

Review Article

Evil and Fear Detection Using Facial Recognition Algorithms for Crime Prevention - A Survey

Ahmad Asnawi Ahmad Shukri¹, Lokman Mohd Fadzil^{1*}

¹National Advanced IPv6 Centre (NAv6), University Sains Malaysia (USM), Penang, Malaysia.

¹Corresponding Author : lokman.mohd.fadzil@usm.my

Received: 06 March 2024

Revised: 07 April 2024

Accepted: 05 May 2024

Published: 29 May 2024

Abstract - The development of facial recognition technology has transformed a number of industries, including crime prevention and law enforcement. This work proposes a revolutionary method for improving crime prevention through the creation of a facial recognition system that can identify expressions linked to fear and malevolent intent. A model is being proposed to recognize minor facial cues suggestive of evil intentions and terror responses by utilizing deep learning techniques and a large dataset. With the use of face cues, including micro-expressions, eye movements, and muscular contractions, the proposed system is able to discriminate between people who are exhibiting such emotions. The system can be used for a wide range of purposes, such as real-time surveillance in public areas and witness and suspect identification to support investigations. However, when using such technology, privacy, ethics, and the possibility of prejudice issues need to be properly considered. The development, validation, and possible societal ramifications of the algorithm are covered in this paper, with a focus on the necessity of finding a balance between technical advancement and defending individual liberties and rights. The research aims to further the ongoing discussion on the appropriate application of facial recognition technology in public safety and crime prevention.

Keywords - Crime prevention, Deep learning algorithm, Evil detection, Facial expression analysis, Facial recognition, Fear detection.

1. Introduction

Facial recognition technology has become increasingly popular in recent years, with applications ranging from security and surveillance to marketing and social media. On the other hand, with time, traditional facial recognition algorithms have been progressing in their ability to accurately identify individuals based on differences in facial expressions or emotions. Facial recognition technology has come a long way in recent years, but there are still limitations when it comes to identifying specific emotions.

Two specific emotions or expressions that have been of particular interest to researchers are the evil- and fear-looking appearance on a person's face. These expressions can be difficult to detect as they are often subtle and fleeting. The evil look appearance is characterized by narrowed eyes, tightened lips, and a furrowed brow. The fear-looking appearance involves widened eyes, raised eyebrows, and an open mouth. It is typically associated with feelings of anxiety or terror.

The importance of identifying these expressions lies in the potential use cases of facial recognition technology. These expressions are often associated with negative emotions, such as anger or contempt, and may indicate a potential threat or danger. For instance, security systems can use this information

to alert authorities when an individual with an evil- or fear-looking is identified in a public area. It can also be used in marketing research to understand how advertisements or products elicit specific emotional responses.

By analyzing subtle changes in facial expression and muscle movement, these algorithms have proven to be highly effective in identifying individuals who may be exhibiting signs of aggression or fear that might not be immediately obvious to human observers. In this technical article, the use of the You Only Look Once (YOLO) algorithm for facial recognition on evil- and fear-looking appearance will be explored.

YOLO algorithm uses convolutional neural networks to identify specific features in the face that correspond to different emotions. It works by breaking down an image into smaller regions, analyzing specific regions of the face, such as the eyes or mouth separately, to identify any relevant features or patterns, and then using this information to make a final prediction about what is present in the image [1].

Implementing facial recognition with the YOLO algorithm requires several technical steps. Firstly, the dataset needs to be prepared, including collecting images of faces



displaying evil- and fear-looking appearances. These images need to be labelled and annotated for training the algorithm. By training these algorithms on large datasets of labelled images, they can accurately recognize evil and fear-looking appearances with high precision. Next, the deep learning network needs to be designed with convolutional layers to extract features from the input image, followed by Region Proposal Networks (RPN) that generate proposals for object detection.

The YOLO algorithm then uses these proposals to classify and localize objects in the image. To achieve accurate facial recognition, fine-tuning of pre-trained models on large datasets is necessary. This involves adjusting hyperparameters, such as learning rate and batch size, and optimizing loss functions. Additionally, data augmentation techniques like random cropping and flipping can increase dataset variety and improve model performance.

The future implications of using the YOLO algorithm for facial recognition are vast and exciting. As technology continues to improve, these algorithms will become even more accurate and efficient at recognizing faces based on specific characteristics such as evil- or fearful appearances. This could have significant applications in security and law enforcement, helping to identify potential threats before the threat actors act.

One of the biggest challenges in implementing facial recognition for evil and fear-looking is the lack of standardization in datasets. There is no comprehensive dataset that includes a diverse range of individuals displaying these emotions, making it difficult to train machine learning models effectively. Another challenge is the need for high-quality images with consistent lighting conditions. Low-quality images or inconsistent lighting can impact the accuracy of facial recognition algorithms, particularly when trying to detect subtle expressions.

Finally, ethical considerations must be considered when implementing facial recognition technology for detecting emotions such as fear or evil looks. The use of this technology must be balanced against privacy concerns, potential biases and misuse that may arise from its use. Regulations need to be put in place to ensure that these systems are used ethically and responsibly as they continue to evolve. Additionally, there is a need for continued research into the potential biases that may exist within facial recognition systems based on factors such as race or gender.

2. Literature Review

Human detection has been an important aspect of human civilization since the earliest days of human society. The earliest forms of human detection were likely based on sensory perception, with humans using their eyes and ears to detect potential threats. In ancient civilizations such as Greece and Rome, security guards were stationed at city walls and

towers to keep watch for potential invaders [2]. The development of technology has played a significant role in the evolution of human detection.

One of the earliest technological innovations was the telescope, which was invented in the early 17th century. The telescope allowed for much greater visibility, and it quickly became a key tool for astronomers. However, it was also used for human detection, particularly during wars. For example, during the American Civil War, both Union and Confederate armies used telescopes to observe enemy troop movements from a distance.

In the late 19th century, the development of photography led to new methods of human detection. Police began to use photography to create “mug shots” of criminals, which they could then use to identify suspects. By the early 20th century, fingerprinting had become a widely accepted method of identifying individuals, and it remains an important tool in human detection to this day. The 20th century saw a number of important advancements in human detection technology. During World War II, radar technology was developed and used extensively to detect enemy planes and ships. After the war, radar was adapted for civilian use, and it quickly became an important tool for air traffic control and weather forecasting.

In the latter half of the 20th century, the development of computer vision technology led to new methods of human detection. In the 1960s, researchers began to explore the use of machine learning algorithms for object recognition, including the recognition of human faces. By the 1980s, computer vision had advanced to the point where it could be used for real-time human detection in security systems and other applications.

One of the key challenges in human detection has been the ability to detect humans in low light conditions or through obstacles such as walls or foliage. In the 1970s, researchers began to develop thermal imaging technology, which uses infrared radiation to detect heat signatures. Thermal imaging is particularly useful for detecting humans in low light conditions or through obstacles, as it can detect the heat given off by the human body. Thermal imaging is now widely used in military and law enforcement applications.

Another key challenge has been the ability to recognize individuals accurately and quickly. In the 1990s, researchers began to explore the use of biometric identification systems, which use unique physical or behavioral characteristics to identify individuals. Biometric systems include technologies such as facial recognition, iris scanning, and voice recognition. While biometric systems have been controversial in some contexts due to concerns about privacy and accuracy, they have proven to be a valuable tool in many applications. In recent years, there has been a surge of interest in using

machine learning and artificial intelligence for human detection. These technologies are being used for a wide range of applications, from facial recognition for law enforcement to object recognition for autonomous vehicles.

Some of the key challenges in using machine learning for human detection include the need for large datasets and the potential for bias in the training data. Overall, the history of human detection is one of constant innovation and advancement. From security guards standing guard on city walls to advanced machine learning algorithms, humans have always sought to improve our ability to detect and identify other humans. As technology continues to evolve, we will likely see even more exciting developments in the field of human detection in the years to come.

2.1. Robbery Cases Comparative Analysis

Assessment of high-value robbery cases that are still open today is a vital component of crime detection based on facial expressions. These incidents are important because they result in huge losses, garner media attention, endanger public safety and the absurd fact that no potential suspects were able to be detected until today. Developing successful tactics for crime prevention and intervention can be aided by scrutinizing the facial expressions of those who potentially participate in any robberies or criminal activities on record. In general, investigating high-value robbery incidents increases the applicability and influence of the research in creating precise criminal detection systems employing facial expression analysis. Examples of big-time robberies were unpredictable by the authorities (Table 1).

Table 1. Robbery cases comparative analysis

Case Name	Year	Chronology	Cost	Status
The Antwerp Diamond Heist [3]	2003	Gained access to Diamond Centre by posing as diamond merchants using fake identities and credentials. overpowered the security guards and turned off the alarm system, which delayed the response from law enforcement	\$100 million = RM380 Million	Unsolved
The Isabella Stewart Gardner Museum Heist [4]	1990	Gained access to the museum by posing as police officers responding to a disturbance call. overpowered the security guards, even heavily guarded cultural institutions	\$500 Million = RM1.35 Billion	Unsolved
The Banco Central Burglary [5]	2005	Dug a tunnel from a rented house to the bank’s vault. Once inside, bypass the bank’s security systems and systematically empty it of cash.	\$70 Million = RM260 Million	Unsolved
The Graff Diamonds Heist [6]	2005	Robbers wearing professional makeup disguises entered the store posing as wealthy customers, brandished their weapons and took control of the premises	\$65 Million = RM227 Million	Unsolved
The Banco de España Heist [7]	2020	Gained access to the bank by turning off the security systems and bypassing the guards. Once inside, the robbers made their way to the vault and successfully breached it.	Not disclosed, but it is believed to be a substantial amount	Unsolved
The Millennium Dome Diamond Heist [8]	2000	Robbers shattered the display case housing the De Beers Millennium Star diamond, one of the world’s largest and most valuable diamonds. With the presence of security personnel and surveillance cameras, the robbers managed to escape	\$270 Million = RM1.026 billion.	Unsolved
The British Museum Heist [9]	2000	Gained unauthorized access to the British Museum. They turned off security systems and made their way to the museum’s Egyptian Antiquities section. Despite the presence of security cameras and alarm systems, the robbers managed to evade detection and escape with the stolen artefacts.	It was not disclosed, but it is believed to be a substantial sum. ~ millions of pounds	Unsolved

This research can help prevent high-value robbery cases by giving us better tools and strategies to identify and stop them before they happen or minimize their impact. By analyzing the facial expressions of individuals with a high potential to commit crimes, researchers can identify patterns and cues that indicate criminal intent or behavior. This information can be used to develop advanced systems that can detect suspicious facial expressions in real-time, allowing for early intervention and prevention.

Additionally, the insights gained from studying these cases can help inform law enforcement and security agencies in implementing targeted measures and improving their response protocols. Ultimately, by understanding the emotional cues and behavioural patterns associated with high-value robberies, this research equips us with valuable knowledge to enhance our ability to prevent such crimes and safeguard our communities.

2.2. Access Control Comparative Analysis

Access control refers to the practice of regulating and managing access to physical or digital resources, systems, or information. In order to guarantee that only authorised people or organisations can access resources or carry out particular actions it entails the implementation of policies, procedures, and rules. For security and secrecy in a variety of contexts, such as computer systems, buildings, networks, and data, access control is essential.

2.2.1. Characteristics of Good Access Control Methods

Whether it is a physical or digital approach, a solid access control method has a few essential elements that make it effective in protecting resources and guaranteeing the integrity of the access control system. These are some key elements of an effective access control strategy.

- **Authentication:** The method should include a robust authentication process to verify the identity of users or entities seeking access. Authentication can involve something the user knows (e.g., password or PIN), something the user has (e.g., access card or mobile device), or something the user is (e.g., biometric data).
- **Authorization:** After authentication, the method should enforce well-defined authorization policies that determine what actions or resources the authenticated user or entity is allowed to access. This includes specifying access permissions and rights.
- **Granularity:** A good access control method allows for fine-grained control over access permissions. It should enable administrators to specify detailed access rights, ensuring that users have access only to the resources necessary for their roles and responsibilities (the principle of least privilege).
- **Security:** The method should provide a high level of security, making it difficult for unauthorized users or

entities to gain access. This includes protection against common attack vectors like brute-force attacks, social engineering, and unauthorized copying or cloning of credentials.

- **Auditability:** A good method maintains comprehensive logs of access events, recording who accessed what, when, and for what purpose. These logs are essential for security monitoring, compliance, and incident investigation.

2.3. Access Control Methods Comparative Analysis

Physical Access Control Systems (PACS) are designed to manage and regulate access to physical spaces, such as buildings, rooms, or facilities. These systems employ various authentication methods to ensure that only authorized individuals can enter specific areas. Here are some common methods used in PACS (Table 2) [10].

All-access control methods, including those mentioned above, have potential vulnerabilities and can be broken or bypassed under certain conditions or with sufficient effort and resources. The level of difficulty in breaking these methods varies based on several factors, including the specific implementation, the security measures in place, and the capabilities of the attacker.

While it is generally said that more difficult-to-break access control methods are often considered more secure, the “best” access control method depends on a variety of factors, including the specific security needs of the organization, the operational requirements, and the context in which the method is used.

On the criminal side, they will carefully prepare all the ways and strategies to commit any crime, especially a major crime such as bank robbery. No exception is the preparation of access control to ensure they can sneak into the target area. So, if criminals have prepared their way to pass the access control before they arrive, this access control and security system is useless. If there is a camera to detect a live facial recognition system, the probability of criminals passing access control will definitely decrease. The camera will be placed at an unexpected place and able to get a comprehensive view.

All method depends on the access method but do not validate the person. Camera (proposal) to validate the intention of a person, not to validate identification. Include this in Gap analysis in the table of research paper. We cannot fully identify a person’s intention, but we attempt to validate partial intention based on available emotion visible on the person’s face. We will attempt to acquire continuous facial recognition at different locations of the targeted site because a person can potentially fake his/her emotions or appearances at the point of entry. However, the person naturally be himself/herself at the other locations leading to the point of entry.

Table 2. Access control methods comparative analysis

Method		Pros	Cons	Application
Key Cards or Access Cards		<ul style="list-style-type: none"> >Widely used and familiar to most users. >Easy to issue, replace, and revoke. >Can be encoded with multiple access levels. >Audit trails can be generated to track card usage 	<ul style="list-style-type: none"> >Cards can be lost or stolen, potentially leading to unauthorized access. >Card sharing is a risk if not closely monitored. >Cards can be copied or cloned, compromising security. >Requires physical contact with a reader, which can lead to wear and tear 	Office buildings, hotels, and educational institutions.
Biometric	Finger Print	<ul style="list-style-type: none"> >Unique to each individual, difficult to fake. >Convenient and quick for users. >No risk of lost or stolen credentials 	<ul style="list-style-type: none"> >Some environmental factors (e.g., dirt, moisture) can affect accuracy. >Not suitable for individuals with certain medical conditions (e.g., damaged fingerprints). >Privacy concerns related to storing biometric data 	High-security environments and government facilities
	Retina/Iris	<ul style="list-style-type: none"> >Extremely difficult to forge. >High accuracy and reliability. >Non-contact method, reducing hygiene concerns 	<ul style="list-style-type: none"> >Requires specialized hardware, making it expensive to implement. >Some users may be uncomfortable with eye scanning. >Privacy concerns regarding the collection of eye-related data 	
	Facial	<ul style="list-style-type: none"> >Non-contact and convenient for users. >Can work with existing surveillance cameras for added security. >Advances in technology have improved accuracy 	<ul style="list-style-type: none"> >Can be fooled by photos or videos of authorized users. >Accuracy can be affected by lighting conditions and facial changes (e.g., growing a beard). >Privacy concerns, as facial data is captured and stored 	
Smart Cards		<ul style="list-style-type: none"> >Encrypted data on the card enhances security. >Can store additional information (e.g., access levels, biometric templates). >Harder to clone than traditional access cards 	<ul style="list-style-type: none"> >Costlier to issue and maintain than standard access cards. >Requires specialized card readers. >Cards can still be lost or stolen 	Corporate environments and government agencies, especially for logical access control
Personal Identification Number (PIN)		<ul style="list-style-type: none"> >Provides an additional layer of security when used with access cards or other methods. >Easy to remember for users. >Can be changed regularly for added security 	<ul style="list-style-type: none"> >Vulnerable to unauthorized disclosure (e.g., someone watching you enter the PIN). >Can be forgotten, leading to lockouts. >Limited complexity compared to longer passwords 	Often used in combination with other methods, such as access cards or smart cards.
Mobile Access		<ul style="list-style-type: none"> >Convenient, as most people carry smartphones. >Can leverage biometrics (e.g., fingerprint or facial recognition) for added security. >Mobile credentials can be easily revoked or updated remotely 	<ul style="list-style-type: none"> >Relies on the security of the mobile device (e.g., password or biometric lock). >Compatibility issues with various smartphones and operating systems. >Potential privacy concerns related to tracking user locations 	Gaining popularity, particularly in the context of building access control. Many modern access control systems offer mobile app integration for unlocking doors using smartphones.

2.4. Current Research Work Comparative Analysis

Analyzing previous research papers before starting this research is important because it helps us build upon existing knowledge and avoid duplicating efforts. By reviewing previous studies on human detection based on human facial expressions, we can understand what has already been explored, what methods and techniques have been used, and what gaps or limitations exist.

This analysis allows us to identify valuable insights, learn from the successes and challenges of previous research, and determine how our study can contribute something new or improve upon existing approaches. By building on the foundation of previous research, we can ensure that our work is informed relevant, and adds value to the field of crime detection using facial expressions (Table 3).

Table 3. Current research work comparative analysis

Research Title	Research Authors	Publish Date	Research Findings	Research Gap
Past, Present, and Future of Face Recognition	Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A.	23 July 2020	Advancements in facial recognition emphasise deep learning’s superiority over traditional computer vision methods. While 2d recognition has room for improvement, 3d sensors offer promising solutions to overcome various limitations.	It does not focus on multimodality, soft facial biometrics, infrared imaging, sketches, deep learning, faster response, 100% accuracy, optimal security, and portable equipment.
Person Recognition in Personal Photo Collections	Oh, S. J., Benenson, R., Fritz, M., & Schiele, B.	25 September 2015	It is hard to detect due to various viewpoints, poses and occlusions. Face not visible, different cues, sometime increasing dataset does not solve the problem.	The lack of a dataset for each person may make it difficult for the system to recognize correctly. Not using YOLO
Real-Time Eye State Detection System for Driver Drowsiness Using Convolutional Neural Network	Hashemi, M., Mirrashid, A., & Beheshti Shirazi, A.	04 August 2020	Successfully detect driver drowsiness using CNN and alert alarm when triggered. Sometimes, the wrong alarm is due to the environment, like external lighting and glasses.	False trigger when using this due to environment and to improve the speed of detection
Vision-Based Human Detection Techniques: A Descriptive Review	Sumit, S. S., Rambli, D. R. A., & Mirjalili, S.	01 March 2021	It has pros and cons for each technique, and some techniques are high maintenance such as SIFT, bow, and oms. Some techniques can resolve the limitations of other techniques.	Limited to further enhancement of the speed, computational training time, and the accuracy of algorithms
A Human-Detection Method Based on YOLOv5 and Transfer Learning Using Thermal Image Data from UAV Perspective for Surveillance System	Mantau, A., Widayat, I. W., Leu, J.-S., & Köppen, M.	4 October 2022	Trained yolov5 can detect an object (human) by image from thermal infrared and TIR images.	Not using the latest YOLO version to utilize the thermal infrared image. Specific facial characteristics cannot be captured.
An Implementation of High Efficient Smart Street Light Management System for Smart City	Yang, Y.-S., Lee, S.-H., Chen, G.-S., Yang, C.-S., Huang, Y.-M., & Hou, T.-W.	21 February 2020	Street lighting management system with a Web-based cloud platform, edge devices, and real-time lighting control function and offers real-time street pole information.	Focus only on weather data, not on pedestrian data and Jetson nano Rpi are low-performance
Face detection techniques: a review	Kumar, A., Kaur, A., & Kumar, M.	August 2019	Difficult or cannot detect face recognition with occlusion or non-uniform illumination	Cannot solve occlusion and non-uniformity illumination problems during facial recognition

Long-Distance Person Detection Based on YOLOv7	Tang, F., Yang, F., & Tian, X.	March 2023	Proposes the TOD-YOLOv7 model with more robust performance in the field of tiny-person detection, which demonstrates significantly superior performance compared to existing mainstream object detectors, achieving an AP of 9.5% in the TinyPerson task	Only focus on detecting long distance/tiny people, but not able to detect specific facial characteristics.
Facial expression recognition method based on PSA—YOLO network	Ma, R., & Zhang, R.	January 2023	Running time of the proposed method and The comparison method is reduced from 1,800 to 200 ms	Using a limited dataset but not using live video feeds. No triggering condition
Real-time human face tracking and recognition system in an uncontrolled environment	Thary Al-Ghraiiri, A. H., Hussein Fallooh Al-Anbari, N., & Zuhair Sameen, E.	December 2022	When the findings of the real-time face recognition system are compared to those of the earlier studies, the real-time system’s recognition rate is found to be 91.12% successful, effective, and resilient with a short execution time.	Detect facial recognition using Viola-Jones algorithm but no crime analysis performed on the algorithm.

Facial expression and human detection have been explored in several previous studies. The methods employed to accomplish the goal, the study findings, and the research gap are some of the topics examined. The research publications that were examined included studies with similar goals to this one but with various approaches and applications. The speed at which the system produces output and the research gap are also looked at. Based on findings from several previous study papers, it was found that there is still no research like this proposed research. Some studies are almost the same but use different methods and different approaches.

2.5. Dataset Comparative Analysis

Collecting many datasets is important in this research because it provides us with a diverse and comprehensive pool of information to analyse. By having a large dataset, we increase the chances of capturing a wide range of facial expressions and variations in criminal behaviour. This helps us train and fine-tune our algorithms to recognize different emotions and identify potential signs of criminal activity more accurately. The abundance of data also enables us to validate our findings and ensure that our methods are robust and effective in real-world scenarios. Overall, collecting data enhances the quality and reliability of our research, leading to better insights and more accurate crime detection systems (Table 4).

Prior to use, several datasets that can be utilized to train and test the method were examined. The dataset’s goal, which must be to recognize people or detect facial expressions, is one of the things checked. Then, the dataset format also checks and finds out which algorithm is suitable to use the dataset.

A variety of face-related datasets have been collected for the algorithm’s testing and training purposes. The human crowd dataset is one of the datasets used to examine how well the system can analyze the facial expressions of everyone in each frame of a picture. A full-body human dataset that was captured via CCTV is another dataset that was collected.

Next, a dataset of human facial images with varied expressions-such as happiness, sadness, anger, and surprise-was collected. All these datasets are offered in the form of a Zip, Dropbox, Google Drive, or TGZ file that users must extract to access the data. All these datasets are in JPG or PNG format, which is ideal for both new and classic algorithms like YOLO as well as RCNN.

2.6. Algorithm Comparative Analysis

Comparing various algorithms in this research is important because it helps us understand which approach is the most effective for crime detection based on human facial expressions. Different algorithms have different strengths and weaknesses, and by comparing them, we can determine which one performs better in terms of accuracy, speed, and reliability. This allows us to identify the most suitable algorithm for our specific research goals.

Additionally, comparing multiple algorithms helps us evaluate their robustness and generalizability across different scenarios and datasets. It enables us to make informed decisions about which algorithm to use in real-world applications to ensure accurate and efficient crime detection. By considering various algorithms, we can choose the best one that maximizes the effectiveness and usability of our research outcomes (Table 5).

Table 4 . Dataset comparative analysis

Datasets Authors	Datasets Purpose	Repository Storage Method/ Format	Datasets Source	Image / Video	Potential Algorithm to Process the Dataset
Lubomir Bourdev and Jitendra Malik Link	Human in 3D (Full Human Body)	TGZ (zip format)	Paper Research	PNG, JPG	F-RCNN C-RCNN YOLO
Konstantin Verner Link	Human from CCTV	Zip	Internet Search	PNG	F-RCNN C-RCNN YOLO
Shao, Shuai and Zhao, Zijian and Li, Boxun and Xiao, Tete and Yu, Gang and Zhang, Xiangyu and Sun, Jian Link	Crowd (Random Capture)	Zip - Google Drive	Internet search	PNG	F-RCNN C-RCNN YOLO
E. Gebhardt and M. Wolf P. Saha, B. A Mudassar and S. Mukhopadhyay Link	Human detection using infrared	Dropbox	Internet search	PNG	F-RCNN C-RCNN YOLO
Unknown Link	Day-Night Pedestrian Dataset	zip	Paper Research	PNG	F-RCNN C-RCNN YOLO
Christian Wojek, Stefan Walk, Bernt Schiele Link	Pedestrian (Random Capture)	TGZ	Paper Research	PNG, avi	F-RCNN C-RCNN YOLO
Manas Sambare FER-2013 Link	Random face image - Grayscale	Zip	Paper Research	JPG	F-RCNN C-RCNN YOLO
Atul Anand LFW - People (Face Recognition) Link	Random face from the Web	Zip	Paper research	JPG	F-RCNN C-RCNN YOLO
Ares Emotion Detection Link	Random face image - Grayscale	Zip	Paper Research	JPG	F-RCNN C-RCNN YOLO
Mahmoudima Mma Facial Expression Link	Facial expression Images	Zip	Paper Research	JPG	F-RCNN C-RCNN YOLO

Investigating algorithms made specifically to detect objects and facial expressions was done before selecting one. One of the criteria considered is the workflow and mechanism of the algorithm, which must currently be updated and enhanced. The Mean Average Precision (MAP) was then used to analyze each algorithm's weakness further. Because it is possible to observe what flaws were fixed in the previous version, both traditional and modern algorithms are included in the research. Mean Average accuracy demonstrates an algorithm's capacity for precise detection, but precision is not the only aspect that should be taken into consideration when making a decision. To ensure that almost real-time detection can be archived, it is also necessary to look at the speed at which the algorithm produces output.

2.7. Smile Construct Comparative Analysis

When conducting this research, it is important to identify and understand the different types of smiles. Smiles can convey various emotions, and by categorizing them, we can gain valuable insights into the emotional states of individuals, and maybe some smiles are not driven to the good things.






By distinguishing between different types of smiles, we can develop more accurate and nuanced algorithms for crime detection based on facial expressions. This knowledge allows us to better analyse and interpret smiles in real-time, helping to identify potential criminal behaviour and enhance the effectiveness of our research in preventing and addressing crime (Table 6).







Table 5. Algorithm comparative analysis

Algorithm Name and Author	Algorithm Mechanism	Findings from Algorithm Work	mAP (%)	Speed (fps)	Algorithm Weakness
Region-based Convolutional Neural Network (RCNN) - Ross Girshick et al.	Create a Bounding box using selective search. An image will get thousands of bounding boxes. Each bounding box will go through CNN to get categorized.	Using selective search first before passing through CNN	66.0	<10	Longer time to train network. It cannot implemented in real-time.
Fast-RCNN - Ross Girshick et al.	Input the image to the CNN to generate a convolutional feature map. Identify the region of proposals and warp them into squares. Predict the class of the proposed region and also the offset values for the bounding box	Pass through CNN first before using selective search to identify the region	70.0	5-15	Use selective search (slow)
Faster-RCNN - Shaoqing Ren et al.	Similar to Fast RCNN but replaced selective method with RPN (Region Proposal Network)	Use another network to replace selective search. Faster	73.2	5-20	The network does not look at the complete image
Original You Only Look Once (YOLO) [11] Joseph Redmon, Santosh Divvala and Ross Girshick	Split an image into an SxS grid; within each of the grids we take m bounding boxes. In each of the bounding boxes, the network outputs a class probability and offset values for the bounding box. The bounding boxes having the class probability above a threshold value are selected and used to locate the object within the image.	Different from the region-based algorithms In YOLO, a single convolutional network predicts the bounding boxes and the class probabilities for these boxes.	63.4	45	Take a longer time and more data to train
YOLOv4 - Alexey Bochkovskiy, Chien-Yao Wang, and Hong-Yuan Mark Liao	Utilizes a backbone network to extract features, followed by several detection layers that predict bounding boxes and class probabilities. It applies non-maximum suppression to remove redundant detections	Divides the input image into a grid and predicts bounding boxes and class probabilities directly from that grid	43-45	65	Struggle with accurately detecting small objects and objects with low contrast. May produce lower-quality bounding box predictions
YOLOv5 [1] - Ultralytics, an AI research organization,	Employs a CNN backbone network to extract features, which are then fed into detection heads to generate predictions for objects in the input image	Based on a single-stage architecture that uses anchor boxes and feature pyramids to predict bounding boxes and class probabilities	50-55	100	Struggle with accurately detecting small objects due to its grid-based detection approach, which may result in lower precision for smaller or low-contrast objects
YOLOv7 - Alexey Bochkovskiy	Passing the image through a series of convolutional layers to extract features, then using anchor boxes to predict object locations and class labels	Dividing images into a grid and predicting bounding boxes and class probabilities for each grid cell	55-60	160	Struggling with small objects due to its coarse grid and occasionally misclassifying ambiguous objects due to limited contextual information

Single Shot Detector (SSD) [12] - Wei Liu, Dragomir Anguelov, Dumitru Erhan, Christian Szegedy, Scott Reed, Cheng-Yang Fu, and Alexander C. Berg	It involves extracting features, generating default bounding boxes, predicting object presence and refining boxes, and applying non-maximum suppression.	Uses a single neural network to detect objects by predicting their categories and bounding boxes	70 -80	20-60	Struggle with small object detection and can produce multiple detections for the same object due to default box scaling.
RetinaNet - Tsung-Yi Lin, Priya Goyal, Ross Girshick, Kaiming He, and Piotr Dollár	Generates anchor boxes, predicts object presence, refines bounding boxes, and assigns class probabilities.	It uses a feature pyramid network (FPN) and focal loss to detect objects at different scales and address class imbalance	30-40	5-20	Struggle with small object detection and can have redundant detections for overlapping objects.
Fully Convolutional One-Stage (FCOS) - Zhi Tian, Chunhua Shen, Hao Chen, Tong He	Divides feature map into grids assigns object annotations, and predicts presence, bounding box, and class probabilities for each grid cell	Treats object detection as pixel-level classification, predicting object presence, bounding box coordinates, and class probabilities for each location on the feature map	36-42	10-30	Challenged with accurate detection of small objects due to pixel-level classification

Table 6. Smile construct comparative analysis [13]

Smile Type	Human Characteristics Associated Smile	Characteristic of Smile	Smile Image Example	Included or Not Included + Reason
Reward smiles	Contentment, approval, or even happiness in the midst of sorrow	Muscles in the mouth and cheeks are both activated, as are muscles in the eye and brow areas. Raised cheeks		Not included
Affiliative smiles	To reassure others, to be polite, and to communicate trustworthiness, belonging, and good intentions	Involve the upward pull of the lips, and often trigger dimpling in the cheeks. It can also include lip pressure, where the lips remain closed during the smile.		Not included
Dominance smiles	To show their superiority, to communicate contempt or derision, and to make others feel less powerful.	It is more likely to be asymmetrical: one side of the mouth rises, and the other side remains in place or pulls downward. Include a lip curl and the raising of an eyebrow.		Not included
The lying smile	Some display this when they are being deceitful.	The zygomaticus major muscle - the one that pulls your lips into a smile - repeatedly fired.		Not included
The wistful smile	The expression conveys a sense of longing, nostalgia, or sadness combined with a touch of sweetness or bittersweetness. Usually gentle and soft in appearance	The corners of the mouth may turn slightly upward, indicating a restrained smile. When someone wears a wistful smile, their eyes might appear distant or introspective.		Not included

The polite smile	A courteous and respectful gesture. It shows acknowledgement of the other person's presence and can convey a sense of politeness and goodwill.	It involves the zygomaticus major muscle but not the orbicularis oculi muscle. In other words, your mouth smiles, but your eyes don't		Not included
The flirtatious smile	To express romantic or sexual interest in someone. It is often characterized by certain facial expressions and body language that convey attraction and playfulness.	Keep your lips together and lift an eyebrow.		Not included
The embarrassed smile	To acknowledge and diffuse a situation that may be uncomfortable, awkward, or embarrassing	A smile provoked by embarrassment is often accompanied by a downward tilt of the head and a shifting of the gaze to the left.		Not included
The pan am smile	The pan am smile was characterized as a polite but seemingly forced smile	They use extra effort to yank on their zygomaticus major muscle. Corners of the mouth are extra high, and more of the teeth are exposed.		Not included
The Duchenne smile	Known as the smile of genuine enjoyment. To express sincere, positive emotions and to create a genuine connection with others.	Involves the mouth, the cheeks, and the eyes simultaneously. It is the one where your whole face seems to light up suddenly.		Not included
The evil smile or The Malicious smile	Associated with villains, antagonists, or mischievous characters. To convey a sense of pleasure or satisfaction in someone else's misfortune or pain	Squinted eyes, raised eyebrows, curled lips, tilted head or other facial expressions that suggest mischief, malice, or pleasure.		Included




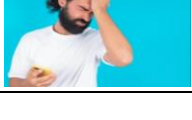
A smile is a facial expression that is synonymous with a feeling of happiness or respect; even a smile can make someone fall in love. Researchers have researched the types of smiles that exist. 10 out of the 11 types of smiles above do not give any prejudice to the smiler and can even make the other party feel closer.

However, there is one type of smile where the smiler looks very scary even when smiling. This type of smile is categorized as an evil smile. This smile is said; the smiler feels a sense of joy when he sees someone in pain or has intended something bad. It is this evil smile that is the focus of researchers to detect because this smile is drawn with evil intentions.

2.8. Sad Construct Comparative Analysis

When conducting this research, it is also important to identify and understand the different types of sadness. Sadness can manifest in various ways, and by categorizing these types, we can gain insights into the emotional states of individuals related to criminal activities. Different types of sadness may indicate different levels of distress, remorse, or involvement in criminal behaviour. By studying and distinguishing between these types of sadness, we can develop more accurate algorithms for crime detection based on facial expressions. This understanding allows us to better analyse and interpret sadness in real-time, aiding in the identification of potential criminal behaviour and contributing to the effectiveness of our research in preventing and addressing crime (Table 7).

Table 7. Sad construct comparative analysis [14]

Sad Type	Human Characteristic	Characteristic of a Sad Face	Sad Image Example	Included or Not Included
Grief	Deep sadness and sorrow experienced after a significant loss	Brows might be furrowed, their eyes may appear watery or red, and their mouth might be turned downwards		Not included
Melancholy	Prolonged and lingering sadness that may be accompanied by a sense of longing or nostalgia	Their eyebrows may be slightly raised, their gaze may be unfocused or looking downward, and their mouth may have a subtle downturn.		Not included
Heartbreak	Intense emotional pain caused by the end of a romantic relationship or the betrayal of trust	Eyes may be teary or swollen, their brows might be furrowed or raised in disbelief, and their mouth may be turned downwards with a quivering lower lip.		Not included
Disappointment	Unmet expectations dashed hopes or let-downs.	Slight frown, lowered eyebrows, and a sense of dejection. The eyes may appear downcast or lacking their usual brightness.		Not included
Sorrow	Deep and often prolonged sadness may arise from a range of life circumstances.	The eyebrows may be slightly furrowed, the mouth may be turned downwards, and the eyes may appear distant or filled with sadness.		Not included
Loneliness	Sadness and isolation result from a perceived lack of connection or meaningful relationships with others.	Brows may be slightly raised, their eyes might have a distant or vacant look, and their mouth may have a subtle frown.		Not included
Nostalgia	Bittersweet sadness that arises from fond memories of the past or a longing for simpler times.	Brows may be slightly raised, their eyes may have a dreamy or faraway look, and their mouth might have a faint smile or a gentle downturn.		Not included
Despair	Hopelessness, sadness, and a feeling that there is no way out of a challenging situation.	Brows may be heavily furrowed, the eyes may appear downcast or filled with tears, and the mouth may be downturned with a sense of hopelessness.		Not included
Regret	Sad and remorseful about past actions or choices, often accompanied by a sense of guilt or self-blame.	Brows may be slightly furrowed, their eyes may appear troubled, and their mouth might have a subtle frown or a compressed line.		Not included

A sad facial expression is a facial expression that looks lifeless and disinterested in doing any activity that involves a lot of muscles and complex thinking. This is because sad expressions are more likely to treat their sadness by being alone or expressing their feelings to someone in private. So all the above types of sadness do not give any concern to do any evil activity.


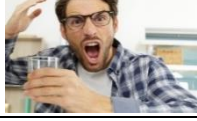








2.9. Anger Construct Comparative Analysis

When conducting this research, it is important to identify and understand the different types of anger. Anger can be expressed in various ways, and by categorizing these types, we can gain insights into the emotional states of individuals during criminal activities. Different types of anger may indicate varying levels of aggression, hostility, or potential for

violent behavior. By examining and classifying these types of anger, we can develop more accurate algorithms for crime detection based on facial expressions. This knowledge enables us to better analyze and interpret anger in real-time, assisting in the identification of potential criminal behavior and enhancing the effectiveness of our research in preventing and addressing crime (Table 8).

At least two parties are needed for an angry facial expression, with one party expressing their fury to the other. There is also a minor form of fury that is directed just against himself. However, this expression on the face appears to be present in every type of fury. An angry face might likely initiate other types of crime, but definitely not premeditated robbery.

Table 8. Anger construct comparative analysis [15]




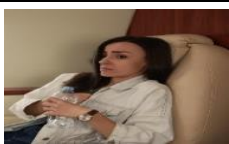



Anger Type	Human Characteristic	Characteristic of Anger Face	Anger Image Example	Included or Not Included
Passive	Indirect or covert style of anger expression. It involves suppressing or hiding anger.	Tense lips, narrowed or squinted eyes, raised eyebrows, limited facial expression, or avoiding direct eye contact.		Not included
Volatile	Intense and explosive outbursts of anger. It can involve aggressive behavior, yelling, shouting, or even physical violence.	Flushed face, clenched jaw, wide eyes, raised eyebrows, a tense or contorted facial expression		Not included
Fear-Based	Arises from a sense of threat or vulnerability. It can manifest as an aggressive response to perceived danger or a defensive reaction to protect oneself.	Tense or startled expression, widened eyes, raised eyebrows, a clenched jaw, and a defensive posture		Not included
Frustration-Based	Stems from feelings of being blocked, hindered, or thwarted in achieving a desired goal	Furrowed brow, tightened jaw, narrowed eyes, an expression of impatience or annoyance.		Not included
Pain-Based	Emerges from emotional or psychological pain, often resulting from past traumas, betrayal, or hurtful experiences	Hardened or guarded expression, narrowed eyes, a tightened jaw, raised eyebrows.		Not included
Chronic	The long-lasting pattern of anger that persists over time. Various situations or perceived injustices can trigger it and may become a habitual emotional response.	Tense expression, clenched jaw, furrowed brow, narrowed eyes, and an overall disposition of irritability or resentment.		Not included
Manipulative	Using anger as a tool for control or manipulation in relationships or situations	Calculated or insincere expression of anger, exaggerated gestures, intense eye contact		Not included
Overwhelmed	Anger becomes intense and difficult to manage due to feeling overwhelmed by stress, frustration, or other emotional factors.	Distressed expression, rapid or shallow breathing, a flushed face, and signs of agitation or distress		Not included
Physiological	Bodily sensations and changes that accompany anger. It involves the activation of the body's fight-or-flight response.	Heightened expression, increased blood flow resulting in a flushed or red face, wide eyes		Not included
Righteous	Intense anger that arises in response to perceived injustice or wrongdoing	Assertive expression, focused eye contact, raised eyebrows, and a resolute posture		Not included

2.10. Fear Construct Comparative Analysis

The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5), is a widely used manual published by the American Psychiatric Association for diagnosing mental disorders. According to the DSM-5, a specific phobia is classified as an anxiety disorder and

involves significant fear about a specific object or situation that does not pose a threat. Fear and phobia may present similarly at first glance, but the latter is often much more intense and disruptive. There are five main types of specific phobia (Table 9) [16].

Table 9. Fear construct comparative analysis [15]

Fear/ Phobia Type	Human Characteristic	Characteristic of Fear-Looking Face	Fear Image Example	Included or Not Included Reason
Fears related to animals	Display a startle response and a rapid or exaggerated movement backwards	Widened or dilated eyes, raised eyebrows, a tense or furrowed forehead, and a tightened jaw		Not included
Fears related to the natural environment	Display facial signs of alert and discomfort	Widened eyes, raised eyebrows, a tense or furrowed forehead, and a tight or partially open mouth.		Not included
Fears related to blood, injury, or medical issues	Paleness, Disgust and Nauseated Expression	Slightly downturned or unsettled mouth, squinting or narrowing of the eyes, or a grimacing expression		Not included
Fears related to specific situations	Fear of flying (aerophobia): May exhibit a tight or clenched jaw as a result of anxiety or stress.	Widened or dilated eyes, raised eyebrows, a tense or furrowed forehead, and a tight or partially open mouth.		Not included
	Fear of small places (claustrophobia): exhibit signs of panic on their face	Widened or dilated eyes, raised eyebrows, a tense or furrowed forehead, and a tight or partially open mouth		Not included
	Fear of murder or killer: Startled or Alert Expression	Involve widened eyes, a slightly dropped jaw, and heightened attention to their surroundings		Included
Others	Example loud noises	Widened or dilated eyes, raised eyebrows, a tense or furrowed forehead, and a tight or partially open mouth		Not included

A scared facial expression occurs when someone is in serious trouble, risking their life or something extremely valuable. The rest types of fear were not included as potential victims due to the fear not related to criminals, but fear of murder or killer was included. This kind of expression makes them more likely to become a victim of a crime. When a person is afraid of being a victim, it usually means someone else intends to harm them.

2.11. Hybrid Detection Method

Certainly, combining multiple detection methods to form a hybrid system is a strategy known as multi-modal or hybrid detection. This approach aims to leverage the strengths of individual methods while compensating for their respective weaknesses, ultimately improving the overall detection accuracy and robustness of the system. Let us explore this concept in more detail:

2.11.1. Weaknesses of Single Detection Methods

In the realm of crime detection, reliance on single detection methods is a common practice. However, despite their widespread use, these methods are not without their flaws. Some weaknesses of using a single detection method are as follows:

- False Positives/Negatives: Single methods may have limitations, such as high false positive rates (identifying non-criminal as criminal) or false negative rates (missing actual criminal).
- Sensitivity to Environmental Factors: Some methods may be sensitive to environmental conditions like lighting, weather, or background noise.
- Biases and Inaccuracies: Individual methods might be biased or inaccurate, especially if the training data used is not representative.

2.11.2. Hybrid Detection Justification

In the quest for more robust and effective crime detection strategies, hybrid detection approaches have emerged as promising solutions. By combining multiple detection methods and leveraging their respective strengths, hybrid detection offers enhanced capabilities in identifying and addressing potential crime. There are some reasons why hybrid detection should be implemented:

- **Combining Complementary Methods:** Hybrid systems often integrate different detection techniques that complement each other. For example, it combines facial recognition with behavioural analysis or object detection.
- **Diversification of Data Sources:** Hybrid systems may use data from various sources, such as cameras, sensors, and contextual information, to create a more comprehensive understanding of the situation.
- **Decision Fusion:** Hybrid systems use decision fusion techniques to combine the outputs of individual detectors. This can include techniques like averaging, voting, or more sophisticated algorithms.

2.11.3. Advantages of Hybrid Detection






Hybrid detection, a methodology that combines multiple detection techniques, has garnered increasing attention and adoption in various fields, particularly in the realm of threat detection and security. This section lists the manifold benefits associated with hybrid detection approaches as listed below:

- **Improved Accuracy:** By combining methods, the system can achieve higher accuracy by reducing the likelihood of false positives and negatives.
- **Robustness:** Hybrid systems are often more robust to variations in the environment or changes in the behaviour of individuals, as they are not reliant on a single mode of detection.
- **Adaptability:** If one method fails or performs poorly in a specific situation, other methods can compensate, making the system adaptable to different scenarios.

2.12. Suspicious Object Construct Comparative Analysis

In security contexts, the perceived threat level of an object can vary based on its context and the specific environment. Objects that are considered normal in one area may raise suspicion or pose a potential threat in a different setting. For example, a suitcase left unattended in a shopping mall might be perceived differently than the same suitcase left unattended at an airport or a train station. This shift in perception is due to the different security concerns and potential risks associated with each location. However, some common elements or behaviours associated with robbery might include (Table 10). In any security system, it is crucial to employ a holistic approach that considers multiple factors, including behaviour, context, and, if applicable, the objects people are carrying. It is also important to implement safeguards to prevent unwarranted intrusions into individuals' privacy and to ensure that any security measures adhere to legal and ethical standards.

Table 10. Suspicious object construct comparative analysis

Object Type	Purpose	Example	Image
Concealing Clothing	Robbers may wear clothing that helps conceal their identity	Hooded sweatshirts, masks, or caps	
Weaponry	Robbers may use weapons to intimidate or threaten victims	Firearms, knives, or makeshift weapons	
Quick Getaway Items	Robbers might use objects or tools that aid in a quick getaway	Motorcycles, bicycles, or even getaway vehicles	
Disguises	Some robbers may use disguises to blend in with the environment or to appear less suspicious.	Security guard, cleaner, maintainer	
Bags or Container	Robbers might carry bags or containers to hold stolen items or to transport goods quickly.	Money bag, bag	

3. Proposed Materials and Methods

A thorough understanding of computer vision, deep learning, and programming is needed to design the YOLOv7 algorithm to conduct facial recognition for the purpose of detecting fear and identifying victims and criminals. This is a condensed list of the steps that are involved:

3.1. Compile a Dataset

Gather a lot of face-containing photos, preferably with people that appear nasty or with scared expressions, like FER-2013, CK+, or JAFFE. A camera or webcam will also be used to produce a number of photographs for an additional dataset. Add annotations to these pictures to show if they depict fear or malevolence.

3.2. Prepare the Dataset

To make the photographs compatible with the YOLOv7 algorithm, resize and normalize them to a standard size. Divide the dataset into sets for testing and training.

3.3. Train the YOLOv7 Model

The YOLOv7 algorithm is trained using the training set. This entails feeding the algorithm the photographs so that it can be trained to identify face traits linked to malevolence and terror. Creating a mapping from the facial expressions to the associated input images is the goal. PyTorch and Darknet are two frameworks that can be used to train the YOLOv7 model. As an alternative, deep learning frameworks like PyTorch, Keras, or TensorFlow can be used to train the model using Convolutional Neural Network (CNN) architectures like VGG, ResNet, or Inception.

3.4. Fine-Tune the Model

You might need to use transfer learning to fine-tune the trained YOLOv7 model to detect fear and maliciousness precisely. In this procedure, a pre-trained model (such as YOLOv7) is used and continues to train using your customized dataset that has annotations for maliciousness and fear.

3.5. Gather and Handle Video Data

Gather video data from surveillance cameras or other sources. Divide the video into its component frames.

3.6. Use the YOLOv7 Model

Use the trained YOLOv7 model to identify faces in each frame of the video and assess their looks and expressions for signs of malice and fear. Model evaluation metrics include F1-score, recall, accuracy, and precision.

3.7. Trigger Matching Detections

You can configure a system to sound an alarm or alert security authorities if the YOLOv7 algorithm detects a face displaying fear or an individual who appears suspicious. This can be accomplished by deploying the algorithm or connecting

it with a notification system or other communication tool. Integrate the trained model into a real-world application, such as a web or mobile app. You can use a deep learning framework such as TensorFlow.js or ONNX to deploy the model on the edge of the cloud.

It is important to note that implementing an effective and accurate system for facial recognition and emotion detection requires expertise in computer vision and deep learning, as well as access to appropriate datasets and computational resources. Additionally, ethical considerations should be considered to ensure privacy and fairness when using such systems.

4. Conclusion

To improve crime prevention mechanisms, this research presented a thorough review of current facial recognition algorithms intended for the detection of fear and evil intent. Using sophisticated machine learning algorithms and a large dataset of facial expressions, our research showed the algorithm's capacity to properly recognize facial expressions and micro-expressions linked to fear and hostile intents. By giving law enforcement and security agencies a proactive tool to monitor and assess threats in real-time, the algorithm's incorporation with security systems has the potential to transform how they anticipate and prevent criminal activity completely.

The results of this study highlight how crucial it is to take strict privacy precautions and ethical issues into account when implementing facial recognition technology for crime prevention. To ensure that the advantages of such advances do not come at the expense of individual liberties and privacy, these technologies must be used in a way that respects individual rights and freedoms.

Looking ahead, the study provides several directions for additional research. Future research could examine how to improve the precision and dependability of intent recognition by integrating additional biometric indications, such as speech patterns and body language. To overcome privacy concerns and increase public confidence in these systems, rules and norms for the moral application of face recognition technology in security applications must be developed.

In conclusion, a major development in crime prevention technology is the use of face recognition algorithms to identify fear and malevolent intent. However, a balanced strategy that considers both the technological capabilities and the ethical implications of their use is necessary for the successful and responsible application of these technologies. Through the prudent application of artificial intelligence in crime prevention, we can anticipate safer communities if these technologies are further developed and the related issues are resolved.

Acknowledgments

The authors would like to acknowledge all Universiti Sains Malaysia (USM) staff and students, especially National Advanced IPv6 Center (NAv6), RCMO and BJIM staff, and those working under Intelligent Connected Streetlights (ICS) research project for their full support, resulting in the publication of this paper.

Funding Statement

This paper is the outcome of the Intelligent Connected Streetlights (ICS) research project work supported by Renesas-Universiti Sains Malaysia (USM) industry matching grant as per MoA#A2021098 agreement with grant account no [7304.PNAV.6501256.R128].

References

- [1] Ultralytics, GitHub. [Online]. Available: <https://github.com/ultralytics/yolov5>
- [2] J.D., and J.A.B. Smith, "The Evolution of Human Detection Systems: From Early Concepts to Advanced Technologies," *Journal of Advanced Technology and Innovation*, pp. 112-128, 2020.
- [3] V.A. City, The Famous Antwerp Diamond Heist!. [Online]. Available: <https://www.visitantwerpcity.com/antwerp-diamond-heist.html>
- [4] The Theft, Isabella Stewart Gardner Museum. [Online]. Available: <https://www.gardnermuseum.org/about/theft-story>
- [5] Lawrence Lease, The Banco Central Burglary: A Daring Heist That Shocked the World, HubPages, 2023. [Online]. Available: <https://discover.hubpages.com/politics/The-Banco-Central-Burglary-A-Daring-Heist-That-Shocked-the-World>
- [6] The Graff Diamond Heist : One of The Most Expensive in London's History, The Natural Sapphire Company, Sapphires, 2015.
- [7] P. Malagarriga, The Robbery in 1981 at the 'Banco Central' and its Connection with Hotel Contintalel Atraco Al Banco Central de 1981 Y Su Vinculación Con Hotel Continental, Hotel Continental, Barcelona, 2023. [Online]. Available: <https://blog.hotelcontinental.com/the-robbery-at-banco-central-in-1981-connection-with-hotel-continental/>
- [8] The Millennium Dome Heist, Crime + Investigation. [Online]. Available: <https://www.crimeandinvestigation.co.uk/crime-files/millennium-dome-heist>
- [9] Sophia S. Pasalis, The British Museum: A Rogue Curator and a Long History of Theft, The Harvard Crimson, 2023. [Online]. Available: <https://www.thecrimson.com/article/2023/11/16/british-museum-rogue-curator-theft-artifacts-digital-collection/>
- [10] BMS Controls Articles, The Benefits of Access Control In Facilities Management: Enhancing Security, [Online]. Available: <https://bmscontrols.co.uk/blog/the-benefits-of-access-control-in-facilities-management-enhancing-security/>
- [11] J. Redmon et al., "You Only Look Once: Unified, Real-Time Object Detection," *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, USA, pp. 779-788, 2016. [CrossRef] [Google Scholar] [Publisher Link]
- [12] Jonathan Hui, SSD Object Detection: Single Shot Multibox Detector for Real-Time Processing, 2018. [Online]. Available: <https://jonathan-hui.medium.com/ssd-object-detection-single-shot-multibox-detector-for-real-time-processing-9bd8deac0e06>
- [13] 10 Main Types of Smiles and What They Really Mean, Healthline, 2019. [Online]. Available: <https://www.healthline.com/health/types-of-smiles>
- [14] American Psychological Association, Publication manual of the American Psychological Association (7th ed.), APA PsycNet, 2020. [Online]. Available: <https://psycnet.apa.org/record/2019-59141-000>
- [15] Marcus Andrews, 10 Types of Anger: What's Your Anger style?, 2002. [Online]. Available: <https://lifesupportscounselling.com.au/resources/blogs/10-types-of-anger-what-s-your-anger-style/>
- [16] Common and Unique Phobias Explained, Healthline. [Online]. Available: <https://www.healthline.com/health/list-of-phobias>