INTELLIGENT CRIMINAL IDENTIFICATION SYSTEM FOR SEMI-REGULATED ENVIRONMENTS

***Ganiyu, S. O.[1]; Akpagher, T. D.[2]; Olaniyi, O.M[3]; &Adebayo, S. O.[4]**

1Department of Computer Science, Kampala International University, Kampala, Uganda
1,2Department of Information Technology, Federal University of Technology Minna, Nigeria
3Department of Computer Engineering, Federal University of Technology Minna, Nigeria
4Department of Computer Science, Islamic University in Uganda, Mbale, Uganda
4Department of Cyber Security Science, Federal University of Technology Minna, Nigeria
Email: ganiyu.shcfiu@kiu.ac.ug, shcfiu.ganiyu@futminna.edu.ng

Abstract

Nowadays, algorithms and technologies for criminal identification systems are imperative for the fight against crime in every environment. Thus, closed-circuit television cameras are now being incorporated into physical security mechanisms to identify suspects and criminals at crime scenes. However, crime investigators often spend a great deal of time unravelling the identities of criminals in lengthy video footage, especially in a semi-regulated environment where both known and unknown faces are always present. However, the research that combined a Single Short MultiBox Detector (SSD) and Local Binary Patterns Histograms (LBPH) for criminal identification in a semi-regulated environment is yet to be explored. Hence, this study developed a system that proactively identifies known criminals or documents the presence of non-criminals for reactive investigation by combining SSD with LBPH. To achieve this, SSD was employed to detect faces, while the LBPH algorithm for face recognition. Also, the system sends security alerts via email and short message service once a criminal is identified in the environment. Based on the faces captured by the identification system, SSD and LBPH achieved a precision of 95% and 90% respectively. With this achievement, the system will not only reduce the time taken to identify criminals in a semi-regulated environment, but also will improve the chances of reporting the presence of confirmed criminals.

Keywords: Criminal Identification, Deep learning, Face Detection, Face Identification, LBPH, Semi-regulated Environment.

INTRODUCTION

Apparently, crime is an aspect of societal challenges that has continued to pervade almost all facets of human endeavours. It can be described as an act that leads to offences, which are punishable under applicable laws of the land and the corresponding punishments depends on magnitude of crime, time and location (Oguntunde *et al.*, 2018). Relatedly, crime can be any action that contradicts the criminal (or penal) code of a state. For example, the penal and criminal codes enacted in Nigeria over 50 years ago are still operational in spite of the waves of new digital crimes. Unfortunately, crime rate has continued to increase yearly in many locations (Kakkar & Sharma, 2018). For example, the number of reported crimes in Nigeria rose from 125,790 in the year 2016 (NBS, 2017) to 134,663 in 2017 (NBS, 2018).

Thus, in order to catchup with present criminal activities, law enforcement agencies are developing or adopting innovative and technology-driven strategies to fight crime, popular among them is the use of biometric identification (Chhoriya, 2019). Simply put, biometric identification is based on the principle that every individual can be

identified by a unique and specific set of recognizable and identifiable set of data (Halvi *et al.*, 2017; Malathi & Raj, 2016). For instance, features such as fingerprint, voice and facial recognition can be used to detect known criminals, spot the entry and exit of individuals.

Ordinarily, security agents are expected to unravel the facial identity of criminals at crime scenes and conduct necessary investigations to aid criminal justice. However, the lack of technology-driven solutions to promptly identify criminals in semi-regulated environments is hampering the smooth operations of security agents. Consequently, the increase in crime rates can be partly attributed to the fact that some criminals who continued to commit crimes in our environments are supposed to be convicted if identified on time. In order to address the problem of criminal facial identification, some research efforts like Abdullah *et al.* (2017), Azeta *et al.* (2015), Chhoriya (2019) Gurav *et al.* (2015), Halvi *et al.* (2017), Kakkar and Sharma (2018), Kumar *et al.* (2018), Sanjay and Priya (2022), Sarkar and Prasad (2022), and Zafar *et al.* (2019) were proposed to assist law enforcement agents in identifying criminals in unregulated and regulated environments through facial recognition systems. However, a thorough review of relevant literature revealed that facial recognition system which combined Single Shot MultiBox Detector (SSD) (Liu *et al*., 2016) with LBPH to identify criminals in semi-regulated environments is yet to be established (Sarkar & Prasad, 2022; Tela *et al*., 2022).

In line with the foregoing, this study designed and developed a facial identification system that combined SSD (a variant of deep learning algorithms) with LBPH to assist criminal identification. Specifically, SSD was used for face detection, while LBPH was used to predict the confidence of detected faces. The developed system is a continuation of Ganiyu *et al.* (2020). It could detect, recognise, document and initiate security alerts when criminals or suspects are in semi-regulated environments. In essence, the system has the potential to identify both known and unknown faces to aid security agencies in criminal investigations. Significantly, this research effort will reduce the time spent searching for criminal faces in video feeds and improves the accuracy of search result. Similarly, it simplifies and provides real-time identification of suspects and criminals in semi-regulated locations by automatically documenting and updating information about known criminals and unknown persons.

The remainder of this paper is organised as follows: section 2 reviews literature that relates to the research, section 3 presents the methodology employed in the design and development of the proposed system, section 4 discusses the implemented facial recognition system and section 5 concludes and recommends future enhancement to the system.

BACKGROUND

The rowdiness and unrestricted movement of people, especially in crowdy public places have provided criminals with a plethora of opportunities to perpetrate various crimes (Kumar *et al.*, 2018). These criminals operate in public and private places, loiter around, stalk unsuspecting individuals, and commit crimes due to insufficient or unavailability of physical security measures. Somehow, the modus operandi adopted by criminals will likely depend on restriction to movement within an environment and time amongst others. For example, the styles adopted by malefactors to perpetrate crimes in public places like train station (unregulated environment), will be quite different from those used in secluded locations such as offices within corporate building (regulated environment). Similarly, criminals might reconnoitre different styles in locations that is neither regulated or unregulated, that is, semi-regulated

environment like banking halls and customer service centres.

Furthermore, facial recognition is a subset of biometric identification with certain advantages, such as high accuracy, uniqueness and low intrusiveness over other biometric-based identification methods (Aanchaladevi *et al.*, 2021; Abdullah *et al.*, 2017). Hence, these advantages make it a modest biometric tool for criminal identification and security systems (Tiwari *et al.*, 2015). Also, facial identification systems largely utilise database of saved faces against which comparison is made with captured faces, this comparison could either lead to a match (recognised face) or an unmatched outcome (unrecognised). Therefore, biometric identification systems are simple, convenient and agile means to mitigate criminal activities in any environment (Naik *et al.*, 2019; Singh & Prasad, 2018). Although biometric recognition systems have some limitations, including privacy violations, illuminations, age changing, falsification of faces, face positions, threats to personal rights and data vulnerabilities, these shortcomings were addressed by Karimov *et al.*, (2017). The expected benefits of facial recognition in this study outweigh the limitations.

Mostly, there are two components in a facial identification systems, namely face detection and face recognition (Abdullah *et al.*, 2017). Foremost, face detection is the ability of such systems to distinguish human face from other background images. Next, the recognition component classifies a detected face as that of human, even in the presence of other animal faces that have close facial geometry with human face. Still, the recognition component compares the detected face with already known faces to comprehensively describe the former. Broadly, facial recognition techniques can be categorised into Eigenface, neural network, Fisherface and elastic bunch graph matching (Reddy, 2017). Thus, several statistical and machine learning algorithms could be implemented to separately detect or recognise faces in identification systems (Alskeini *et al.*, 2018; Deeba & Ahmed, 2019; Du *et al.*, 2018; Singh & Prasad, 2018; Zafar *et al.*, 2019). Likewise, several criteria such as the distance of the face from the camera, the angle of the camera relative to the face, wearing of face accessories, memory usage, recognition rate, and data representation, are commonly used to evaluate the accuracy of these algorithms to ascertain their effectiveness for detecting or recognising human faces (Ahmad *et al.*, 2021; Saini *et al.*, 2014).

Currently, the trend in face identification is progressively transitioning from manual methods to the use of deep learning algorithms (Sarkar & Prasad, 2022; Trigueros *et al.*, 2018). Deep learning is an emerging machine learning concept that is based on Convolutional Neural Network (CNN). It is now being used in various aspect of computing including image processing, particularly for computer vision project with very large dataset (Trigueros *et al.*, 2018). Relatedly, Local Binary Patterns Histograms (LBPH) is among the efficient and simple facial recognition algorithms (Deeba & Ahmed, 2019). It extracts local features from digital images and performs well in recognising both front and side views of human face in different lighting situations (Kakkar & Sharma, 2018), differing facial expressions and poses (Jaturawat & Phankokkruad, 2017; Tela *et al.*, 2022).

Interestingly, some systems and conceptual frameworks have been developed to ease the process of recognising or identifying people through facial identification systems (Azeta *et al.*, 2015; Halvi *et al*., 2017; Sukhija *et al*., 2016; Zafar *et al*., 2019). For example, Ganiyu et al., (2020) proposed an architecture that used deep learning approach for face detection and LBPH algorithm for face recognition, thus creating a hybrid approach to harness the advantages of both LBPH and deep learning approaches for facial identification. Some recent criminal identification systems only find a match for a particular criminal face

(Aanchaladevi *et al.*, 2021; Kakkar & Sharma, 2018; Kumar *et al*., 2020), while others can send threat notifications when faces of documented criminals are detected (Baraka *et al.*, 2021; Kumar *et al.*, 2018).

RELATED WORK

Over the years, facial detection, recognition and identification algorithms have caught the attention of researchers in the field of computer vision. Hence, some research in the domain developed and enhanced the algorithms and their applications to various challenges requiring computer vision, such as crime prevention, control, and analysis. For this reason, Alskeini *et al.* (2018), Deeba and Ahmed (2019), Sukhija *et al.* (2016), Zafar *et al.* (2019) conducted researches on different facial recognition algorithms to demonstrated their suitability and performances. On one hand, Zafar *et al.* (2019) investigated the performance of Bayesian convolution network for facial recognition in surveillance camera. On the other hand, Deeba and Ahmed (2019) proposed an enhancement to LBPH for real-time facial detection. More so, Du *et al.* (2018) and Siregar *et al.*, (2018) applied facial recognition algorithms to embedded system and cloud security respectively. Specifically, Abdullah *et al.* (2017), Azeta *et al.* (2015), Chhoriya (2019), Gurav *et al.* (2015), Kakkar and Sharma (2018), Kumar *et al.* (2018), Naik *et al.* (2019), and Nguyen *et al.* (2018) developed criminal recognition or identification systems using facial detection and recognition algorithms.

Furthermore, Tela *et al.* (2022) used CNN to implement criminal identification system but the system cannot take image directly from CCTV camera in real time. In addition, Aanchaladevi *et al.* (2021), Kumar *et al.* (2020), and Sarkar and Prasad (2022) implemented criminal detection with Haar cascade algorithm. Likewise, Sanjay and Priya (2022) developed a system to improve criminal identification system using CNN and Haar cascade. Similarly, Ahmad *et al.* (2021) implemented a video surveillance system using Haar cascade to identify faces under the following constraints; when accessories cover parts of the face, when a face is positioned at particular angles to the camera, and when the face is far from the camera. According to Sanjay and Priya (2022) and Shepley (2019), Haar cascade classifier is less efficient than CNN for criminal identification.

In order to underpin the importance of computer vision algorithms to criminal identification, Jaturawat and Phankokkruad (2017), Reddy (2017), Saini *et al.* (2014), Singh and Prasad (2018) and Trigueros *et al.* (2018) conducted extensive reviews and evaluations of several facial recognition algorithms. Recently, Ganiyu *et al.* (2020) reviewed facial recognition algorithms and systems for criminal detection. The authors classified the application domains of existing facial recognition systems into *regulated*, *semi-regulated* and *unregulated* environments. Additionally, the systematic review showed that significant effort had been expended on criminal detections in unregulated and regulated environments, while semi-regulated environment is yet to receive research attention.

Generally, one obvious limitation of existing criminal identification systems is that they rely on a sufficiently populated database of criminals' faces against which comparison were made to recognise and subsequently identify criminals. However, the prepopulated database might not be readily available for identification systems deployed in unregulated or semi-regulated environments. Again, as opined by Trigueros *et al.* (2018), previous research efforts have not explored any hybrid method that comprises deep learning and LBPH for criminal identification, especially in a semi-regulated environment where the dataset of suspected criminals might be limited.

METHODOLOGY

This section presents the tools employed to design and develop the proposed criminal identification system, including use case

diagram, system architecture and block diagram. Also, it covers the technique adopted to evaluate the performance of the proposed system.

SYSTEM DESIGN

Primarily, the proposed system will identify criminals in a semi-regulated environment. The system works with three categories of people commonly found in the semi-regulated environment during crime investigations. First, it documents the presence of *known criminals* already tagged due to previous criminal activities. The people in the second category are *known individuals* whose identities are known to the system as non-criminals. The third category belongs to *unknown individuals (strangers)* neither tagged as criminals nor recognised by the system as non-criminals. In events of crime cases, the people in the third category become prime suspects. Thus, Fig. 1 represents the architecture of the proposed system. It also depicts all the major components within the system and external entities and the interactions among all the system's modules. These components include CCTV cameras, security officers designated in an organisation, the system administrator, external security personnel or law enforcement agents (e.g., police) and facial identification software, which in turn comprises detection and recognition algorithms.

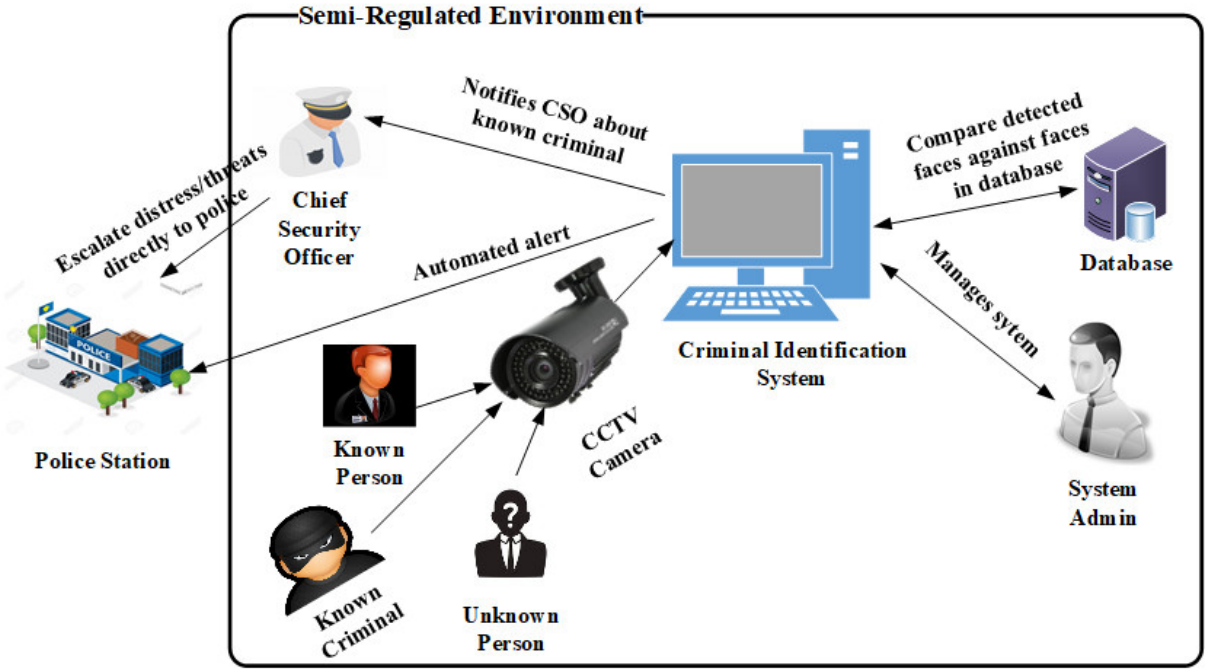

Fig. 1: Architecture of proposed system

Use Case of the Proposed System

The use case diagram captures the basic actions performed by each user in the proposed system, as represented in Fig. 2. As depicted in the figure, the supervisor is in charge of all the activities relating to system maintenance. Thus, the Admin creates security staff who can log into the system to register known individuals and criminals. For security reasons, certain security privileges are restricted for execution by the supervisor to ensure that other security staff who have access to the system do not perform the function, which can compromise the security of the criminal identification system. For instance, any record deleted by the staff is still viewable by the supervisor or even restored to the system.

As shown in Fig. 2, any individual detected by the CCTV camera could be a known person, criminal or stranger. Once a camera

detects a criminal, the Chief Security Officer (CSO) will receive a security notification or alert. In addition, the CSO oversees that particular environment and gives instructions for immediate actions. Thus, the CSO manages physical security devices and escalates security alerts about criminals or suspects to law enforcement agents duly registered on the system. The threat escalation component sends distress notifications via Short Message Service (SMS) and Electronic Mail (email) messages to the law enforcement agent for necessary action to complement the internal security posture of an organisation.

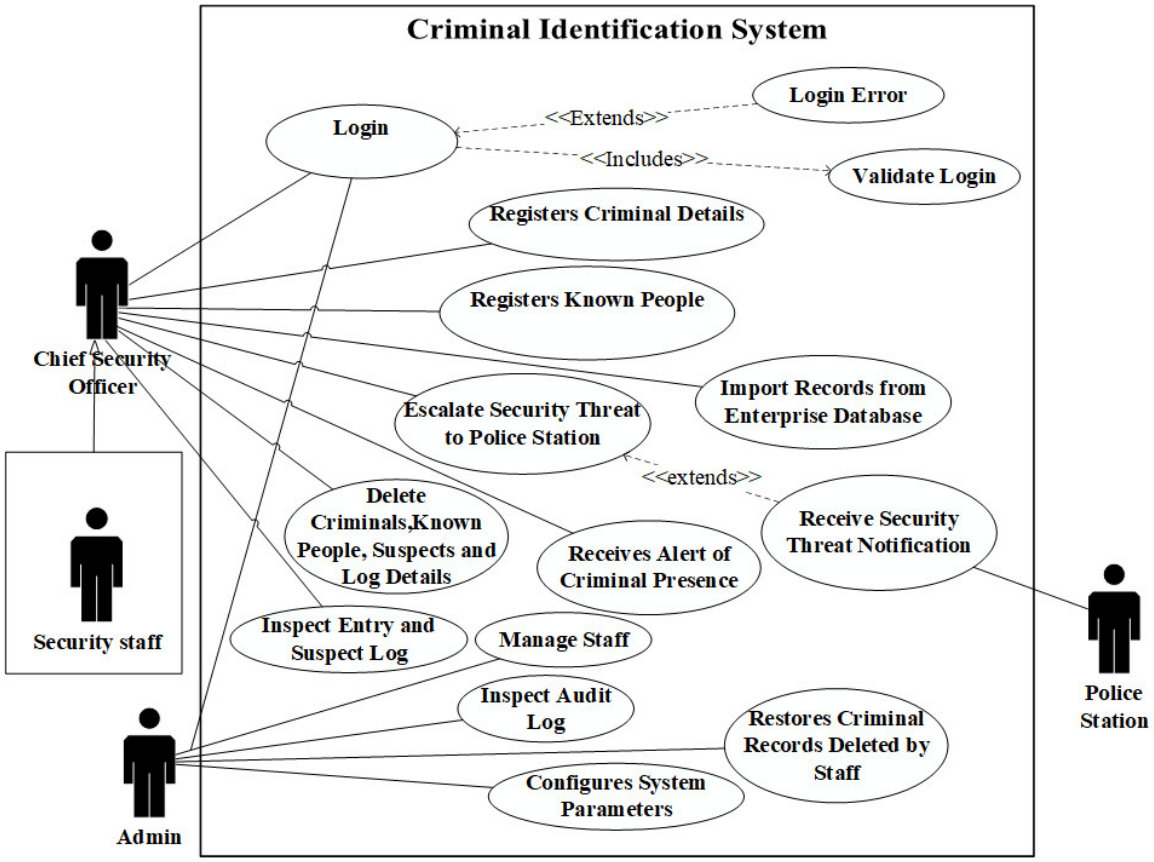

Fig. 2: Use Case Diagram of the Proposed

Flowchart of the Proposed System

In addition, the flowchart presented in Fig. 3 reinforces the design of the proposed system. For this purpose, the entire system is divided into distinct programming tasks and rendered with appropriate flowchart symbols. Primarily, identifying faces involves training the model with the faces of known individuals (registered) in the system. These faces will constitute the training dataset. Afterwards, the recognition module processes the faces captured by the CCTV camera. Once a face is detected, the system predicts its confidence value. If the confidence value is less than the predetermined ideal confidence, the face is recognised as either a known individual or a criminal. Otherwise, the system categorises the face as an unknown face and saves the detected face along with other information like the date and time of detection.

Block Diagram of the Proposed System

Furthermore, the flow of the proposed system is illustrated by the block diagram presented in Fig. 4. The block diagram provides an overview of relevant modules that ensure the seamless and effective running of the system. As the block diagram reveals, the system receives the video feed from strategically positioned cameras. Next,

the deep learning algorithm detects the human faces in the video feed. Subsequently, a face recognition module executes to predict the confidence of the detected face. Once the confidence value is determined using the LBPH recogniser, the value is compared with the target value (of known faces). Therefore, if the confidence value is less than the target value, then the face is recognised. It follows that a recognised face can either be a criminal or a known (non-criminal) face whose identity already exists in the system. The proposed facial identification system will document the necessary details after a criminal's face is recognised. In addition, the system will send an alert to the CSO of the organisation, and the registered police unit will be alerted. In the case of an identified non-criminal individual, the time and date are documented appropriately for future reference. However, if the confidence value is greater than the target value, the detected face of the unknown individual is cropped, and documented with the time and date when it was captured. In such case, the system's flow would stop at the recognition phase, because identification cannot be performed without prior information of individuals. Lastly, the admin has access to the facial records of both criminals and known people and can restore deleted records of criminals.

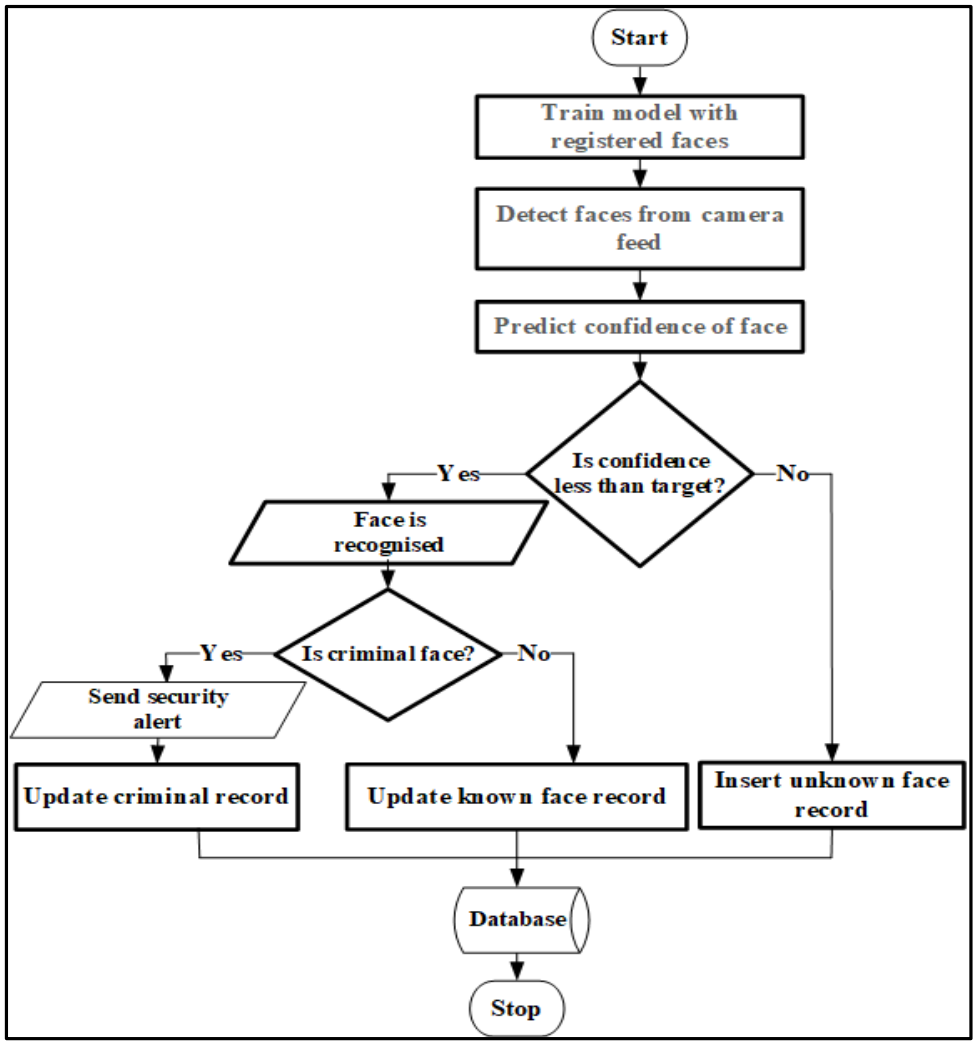

Fig. 3: Flowchart of Criminal Facial Identification System

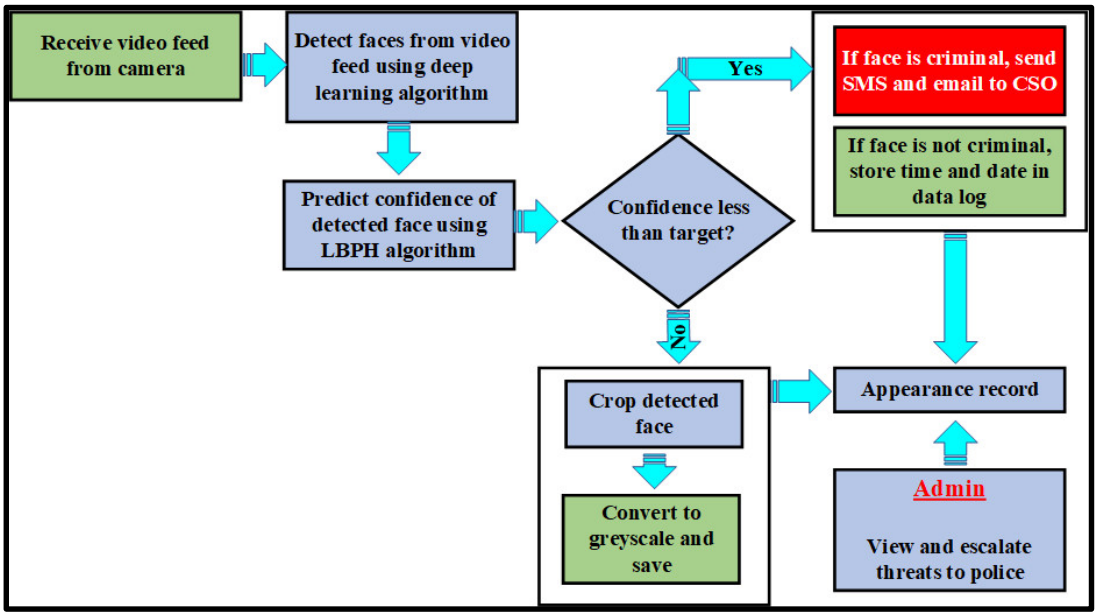

Fig. 4: Block diagram showing important modules (Adapted from Ganiyu *et al.*, (2020))

Implementation of the Proposed Criminal Identification System

The proposed system was implemented as a desktop application using *JavaFX*. Further, MySQL was used to store and manage all data for the proposed facial identification system. Also, Application Programming Interfaces (APIs) from *JavaCV*, which is a Java flavour of *OpenCV* was employed for detection and recognition modules. The detection module was implemented using deep learning that consists of two files; a *Prototxt*, which defines the model architecture, and a *Caffe model*, which contains the weights of actual layers. Furthermore, the detection module is built on an SSD framework with a *ResNet*-based network. Particularly, SSD was selected due to its efficiency over other traditional methods for face detection such as LBP and Haar Cascade classifiers (Shepley, 2019). Subsequently, the recognition of faces was achieved using LBPH facial recognition algorithm. Before adopting LBPH, a comparison between Eigenface, Fisherface and LBPH algorithms was carried out. Interestingly and LBPH gave the best result for face recognition.

Performance Evaluation of Proposed Criminal Identification System

This performance evaluation was performed using a confusion matrix presented in Table 1. The matrix comprises measures like a true positive, false positive, false negative and true negative. Also, the performance evaluation involves other performance metrics such as precision, recall, error rates, accuracy and sensitivity. All the performance metrics were utilised to evaluate how well the facial recognition system correctly identified faces already tagged as criminal and non-criminal.

Table 1: Confusion Matrix

		Actual Values	
		Positive	Negative
Predicted Values	Positive	True Positive (TP)	False Negative (FN)

The explanation and mathematical realisation of these performance metrics are as follow:

Precision: Otherwise known as reliability, is the fraction of the detected images that are correctly identified. As shown in Equation 1, precision is the total number of correctly recognized images divided by the total images tested,

$$Precision = \frac{TP}{(FP + TP)}. \quad (1)$$

Recall: This is also known as true positive rate and it is the proportion of positive cases that were properly identified as expressed in Equation 2. That is, it is the fraction of relevant images that are successfully detected,

$$Recall = \frac{TP}{(TP + FN)}. \quad (2)$$

Error Rate: This represents quantity of misclassification (misrecognition) over the overall number of validation samples as shown in Equation 3,

$$Error\ Rate = \frac{(FP + FN)}{(TP + FP + FN + TN)}. \quad (3)$$

Accuracy: Accuracy is defined as "the fraction of quantity of correct classification over the entire number of samples." This is represented by Equation 4. The number of predictions in classification techniques relies upon the counts of the test records that were properly or incorrectly predicted,

$$Accuracy = \frac{(TP + TN)}{(TP + FP + FN + TN)}. \quad (4)$$

Sensitivity: Sensitivity is otherwise known as true positive rate (TPR) or hit rate. As shown in Equation 5, it is a measure of how well a binary classification test properly identifies a condition probability of properly labelling members of the target class,

$$Sensitivity = \frac{TP}{(TP + FN)}. \quad (5)$$

RESULTS

Result Presentation

The proposed criminal identification system was implemented and all the modules were tested to ensure their functionality. Similarly, performance evaluation was conducted on the identification system using the performance metrics.

Implemented Criminal Identification System

Generally, all the modules included in the block diagram functioned as designed and implemented. Hence, this section illustrates the core module in the criminal identification system with appropriate screenshots.

Registering Known and Criminal Faces

The process of registering a known individual or criminal by security staff involves saving their basic details such as name, age, gender, and address amongst others. Thus, the registration involved capturing at least 20 images per individual. The face in each image is detected, cropped and then converted to grayscale as illustrated in Fig. 5, with a total of 20 individual faces captured.

Criminal Identification Message for Known Criminal

Normally, the system only documents the time and date for known individuals who can be customer, staff or known person who has not been flagged as a criminal. However, once a known criminal is identified, the

system automatically generates and sends alert notifications (email and SMS) to the chief security officer of the organization as shown in Figs. 6(a) and 6(b) respectively.

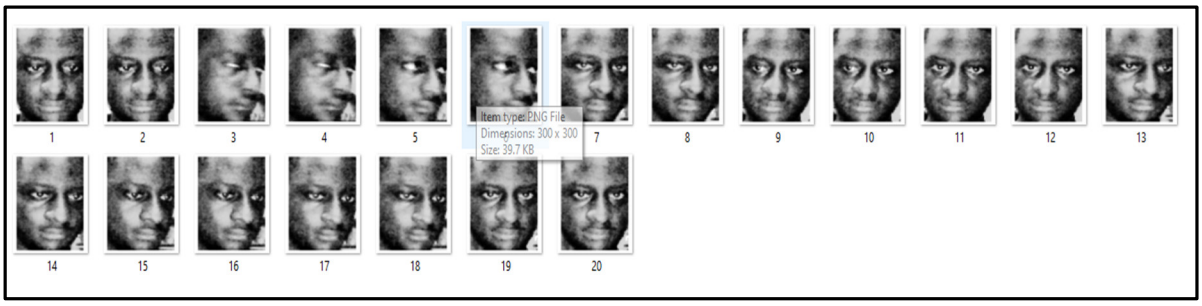

Fig. 5: Grayscale pictures of each individual

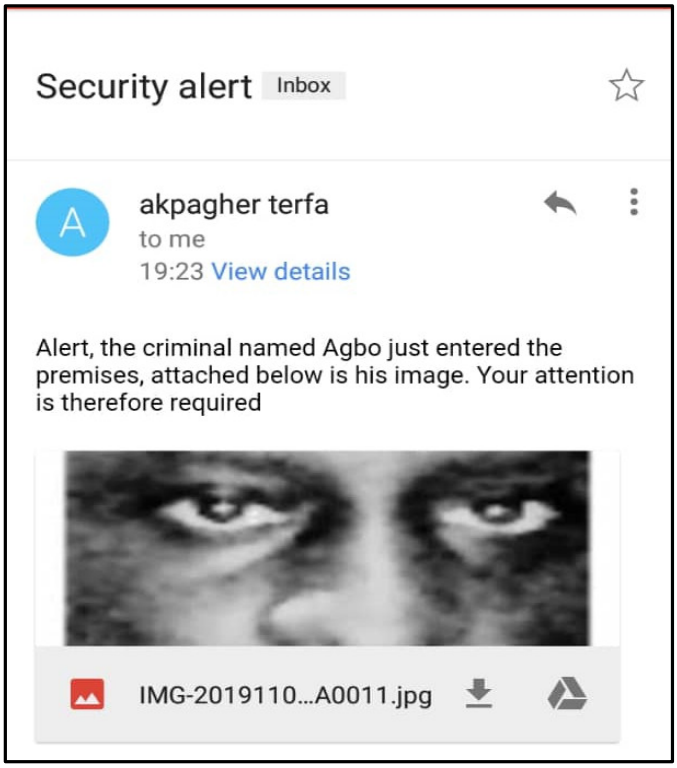

Fig. 6(a): Email notification to chief security officer

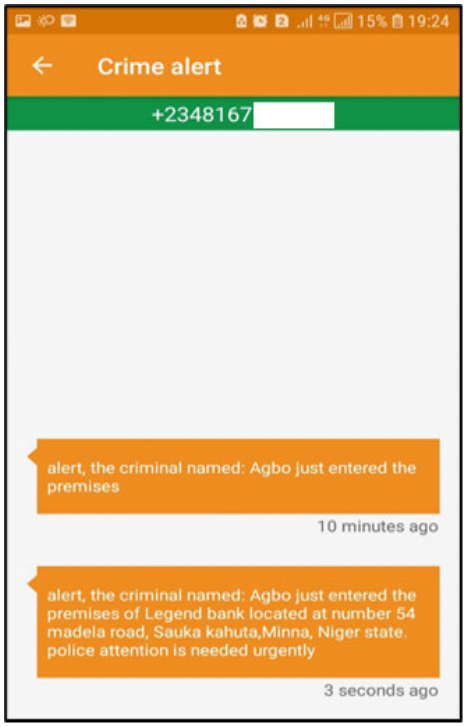

Fig. 6(b): SMS alert to police station

Generating Distress Security Alert

Additionally, any security staff who is currently logged into the system could generate and send distress emails and SMS to the registered law enforcement unit as shown in Figs. 7 and 6(b) respectively. This functionality is incorporated into the system to address security situations when the CSO has been overpowered or rendered incapacitated by criminals.

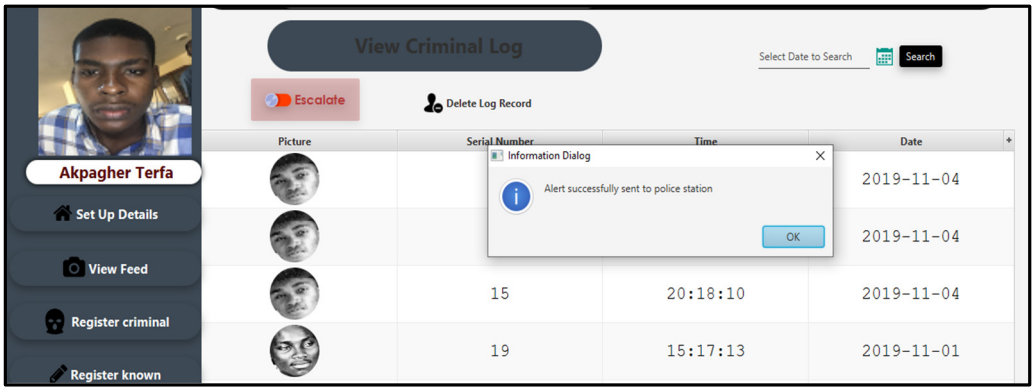

Fig. 7: Distress security alert

Documenting Unknown Faces for Future References

In a situation where the face that is spotted by the system neither matches the registered (known) person nor documented criminal, then the unidentified individual is tagged as a stranger to the semi-regulated environment. Reasonably, the system will automatically and temporarily retag such a stranger as a suspect, if any crime is reported during the time the stranger is within a semi-regulated environment. Hence, the system stores the face, time and date of each suspect as shown in Fig. 8. Therefore, it will become easier for both the security department of the

organisation and the police unit to search for the faces of strangers who are present at crime scenes. Furthermore, this functionality will reduce the time taken to recognise suspects, rather than filtering hours of video footage in the advent of crime occurrence.

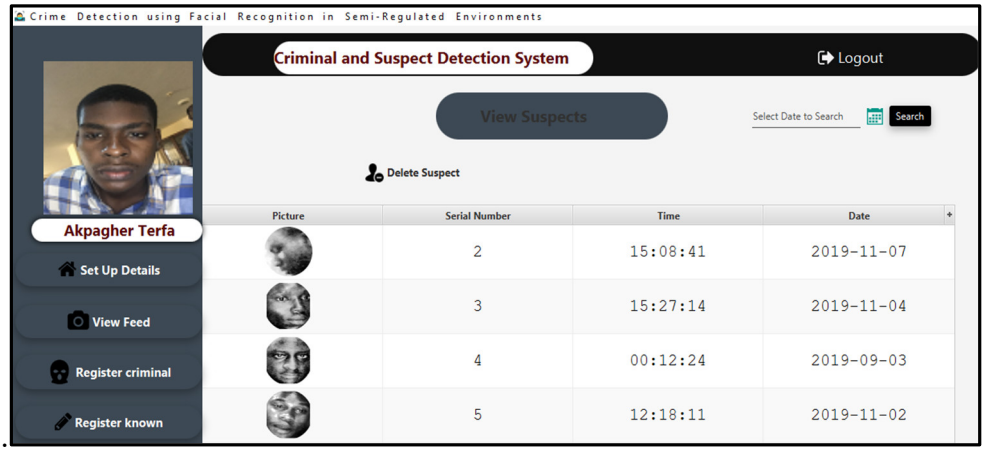

Fig. 8: Record of Unknown (Unidentified) Face

Performance Evaluation of Implemented Criminal Identification System

The detection and recognition modules of the criminal identification system were evaluated using a dataset comprising 20 images per person for 30 persons which were captured by the system. On one hand, deep learning algorithms were adopted due to their efficacy as facial detection algorithms (Sarkar & Prasad, 2022). On the other hand, LBPH, Fisherfaces and Eigenfaces are compared in order to determine the one with the best performance.

Performance Evaluation of Facial Recognition Algorithms

Foremost, a comparison of the three most reported facial recognition algorithms was conducted in order to select the facial recognition algorithm with the best performance as shown in Table 2. Hence, it revealed that LBPH has the best performance under the five (5) performance metrics that were discussed in section 3.3. For example, Fig. 9 shows performances of the algorithms under precision metric. As observed in the figure, LBPH had the best precisions even when the images were fewer than 10. In the case of Fisherfaces and Eigenfaces, there is no significant difference in their precision rates. Similarly, the precision of LBPH steadily increased with more images. Also, Fisherfaces and Eigenfaces had a steady increase in precision rates, and the three algorithms almost converged to the same precision when images were close to 30. Thus, LBPH learned better than the two other algorithms. The result made LBPH a more suitable facial recognition algorithm in a semi-regulated environment where only a few faces are known to the criminal identification system.

Table 2: Comparison of the three algorithms against dataset of registered faces

Algorithm	Precision	Recall	Error rate	Accuracy	Sensitivity
LBPH	0.90	0.90	0.15	0.84	0.9
Fisherfaces	0.85	0.83	0.23	0.77	0.80
Eigenfaces	0.82	0.80	0.25	0.75	0.80

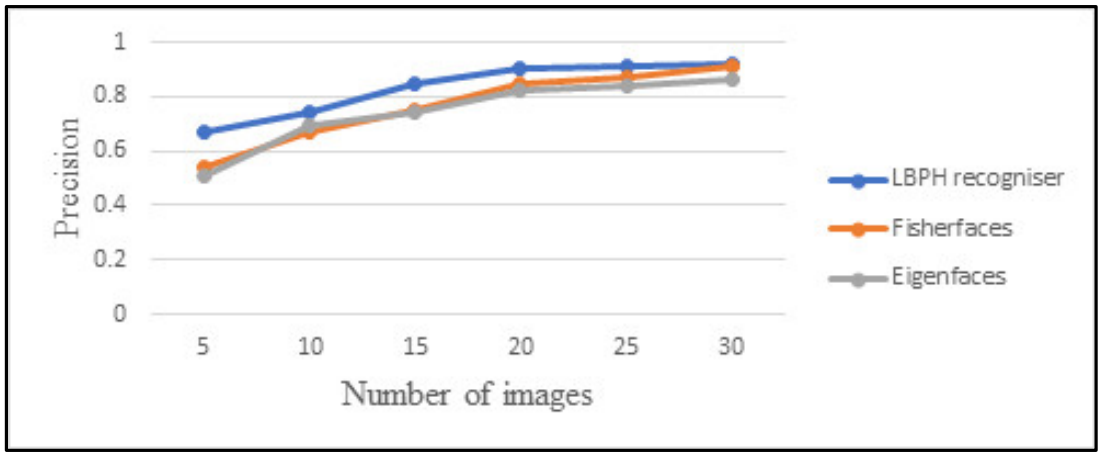

Fig. 9: Graph Precision Performance of Facial Recognition Algorithms

In addition, Figure 10 shows a graph comparing the speed of processing against number of images per person for LBPH algorithm. From Fig. 10, it can be can be seen that the processing time increases with increase in the number of images. Therefore, the number of images per person in the system was chosen to be 20 since it yielded moderate processing time and produced a high precision value. Significantly, the performance recorded by LBPH on this dataset points to the fact that this module was effective in recognising the registered faces in the system. Thus, it will contribute to the performance effectiveness of the system at large.

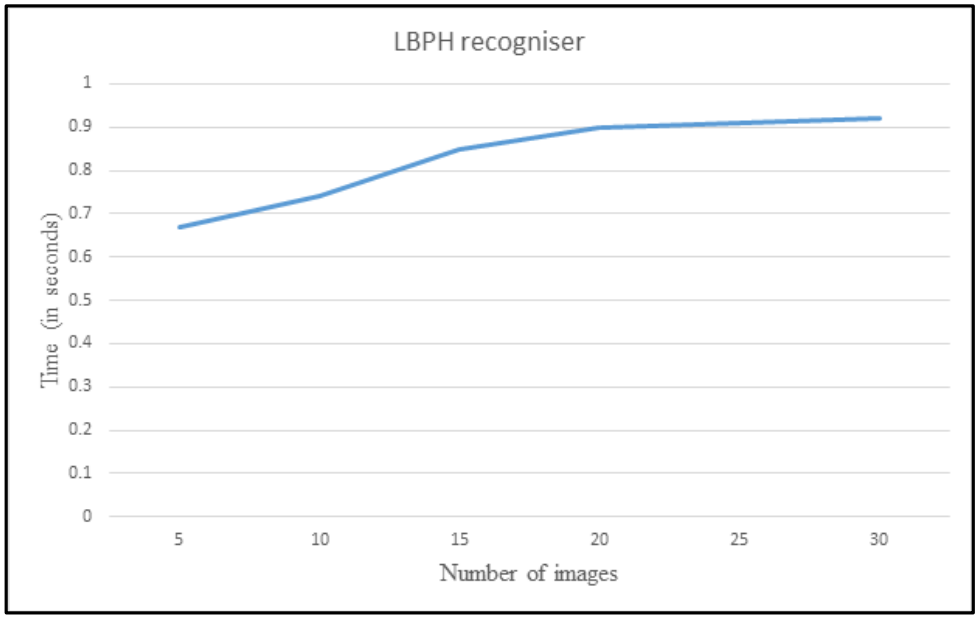

Fig. 10: graph of time against number of images for LBPH recognizer

Performance Evaluation of Face Detection

For the face detection module, the SSD algorithm was adopted and Table 3 is a Confusion matrix that shows the result of its performance evaluation. Again, the algorithm recorded precision and accuracy scores of 0.95 and 0.85 respectively. Going by the precision and accuracy attained by deep learning of the face detection module and considering the small size of the dataset, it was obvious that the detection of faces by the systems is effective enough to detect

faces in video footage. Above all, the performance of the module is expected to even increase for datasets with more facial records.

Table 3: Confusion Matrix for Deep Learning

		Actual Values	
		Positive	Negative
Predicted Values	Positive	19	3
	Negative	1	4

DISCUSSIONS

The proposed system provides security officials with an additional tool to promptly identify known criminals loitering in their environments. It is worth noting that uncovering criminals in semi-regulated environments can be a difficult task. For illustration, the manual processes involved in pinpointing criminals when both known and unknown faces visit a place, consume time and human effort. The manual methods involve scanning through CCTV live cameras or recorded videos to identify criminals. In addition, it is a common practice by physical security professionals to stack multiple layers of crime detection and prevention mechanisms. Therefore, it will be easy to integrate this crime prevention mechanism with existing access control measures to strengthen the security architecture of organisations operating in a semi-regulated environment.

Also, the criminal identification system generates alerts to notify security agents when a known criminal appears in an environment of interest. This notification module operates unobtrusively and criminals will not have any clue of impending actions on them. More so, the time taken to process facial data significantly reduces when the dataset increases. This suggests that the LBPH learns faster with the availability of more datasets. Correspondingly, the confusion matrix shows the impressive accuracies and precisions of the SSD and LBPH algorithms. Therefore, the system will flag criminals before they can execute their nefarious intents. The proposed criminal identification system benefits from the strengths of deep learning algorithms, and updating the system with more facial data is possible with backpropagation. Similarly, possessing digitised crime facts improves the storage and backup of information against sabotage and repudiation of crimes.

The operators of the criminal identification system must ensure the safety of facial records and other vital information about individuals. Any unnecessary disclosure or careless handling of records can jeopardise people's privacy. On the contrary, the system inherits the weaknesses of the deep learning algorithms on which it operates for precision and accuracy. For example, the identification system needs more computing resources to train the detection and identification modules as the number of facial records increases in capacity. Although, the cost implications of additional system resources are negligible compared to the loss that criminals can bring to the assets and organisation's reputation.

CONCLUSION AND RECOMMENDATIONS

Security of lives and properties from criminal elements is essential in public and private places. As part of contributions to academic values, this study designed and developed a criminal identification system for a semi-regulated environment using SSD to detect faces and LBPH for facial recognition. Despite the few facial records commonly found in semi-regulated

environments, the security system showed a high degree of accuracy in identifying known criminals' faces. Thus, social settings having few facial datasets could benefit from the system's adoption to maintain detailed information on criminals for future legal reference. Similarly, the proposed system will not only identify criminals, but it can also assist security officers in tracking individuals, thus creating a robust security system that could reduce the time spent by law enforcement agents in crime investigation. A limitation of the security system is that it encroaches on the data privacy of individuals in an environment since it tracks their facial records.

Moving forward, further research is needed to improve the efficacy and performance of the proposed system. Foremost, more research is required to develop more efficient and computationally inexpensive algorithms for handling facial recognition. Additionally, the design of a psychological-oriented module that can predict the likelihood of an unknown individual committing a crime is needed to complement the approach implemented in this study. Again, further research on privacy preservation is desirable to make the proposed system more acceptable in semi-regulated environments. Lastly, there is a need to integrate this system with the national citizen database to identify criminals and document the movement of other individuals in a semi-regulated environment to foster comprehensive security coverage at the national level.

REFERENCES

Aanchaladevi, T. S., Shubhangi, G. S., Ashwini, G. S., Mayuri, M. A., & Bankar, A. A. (2021). Criminal Identification by Using Real Time Image Processing. *International Journal of Research in Engineering and Science (IJRES)*, Vol. *9,* No. 6, 37–42.

Abdullah, N. A., Saidi, M. J., Rahman, N. H. A., Wen, C. C., & Hamid, I. R. A. (2017). *Face recognition for criminal identification: An implementation of principal component analysis for face recognition*. *October*, 020002. https://doi.org/10.1063/1.5005335

Ahmad, A. H., Saon, S., Mahamad, A. K., Darujati, C., Mudjanarko, S. W., Nugroho, S. M. S., & Hariadi, M. (2021). Real Time Face Recognition of Video Surveillance System Using Haar Cascade Classifier. *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 21, No. 3, 1389–1399. https://doi.org/10.11591/ijeecs.v21.i3.pp1389-1399

Alskeini, N. H., Thanh, K. N., Chandran, V., & Boles, W. (2018). Face recognition: Sparse representation vs. Deep learning. *ACM International Conference Proceeding Series*, 31–37. https://doi.org/10.1145/3282286.3282291

Azeta, A. A., Omoregbe, N. A., Adewumi, A., & Oguntade, D. (2015). Design of a Face Recognition System for Security Control. *International Conference on African Development Issues (CU-ICADI) 2015: Information and Communication Teclmology Track*, 55–57.

Baraka, A., Kataliko, S., & Digne, A. (2021). An Intelligent Criminal Detection System: A Case Study of Beni-town. *International Journal of Scientific and Research Publications*, Vol. 11, No. 11, 474–479. https://doi.org/10.29322/IJSRP.11.11.2021.p11961

Chhoriya, P. (2019). *Automated Criminal Identification System using Face Detection and Recognition*, Vol. 06, No. 10, 910–914.

Deeba, F., & Ahmed, A. (2019). LBPH-based Enhanced Real-Time Face Recognition. *International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 5, 274–280.

Du, B., Guo, X., & Chen, Y. (2018). Research on Face Recognition System based on Embedded Processor and Deep Neural

Network. *ACM International Conference Proceeding Series*, 11–14. https://doi.org/10.1145/3268866.3268880

Ganiyu, S. O., Olaniyi, O. M., Adebayo, O. S., & Daniel, A. T. (2020). Systematic Review of Facial recognition Algorithms and Approaches for Crime Investigations. *International Journal of Information Processing and Communication (IJIPC)*, Vol. 8, No. 1, 55–69.

Gurav, A., Chevelwalla, A., Desai, S., & Sadhukhan, S. (2015). Criminal Face Recognition System. *International Journal of Engineering Research And*, Vol. V4, No. 03, 47–50. https://doi.org/10.17577/ijertv4is030165

Halvi, S., Ramapur, N., Raja, K. B., & Prasad, S. (2017). Fusion Based Face Recognition System using 1D Transform Domains. *Procedia Computer Science*, *115*, 383–390. https://doi.org/10.1016/j.procs.2017.09.095

Jaturawat, P., & Phankokkruad, M. (2017). An evaluation of face recognition algorithms and accuracy based on video in unconstrained factors. *Proceedings - 6th IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2016*, *November*, 240–244. https://doi.org/10.1109/ICCSCE.2016.7893578

Kakkar, P., & Sharma, V. (2018). Criminal Identification System Using Face Detection and Recognition. *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 7, No. 3, 238–243. https://doi.org/10.17148/IJARCCE.2018.7346

Karimov, M. M., Ugli, I. S. Z., & Davronova, L. O. K. (2017). Problems in face recognition systems and their solving ways. *2017 International Conference on Information Science and Communications Technologies, ICISCT 2017*, *2017-Decem*, 1–4. https://doi.org/10.1109/ICISCT.2017.8188594

Kumar, P., Majeed, A., Pasha, F., & Sujith, A. (2020). Real-time Criminal Identification System Based on Face Recongnition. *Advanced Science Letters*, *26*(05), 320–328.

Kumar, V. D. A., Kumar, V. D. A., Malathi, S., Vengatesan, K., & Ramakrishnan, M. (2018). Facial Recognition System for Suspect Identification Using a Surveillance Camera. *Pattern Recognition and Image Analysis*, Vol. 28, No. 3, 410–420. https://doi.org/10.1134/S1054661818030136

Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.-Y., & Berg, A. C. (2016). SSD: Single Shot MultiBox Detector. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 9905 LNCS* (pp. 21–37). https://doi.org/10.1007/978-3-319-46448-0_2

Malathi, R., & Jeberson Retna Raj, R. (2016). An Integrated Approach of Physical Biometric Authentication System. *Procedia Computer Science*, Vol. 85, No. Cms, 820–826. https://doi.org/10.1016/j.procs.2016.05.271

Naik, A., Bakusala, R., Tiwari, S., Tiwari, T., Bhandari, P., & V, A. (2019). *Criminal identification using facial recognition*. Vol. 5, No. 3, 1936–1940.

NBS. (2017). *Crime Statistics : Reported Offences by Type and State*.

NBS. (2018). *Crime Statistics : Reported Offences by Type and State*.

Nguyen, T., Lakshmanan, B., & Sheng, W. (2018). *A Smart Security System with Face Recognition*. *December 2018*. https://doi.org/10.48550/arXiv.1812.09127

Oguntunde, P. E., Ojo, O. O., Okagbue, H. I., & Oguntunde, O. A. (2018). Analysis of

selected crime data in Nigeria. *Data in Brief*, Vol. 19, 1242–1249. https://doi.org/10.1016/j.dib.2018.05.143

Reddy, K. S. M. (2017). Comparison of Various Face Recognition Algorithms. *International Journal of Advanced Research in Science, Engineering and Technology*, Vol. 4, No. 2, 3357–3361.

Saini, R., Saini, A., & Agarwal, D. (2014). Analysis of Different Face Recognition Algorithms. *International Journal of Engineering Research & Technology (IJERT)*, Vol. 3. No. 11, 1263–1268.

Sanjay, T., & Priya, W. D. (2022). Criminal Identification System to Improve Accuracy of Face Recognition using Innovative CNN in Comparison with HAAR Cascade. *Journal of Pharmaceutical Negative Results*, Vol. 13, No. 4, 218–223. https://doi.org/10.47750/pnr.2022.13.S03.023

Sarkar, R. R., & Prasad, G. N. R. (2022). Criminal Detection Using Face Recognition. *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 11, No. 4, 367–370. https://doi.org/10.17148/IJARCCE.2022.11466

Shepley, A. J. (2019). *Deep Learning For Face Recognition: A Critical Analysis*. https://doi.org/10.48550/arXiv.1907.12739

Singh, S., & Prasad, S. V. A. V. (2018). Techniques and challenges of face recognition: A critical review. *Procedia Computer Science*, *143*, 536–543. https://doi.org/10.1016/j.procs.2018.10.427

Siregar, S. T. M., Syahputra, M. F., & Rahmat, R. F. (2018). Human face recognition using eigenface in cloud computing environment. *10th International Conference Numerical Analysis in Engineering*, *308*(1). https://doi.org/10.1088/1757-899X/308/1/012013

Sukhija, P., Behal, S., & Singh, P. (2016). Face Recognition System Using Genetic Algorithm. *Procedia Computer Science*, Vol. 85, No. Cms, 410–417. https://doi.org/10.1016/j.procs.2016.05.183

Tela, G., Hiwarale, S., Dhave, S., & Rathi, D. (2022). CNN Based Criminal Identification. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, Vol. 2, No. 2, 239–246. https://doi.org/10.48175/IJARSCT-3645

Tiwari, T., Tiwari, T., & Tiwary, S. (2015). Biometrics based user authentication. *Amercian Journal of Engineering Research*, *4*(10) Vol. 4, No, 10, 148–159.

Trigueros, D. S., Meng, L., & Hartnett, M. (2018). *Face Recognition: From Traditional to Deep Learning Methods*. https://doi.org/10.48550/arXiv.1811.00116

Zafar, U., Ghafoor, M., Zia, T., Ahmed, G., Latif, A., Malik, K. R., & Sharif, A. M. (2019). Face recognition with Bayesian convolutional networks for robust surveillance systems. *Eurasip Journal on Image and Video Processing*, Vol. 2019, No. 1. https://doi.org/10.1186/s13640-019-0406-y