continues to rise throughout the year. Snatch theft is a criminal conduct in which a pedestrian's personal belongings, such as a necklace, cell phone, and handbag, are forcibly taken. This crime is committed using either running or robbery techniques. Nowadays, one of the most common street crimes is snatch theft [3], which usually involves two persons, one handling the motorcycle and the other committing the crime or stealing [3]. This is a concerning issue among pedestrians since it can harm and cause worry, trauma, and shock.

Pedestrians are sometimes unaware of their surroundings, creating more opportunities for perpetrators to commit crimes. Nowadays, the use of closed-circuit television (CCTV) as surveillance cameras is becoming increasingly common in public places such as streets, banks, parking lots, and residential units as a preventative measure against crime. The primary function of surveillance cameras is to monitor and record any abnormal behavior in the neighborhood, and detection is done manually by humans. Although humans may classify the snatch theft scenario, machines face significant difficulties. Many regions have already installed CCTV that allows users to monitor or record their daily activities, but manually watching the prolonged video of CCTV can be tiresome and exhausting. Therefore, it is vital to establish a feasible method using machine learning techniques to detect anomalous activities automatically.

Conversely, numerous types of research on crime classification have been explored. Each study made use of its distinct features. Most of these features were considered physical traits. The most commonly used features are facial information by Xia *et al.,* [4] and a scene of the incident by Mandal and Choudhury [5]. However, snatch theft perpetrators typically wear helmets when conducting crimes, and obtaining facial information is sometimes impossible. Thus, artificial intelligence (AI) could be utilized to categorize and use snatch theft footage or pictures. Hence, the snatch theft crime pattern was used as an effective characteristic in snatch theft classification as reported in previous work [6-7].

In addition, pre-trained CNN models that utilize transfer learning offer alternative methods that can provide better outcomes, faster training, and are also suitable for processing fewer input data. Transfer learning can be used on two types of pre-trained CNNs: series networks that include AlexNet, VGG-16, and VGG-19, and directed acyclic graph (DAG) networks, such as GoogLeNet, Inception-v3, ResNet-18, ResNet-50, and ResNet-101 [8-14]. Technically, transfer learning takes the knowledge of pre-trained CNNs that have previously learned on a large dataset and applies it to discover new, related, or even complete tasks in different domains.

Moreover, convolutional network layers for image classification are generally divided into two sections: the convolution base and the dense base. Both approaches use the convolution base of pre-trained CNNs to obtain reusable knowledge of learned weights. However, the dense base usually requires fine-tuning of the layers or hyperparameters since it has specific knowledge of the primary task that is not necessarily relevant to the current assignment [15].

Researchers in crime surveillance and detection heavily rely on anomalous data to help them improve their results [5,8,16]. Anomaly detection is a method or process for identifying behavior that deviates from normal behavior, which can be complex and diverse from normal behaviors. This strategy has been used in many research studies on human behavior anomalies, either individually or in groups, in high and low crowd-density circumstances. For example, these researchers were predicting unusual behavior when someone wields a firearm [11,17,18], detecting suspicious

abandoned luggage [16], or detecting unusual behavior in public places such as ATMs, banks, and elevators [4-5].

Additionally, street and theft offenses are among the most severe crimes committed worldwide. Petty crime, such as snatch theft, is increasing, particularly in light of the global economic downturn. Snatch theft is the criminal act of stealing pedestrians' necklaces, cell phones, handbags, and other possessions. Criminals frequently employ the run-and-rob tactic when committing crimes. This tactic involves a partnership between two individuals, one handling the motorcycle and the other stealing from the intended victim [3]. For instance, [8] used 21 videos as a database. The researchers employed the VGG19 convolution neural network (CNN) to distinguish large-scale images or videos of snatch theft crimes and achieved 81% accuracy in identifying snatch theft. In addition, a public system security, a video surveillance system comprising four sequential blocks, namely data collection, object detection, feature extraction, and scene categorization, was built. The monitoring in this study by Goya *et al.,* [19] was based on human motion, with optical flow and background subtraction used to calculate the object's speed in the target scene.

Hence, this paper aims to investigate the capability of deep learning in detecting snatch theft in real-time, based on findings attained during offline that have shown high accuracy in detecting anomalous behavior using the proposed transfer learning [15].

2. Methodology

2.1 Data Acquisition

The database comprises videos collected from YouTube and Google platforms, with a total of 120 videos divided into two datasets: 60 anomaly videos and 60 normal videos. For training, 42 videos (70%) were used for both abnormal and normal scenes, while the remaining 18 videos (30%) were used for testing. The total number of frames for training was 4488, while that for testing was 2032. The total frames for both normal and anomaly scenes were similar.

2.2 Transfer Learning

CNNs have shown promising results in various applications, including classification, modeling, and prediction. One of the significant advantages of CNNs is their ability to learn from examples, making them a powerful tool. Transfer learning is a machine learning method that leverages knowledge acquired in one environment to improve performance in another, even when modeling a different set of tasks. Transfer learning has greatly benefited deep learning with image data by providing the best architecture of pre-trained CNN models and enabling better results with fewer data [7,20,21].

2.3 Pre-Trained CNN

The first step is to select a pre-trained CNN model. Pre-trained CNN models and deep learning share similar characteristics in terms of training datasets, which are usually large and complex. MATLAB offers two types of pre-trained CNN models, as shown in Table 1. Pre-trained CNN models with series networks have a sequential architecture of layers with fewer layers but a large number of trainable parameters.

Table 1
Popular pre-trained CNN models

Network	Deep Layers	Total Layers	Layers Connection
Series			
AlexNet	8	25	25
VGG16	16	41	41
VGG19	19	47	47
DAG			
InceptionV3	22	144	170
GoogleNet	42	316	350
ResNet-18	18	72	79
ResNet-50	50	177	192
ResNet-101	101	347	379

On the other hand, pre-trained CNN models with DAG networks have more layers arranged in a directed acyclic graph, but fewer trainable parameters. The construction of graph layers is more intricate since network variables are not limited to connecting layers one after the other. The layers may have numerous variables as input and output connections. In this study, both types of pre-trained networks were used to train both normal and abnormal datasets. Three pre-trained Series networks, namely Alex Net, VGG16, and VGG19, were rebuilt, while five pre-trained networks, namely Google Net, Inception-v3, ResNet-18, ResNet-50, and ResNet-101, were redesigned as DAG networks. The transfer learning approach yielded comparable results for all pre-trained networks.

In pre-trained CNN models, the final three layers of the dense base are typically configured for 1000 classes. However, in this study, these layers were substituted with three new layers to generate two types of snatch theft scenes, as shown in Table 2. No additional layers were added to synchronize with pre-trained layers. The learning rate hyperparameter of the newly added layer was increased for the weights and biases in the new fully connected layer to learn faster. The DAG network's regularization factor hyperparameters remained stable during the learning phase.

Table 2
Transfer learning process of series networks and DAG networks

Parameters	Pre-Trained Series Network	Remodeled Pre-Trained Series Network
Fully Connected Layer	Layer (end-3):	Layer (end+1):
Learning Rate of Weight	1	10
Learning Rate of Bias	2	10
Regularization Factor of Weight	1	1
Regularization Factor of Bias	0	0
SoftMax Layer	Layer (end-2):	Layer (end+2):
Classification Output Layer	Layer (end-1):	Layer (end+3):

2.4 Preventing Overfitting for Improving Machine Learning Models

To prevent overfitting, all CNN models in this study utilized data augmentation and early stopping techniques. Augmentation techniques such as rotation, Y reflection, translation, and scaling were applied during training, as shown in Figure 1, to increase the model's ability to generalize as described by Guo *et al.,* [22] Early stopping was used to stop training before the model starts learning the noise within the data, which helps ensure that the model fits the data well [23].

Fig. 1. Example of images upon augmentation

2.5 Real-Time Mode Implementation

Machine learning has demonstrated that deep neural networks outperform traditional methods significantly. For instance, Deep Anomaly Detection (DAD) algorithms are employed in real-time Big Data applications [24]. There are numerous scenarios where data needs to be analyzed in real-time, as analyzing data offline would either generate no results or lead to significant losses. In most cases, these scenarios deal with large amounts of rapidly changing data in a complex context. Deep learning algorithms are ideal for this purpose due to their scalability, particularly for real-time detection. For example, Arefin *et al.,* [25] used Alexnet to recognize real-time scenarios of several distracted driving behaviors and achieved 93% detection accuracy. Similarly, Muhammad *et al.,* [26] detected fire in photos with 94% accuracy using image analysis. In terms of real-time flame detection, the authors reported a false alarm rate of 0.054%. Furthermore, Guo *et al.,* [22] used real-time detection to identify an insulator and a bird's nest on a transmission line, with the bird's nest being classified as an abnormality. The maintenance crew of the transmission line was promptly informed of the situation. As previously stated, real-time detection is utilized in this study to evaluate the effectiveness of the proposed deep-learning network.

3. Results

This section discusses the results obtained using the proposed method. Table 3 lists the accuracy and sensitivity of each remodelled pre-trained CNN model. The training time for the Series networks AlexNet, VGG16, and VGG19 is 2 hours, 10 hours, and 24 hours, respectively. Meanwhile, GoogleNet, InceptionV3, ResNet-18, ResNet-50, and ResNet-101 of DAG networks take 2 hours, 18 hours, 3 hours, 9 hours, and 20 hours, respectively. Table 3 summarizes the total number of iterations, training accuracy, and testing accuracy for all models. Compared to other models, VGG19 achieved 100% training accuracy, but performed poorly in testing, scoring only 96.9%. ResNet50 obtained the best score for testing accuracy, with 98.9%. However, despite having the highest training score, VGG19 did not perform as well in testing. The results showed that the remodelled AlexNet produced false positives with the highest number of misclassified anomaly frames, specifically 441 frames.

Figure 2 depicts some examples of misclassified images during the classification stage, including false positive and false negative images**.**

Table 3
Results of remodeled pre-trained CNN models

Remodelled Pre-Trained CNN models	Total iteration	Train Accuracy (%)	Test Accuracy (%)	Misclassified Images		
				Normal	Anomaly	Total
AlexNet	701	99.66	89.1	0	441	441
VGG16	121	98.05	95.1	0	199	199
VGG19	301	100	96.9	0	128	128
GoogleNet	451	99.89	89.4	0	431	431
IncecptionV3	803	95.41	93.9	0	249	249
ResNet-18	721	97.94	92.4	0	308	308
ResNet-50	930	96.22	98.9	0	44	44
ResNet-101	930	99.77	98.7	3	48	51

Fig. 2. Misclassified images of remodelled pre-trained CNNs for anomalous behaviour

Overall, all models successfully classified normal scenes as "normal" except for ResNet-101, which obtained false negative results with three misclassified normal frames. In contrast, the remodelled ResNet-50 achieved the lowest false positive rate with 44 misclassified anomaly frames. In order to further evaluate the proposed method in real-time mode, snatch theft detection analysis was conducted using the fifteen frames presented in Figure 3. The real-time scenario was based on a situation where a subject snatched an item while running, as it comprised both normal and anomalous scenes related to snatch theft. The detection of snatch theft began with "normal," followed by "anomaly" as the subject attempted to snatch the victim's handbag and then back to "normal" once the perpetrator had left the scene. The results indicated that only AlexNet and ResNet18 were able to distinguish the anomaly and normal scenes, while the other CNN models failed to recognize all the normal scenes as "normal" and instead recognized some of these misclassified scenes as "anomaly." Figure 3 also presents the time taken by AlexNet and ResNet18 to

detect each frame, which included 15 frames from each scenario of snatch theft and a normal scene. Note that the red colour bars represent incorrectly classified frames. It was observed that AlexNet misclassified three "anomaly" scenes in frames 5, 9, and 12 as "normal."

In comparison, ResNet18 misidentifies two anomaly scenes as 'normal' - namely, the 8th and 9th frames. As for detection time, AlexNet takes between 0.06 and 0.12 seconds, while ResNet18 takes between 0.04 and 0.12 seconds. For detecting normal scenes, AlexNet takes between 0.02 to 0.09 seconds, and ResNet18 takes 0.02 to 0.1 seconds. However, both AlexNet and ResNet18 successfully classify all normal scenes.

To further validate the effectiveness of AlexNet and ResNet18, another scenario is used, as shown in Figure 4, which involves a motorcyclist snatching act. As depicted in Figure 4, the detection for snatch theft begins with 'normal', then 'anomaly' once the perpetrator on the motorbike attempts to snatch the victim's handbag, and back as 'normal' after the perpetrator leaves the scene. AlexNet detects anomalous scenes in the 6th, 9th, and 10th frames as 'normal' with a detection time between 0.05 and 0.13 seconds. AlexNet correctly classifies all normal scenes. As for ResNet18, the detection time is between 0.04 and 0.12 seconds, with the wrongly classified frames including the 3rd frame, which is actually a normal scene, and three normal scenes incorrectly classified as abnormal, namely the 6th, 7th, and 10th frames. Therefore, based on these findings in real-time mode, it can be summarised that the ability of ResNet18 and AlexNet to be used as classifiers for snatch theft detection is indeed promising, based on the detection time and accuracy obtained.

4. Conclusions

In conclusion, this study analysed and validated the effectiveness of eight CNN models in identifying and distinguishing snatch theft detection using transfer learning methods. While the remodelled CNN models showed promising results in identifying both normal and abnormal activities during offline mode, most models failed to perform well in real-time mode, except for AlexNet and ResNet-18 (Figure 3). These two models demonstrated accurate detection and quick response times. Additionally, they were tested on another scenario of motorcyclist snatching, and AlexNet was found to perform better than ResNet-18 (Figure 4). Future work includes incorporating forensic gait analysis to examine the anomalous behaviour and posture of the thief, as well as developing a method to eliminate false alarms.

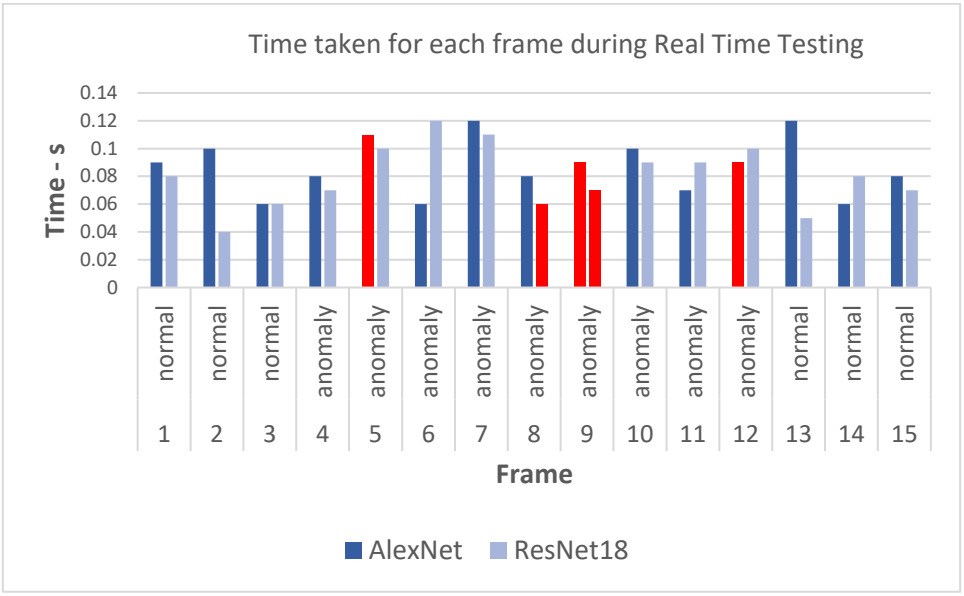

Fig. 3. Result of Real-Time testing for AlexNet & ResNet18 for all 15 frames and ResNet18 versus Time

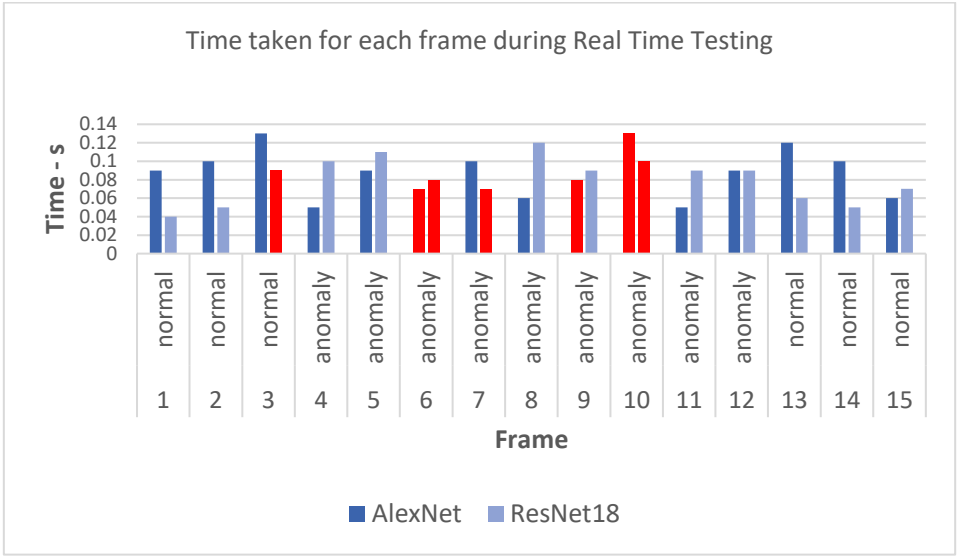

Fig. 4. Result Real-Time for AlexNet and ResNet18 versus Time based on Scenario Motorcyclist Snatching

Acknowledgement

This research was funded by the Ministry of Higher Education (MOHE) Malaysia, Grant No: 600-IRMI/FRGS 5/3 (394/2019), Sponsorship File No: FRGS/1/2019/ TK04/UITM/01/3. The authors

would like to thank the College of Engineering, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia for the facilities provided in this research.

References

[1] Truntsevsky, Yu V., I. I. Lukiny, A. V. Sumachev, and A. V. Kopytova. "A smart city is a safe city: the current status of street crime and its victim prevention using a digital application." In *MATEC Web of Conferences*, vol. 170, p. 01067. EDP Sciences, 2018. https://doi.org/10.1051/matecconf/201817001067

[2] Latimaha, Rusli, Zakaria Bahari, and Nor Asmat Ismail. "Examining the linkages between street crime and selected state economic variables in Malaysia: A panel data analysis." *J. Ekon. Malays* 53 (2019): 59-72. https://doi.org/10.17576/JEM-2019-5301-6

[3] Salleh, Mohd Najib Moihd. "Linear Street Pattern in Urban Cities in Malaysia Influence Snatch Theft Crime Activities." *Environment-Behaviour Proceedings Journal* 3, no. 8 (2018): 189-199. https://doi.org/10.21834/e-bpj.v3i8.1386

[4] Xia, Yizhang, Bailing Zhang, and Frans Coenen. "Face occlusion detection based on multi-task convolution neural network." In *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, pp. 375-379. IEEE, 2015. https://doi.org/10.1109/FSKD.2015.7381971

[5] Mandal, Rupesh, and Nupur Choudhury. "Automatic video surveillance for theft detection in ATM machines: An enhanced approach." In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 2821-2826. IEEE, 2016.

[6] Dorogyy, Yaroslav, Vadym Kolisnichenko, and Kseniia Levchenko. "Violent crime detection system." In *2018 IEEE 13th international scientific and technical conference on computer sciences and information technologies (CSIT)*, vol. 1, pp. 352-355. IEEE, 2018. https://doi.org/10.1109/STC-CSIT.2018.8526596

[7] Cai, Jingye, Jianhua Deng, Muhammad Saddam Khokhar, and Muhammad Umar Aftab. "Vehicle classification based on deep convolutional neural networks model for traffic surveillance systems." In *2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 224-227. IEEE, 2018.

[8] Butt, Umair Muneer, Sukumar Letchmunan, Fadratul Hafinaz Hassan, Sultan Zia, and Anees Baqir. "Detecting video surveillance using VGG19 convolutional neural networks." *International Journal of Advanced Computer Science and Applications* 11, no. 2 (2020). https://doi.org/10.14569/IJACSA.2020.0110285

[9] He, Kaiming, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. "Deep residual learning for image recognition." In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770-778. 2016. https://doi.org/10.1109/CVPR.2016.90

[10] Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton. "Imagenet classification with deep convolutional neural networks." *Communications of the ACM* 60, no. 6 (2017): 84-90. https://doi.org/10.1145/3065386

[11] Nakib, Mohammad, Rozin Tanvir Khan, Md Sakibul Hasan, and Jia Uddin. "Crime scene prediction by detecting threatening objects using convolutional neural network." In *2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2)*, pp. 1-4. IEEE, 2018. https://doi.org/10.1109/IC4ME2.2018.8465583

[12] Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." *arXiv preprint arXiv:1409.1556* (2014).

[13] Zakaria, Fazrul Faiz, Asral Bahari Jambek, Norfadila Mahrom, Rafikha Aliana A. Raof, Mohd Nazri Mohd Warip, Phak Len Al Eh Kan, and Muslim Mustapa. "Tuberculosis Classification Using Deep Learning and FPGA Inferencing." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 3 (2023): 105-114. https://doi.org/10.37934/araset.29.3.105114

[14] Alias, Nur Ain, Wan Azani Mustafa, Mohd Aminudin Jamlos, Shahrina Ismail, Hiam Alquran, and Mohamad Nur Khairul Hafizi Rohani. "Pap Smear Image Analysis Based on Nucleus Segmentation and Deep Learning–A Recent Review." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 3 (2023): 37-47. https://doi.org/10.37934/araset.29.3.3747

[15] Zamri, Nurul Farhana Mohamad, Nooritawati Md Tahir, Megat Syahirul Amin Megat Ali, and Nur Dalila Khirul Ashar. "Snatch Theft Detection Using Deep Learning Models." In *Proceedings of the Future Technologies Conference (FTC) 2022, Volume 1*, pp. 260-274. Cham: Springer International Publishing, 2022.

[16] Loganathan, Sathyajit, Gayashan Kariyawasam, and Prasanna Sumathipala. "Suspicious activity detection in surveillance footage." In *2019 International Conference on Electrical and Computing technologies and applications (ICECTA)*, pp. 1-4. IEEE, 2019. https://doi.org/10.1109/ICECTA48151.2019.8959600

[17] Karim, Shahid, Ye Zhang, Asif Ali Laghari, and Muhammad Rizwan Asif. "Image processing based proposed drone for detecting and controlling street crimes." In *2017 IEEE 17th International Conference on Communication Technology (ICCT)*, pp. 1725-1730. IEEE, 2017. https://doi.org/10.1109/ICCT.2017.8359925

[18] Kaya, Mustafa, Betül Ay Karakuş, and Serkan Karakuş. "Binary classification of criminal tools from the images of the case using CNN." In *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1-6. IEEE, 2018. https://doi.org/10.1109/IDAP.2018.8620886

[19] Goya, Koichiro, Xiaoxue Zhang, Kouki Kitayama, and Itaru Nagayama. "A method for automatic detection of crimes for public security by using motion analysis." In *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 736-741. IEEE, 2009. https://doi.org/10.1109/IIH-MSP.2009.264

[20] Abd Almisreb, Ali, Mohammed Ahmed Saleh, and Nooritawati Md Tahir. "Anomalous behaviour detection using transfer learning algorithm of series and dag network." In *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*, pp. 505-509. IEEE, 2019.

[21] Vaidya, Bhaumik, and Chirag Paunwala. "Deep learning architectures for object detection and classification." *Smart Techniques for a Smarter Planet: Towards Smarter Algorithms* (2019): 53-79. https://doi.org/10.1007/978-3-030-03131-2_4

[22] Guo, Yanpeng, Zhenjiang Pang, Jun Du, Fan Jiang, and Qilong Hu. "An improved AlexNet for power edge transmission line anomaly detection." *IEEE Access* 8 (2020): 97830-97838. https://doi.org/10.1109/ACCESS.2020.2995910

[23] Mohamad Zamri, Nurul Farhana, Nooritawati Md Tahir, Megat Syahirul Amin Megat Ali, and Nur Dalila Khirul Ashar. "Deep learning optimisation algorithms for snatch theft detection." *Journal of Electrical and Electronic Systems Research (JEESR)* 20 (2022): 34-40. https://doi.org/10.24191/jeesr.v20i1.005

[24] Chalapathy, Raghavendra, and Sanjay Chawla. "Deep learning for anomaly detection: A survey." *arXiv preprint arXiv:1901.03407* (2019).

[25] Arefin, Md Rifat, Farkhod Makhmudkhujaev, Oksam Chae, and Jaemyun Kim. "Aggregating CNN and HOG features for real-time distracted driver detection." In *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-3. IEEE, 2019. https://doi.org/10.1109/ICCE.2019.8661970

[26] Muhammad, Khan, Jamil Ahmad, Irfan Mehmood, Seungmin Rho, and Sung Wook Baik. "Convolutional neural networks based fire detection in surveillance videos." *Ieee Access* 6 (2018): 18174-18183. https://doi.org/10.1109/ACCESS.2018.2812835