Online: ISSN 2645-2960; Print ISSN: 2141-3959

Systematic Review of Facial Recognition Algorithms and Approaches for Crime Investigations

Shefiu Olusegun Ganiyu[1], Olayemi Mikail Olaniyi[2], Olawale Surajudeen Adebayo[3] and Akpagher Terfa Daniel[4]

[1,4]Department of Information and Media Technology, Federal University of Technology Minna, Nigeria
[2]Department of Computer Engineering, Federal University of Technology Minna, Nigeria
[3]Department of Cyber Security Science, Federal University of Technology Minna, Nigeria

[1]shefiu.ganiyu@futminna.edu.ng, [2]mikail.olaniyi@futminna.edu.ng, [3]waleadebayo@futminna.edu.ng, [4]terfa.akpagher@st.futminna.edu.ng

Abstract

Crime control in human societies has continued to pose significant problems and requires dynamic approaches to be subdued through effective investigation mechanisms. Notable among these approaches is the use of biometric facial recognition which has proven to be ideal, due to its flexible and non-intrusive nature. Mainly, this research conducted a systematic review on algorithms and approaches for facial recognition to aid security operatives in crime investigations. For the first time, the review coined and described three operational environments namely, regulated, unregulated and semi-regulated to which facial recognition is applicable. However, semi-regulated environment is yet to be addressed based on its peculiar characteristics. Subsequently, this study proposed the design of a facial recognition system premised on deep learning and local binary patterns histograms algorithm (LBPH). Certainly, future implementation of the design will help to identify and document known and unknown individuals, thus creating a more efficient and effective approach for crime control.

Keywords: *Face, crime, facial recognition, facial recognition algorithms, crime investigation*

1. Introduction

Obviously, criminalities in human societies predated human civilisation and have continued to plague societies since time immemorial. Over the years, several approaches have been adopted to handle cases relating to crimes. Some of these approaches have gone from the use of traditional techniques such as reliance on eye witness reports to more sophisticated techniques like checking for deoxyribonucleic acid (DNA) residues at crime scenes.

The tremendous breakthroughs recorded by technology over the years have led to its adoption and use by law enforcements to solve crime challenges. Law enforcement and forensic officers have employed technological means to investigate crimes, especially, the use of biometric identification. In its simplest form, biometric technology basically analyses and measures distinct biological traits in living organisms (Malathi & Raj, 2016). In line with this, biometric identification is therefore based on the principle that every individual can be identified by a set of recognizable and identifiable biometric data, which are unique and specific to individuals.

Specifically, biometric authentication systems can be categorised into two forms namely, behavioural and physiological systems. The physiological biometric systems use the physical characteristics of humans to distinguish between individuals. In these systems, physical characteristics such as faces, fingerprints, and iris are mostly used. These measurable physical features possess characteristics such as permanence, collectability, universality and distinctiveness, which are the requirements of biometric characteristics (Tiwari, Tiwari, & Tiwari, 2015). The behavioural biometric systems on the other hand, refer to user behaviour such as typing, gait or voice. However, human behaviour is likely to change over time for several reasons such as age, weather condition or mood. This in certain cases, may lead to lower performance in real world applications, although it can be controlled by regularly updating the stored template of the behavioural characteristic to ensure that the stored template corresponds to the current behaviour (Olszewska, 2016; Tiwari et al., 2015).

Further technological advancements, especially in the area of biometric systems have provided an invaluable tool, which is referred to as facial recognition to support the never-ending fight against crime. Furthermore, facial recognition in currently being employed in numerous organisations including, airport security systems and by Federal Bureau of Intelligence (FBI) to aid crime investigations in tracking drug peddlers, find missing individuals and monitoring suspects (Silk, 2017). Somewhat, human face is a unique biometric feature that varies considerably in appearance from one person to another. Thus, in computer vision, facial recognition is considered to be an interesting and necessity, but tough research area. In this research area, speed and accuracy of identification are serious challenges (Chevelwalla, Gurav, Desai, & Sadhukhan, 2015). Hence, various approaches have been developed over the years to efficiently handle facial recognition and subsequently use it to handle the problems relating to various crimes.

Primarily, this study conducts a systematic review on existing literatures on the use of facial recognition algorithms and approaches for criminal detection. Afterward, we proposed the application of deep learning algorithm for face detection and local binary patterns histograms (LBPH) algorithm for facial recognition in order to create an approach that adequately monitors the movement of criminals in semi-regulated environment. The remainder of this article is organised as follows: Section 2 presents background of some fundamental concepts and terminologies in facial recognition, Section 3 reviews some related literatures, Section 4 analyses the existing facial recognition systems, Section 5 discusses the methodology of the proposed system and Section 6 concludes the article.

2. Background of Facial Recognition Concepts

Over the years, various concepts have been adopted to basically control crime using technology. Thus, this section presents a review on concepts relating to computer vision, face detection and facial recognition. These concepts provide the necessary pivotal to understand the use of facial recognition for crime control. For example, Piza, Welsh, Farrington, and Thomas (2019) carried out analysis on the effects of closed-circuit television (CCTV) cameras for crime prevention. The analysis showed the benefits of leveraging CCTV camera feed for crime prevention and investigations. However, the use of just CCTV cameras poses challenges such as large memory consumption, lack of flexibility and automation. Furthermore, the use of CCTV alone, does not provide avenue for generating crime notifications via short messaging service (SMS) or electronic mail (email) (Ran, Lavanya, & Poojitha, 2018).

2.1 Computer Vision

Generally, computer vision is aimed at reconstructing and interpreting natural images based on the content captured by cameras (Peters, 2017). It focuses mainly, on the science with which computers can see. The hardware employed in computer vision systems includes some forms of programmed digital camera for approximate visual perception. In view of this, extensive researches have been done to enable computer extract only useful information from images. Such computer vision systems consist of two fundamental units, which include acquisition of image and processing of the image.

2.2.1 Image Acquisition

Image acquisition involves retrieving digital image from sources like digital camera and scanner. This represents the first unit in a computer vision system and encompasses all the necessary steps for transforming electronic signal supplied by image acquisition sources or devices to digital formats (Zareiforoush, Minaei, Alizadeh, & Banakar, 2015). The image acquisition precedes image processing phase and factor like illumination is important to guarantee the acquisition of good quality images. More image acquisition or capturing devices include X-ray, ultrasound machines, photo cameras, near spectroscopes etc.

2.2.2 Image Processing

Image processing involves some set of activities that are performed to improve the quality of acquired images. These activities help to improve the quality of images and eliminate defects like repetitive noise, geometric complexity, ununiform illumination, inappropriate focus and camera motion (Zareiforoush *et al.*, 2015). Generally, this unit is subdivided into three processing levels including high-level, low-level and intermediate-level. The low-level processing covers processing of images, noise elimination, gray-level adjustment amongst others. Also, the intermediate-level processing entails segmentation, representation and description of image. Again, the high-level processing involves recognition of particular region of interest and interpretation of such region, which is normally achieved through multilayer neural networks or some statistical classifiers (Zareiforoush *et al.*, 2015).

2.2 Facial Recognition

In computing, facial recognition refers to a set of activities using pattern recognition, which is explicitly and mostly conducted on human faces (Sukhija, Behal, & Singh, 2016). Indeed, facial recognition involves algorithms through which computers recognise faces by comparing images or video feed against some stored facial templates. Facial recognition sequentially follows image processing and it allows relevant images to be stored in database. Consequently, for recognition to take place, a recognition algorithm is trained and ideal confidence values are chosen as thresholds. For face similarity to occur, that is, for a face to be recognised, it has to be compared against the existing faces that are stored in the database. Perhaps, the confidence value that results from the comparison is lower or higher than the similarity threshold, then the face is recognised and given the appropriate label. In the minimum, facial recognition systems usually encompass three modules namely, face acquisition, facial recognition, feature extraction and storage.

2.2.1 Face Acquisition Module

In this module, the images captured from sources like cameras are first detected and the detection process distinguishes the part of a video or image stream that constitutes a face. After detection, the face images are converted to grayscale and resized to eliminate problem relating to “pose” (Diwate & Ingole, 2016). Again, pre-processing is carried out to remove noise from the image, while other processes are carried out to handle illumination and brightness issues. Some of the popular traditional algorithms for detection of faces and face features include Haar-cascades, linear binary patterns and sift points (Olszewska, 2016). Recently, deep learning approaches are being increasingly employed for more accurate and efficient face detection, these approaches are based on convolutional neural networks and they have been used, not to only develop efficient facial recognition systems for desktops, but for mobile devices as well (Li, 2016).

2.2.2 Feature Extraction Module

Primarily, feature extraction module involves extracting relevant parts of the detected face. Often, the extraction process goes hand in hand with the face detection process. However, the features to be extracted depend on the algorithm being employed. Thus, common feature extraction algorithms includes neural-network-based eye feature detector, Log Gabor wavelet network, hierarchical 2-level wavelet network, Adaboost and elastic bunch graph matching (Naik *et al.*, 2019).

2.2.3 Facial Recognition Module

The recognition module is meant to compare faces from video or picture feed with already stored facial images in order to determine similarity between the images. Though, various algorithms exist for handling facial recognition, but only traditional, deep learning and hybrid approaches are well documented. Firstly, the traditional procedures depend on hand-crafted characteristics, like descriptors for texture and edges are normally combined with machine learning techniques, support vector machines and other analysis-based approaches. Examples of some widely used analysis-based approaches are linear discriminant analysis and principal component analysis. Secondly, deep learning methods that were designed in line with convolutional neural networks (CNNs), are also gaining popularity for facial recognition (Daniel, Al, & Hartnett, 2018). Thirdly, hybrid approaches combined techniques from two or more algorithms for optimal facial recognition. The major advantage of any hybrid approach is the ability to combine the strengths of two or more algorithms and minimise the weaknesses that each may possess (Daniel *et al.*, 2018). Really, choosing any these three approaches is dependent on the underlying purpose of the facial recognition system and the types of available face dataset.

3. Review of Related Literatures

Over the years, quite a number of algorithms have been developed to handle facial recognition and each demonstrated couple of advantages and disadvantages. Mostly, these algorithms involve basic tasks comprising of detecting faces from images or video streams, saving, cropping and extracting features from images. These tasks are essential, in order to train the model generated by facial recognition algorithm and then recognise trained faces. Similarly, some of these approaches that are explained in sections 3.1 and 3.2, have been implemented in facial recognition systems. Operationally, each system leveraged on one of more algorithms to apply the concept of facial recognition to criminal investigation and crime prevention. Hence, this systematic review is logically divided into two areas as follow:

1. Review of literatures relating to algorithms for facial recognition.
2. Review of existing facial recognition systems for criminal detection in different environments.

3.1 Review of Algorithms for Facial Recognition

Karamizadeh *et al.*, (2013) proposed the use of principal component analysis (PCA) as a traditional method for facial recognition. Notably, the authors considered the benefits of PCA algorithm, which include increase in efficiency, decrease in memory capacity and low sensitivity for noise. PCA was implemented to extract the crucial characteristics of face image and then represent each image in the training dataset as a linear aggregate of weighted Eigenvectors, that is also known as Eigenfaces. Furthermore, the recognition phase was developed by projecting face image into space that is formed by Eigenfaces. Thereafter, comparison between faces was based on Euclidian distance of Eigenvectors, which is controlled by Eigenface and Eigenvector from which the image being recognised was derived. Thus, the face in an image is appropriately recognised, when the Euclidean distance is quite small (Karamizadeh *et al.*, 2013). On the one hand, light has significant impact on the recognition accuracy of

PCA. On the other hand, pose and facial expression have small effects on the success rate of the recognition algorithm (Saini, Saini, & Agarwal, 2014).

In their research, Daniel *et al.*, (2018) proved that Fisherfaces (linear discriminant analysis) algorithm solved the issues identified with PCA approaches, whereby the top eigenvectors may have a negative impact on the recognition accuracy. This is due to the fact that eigenvectors might correspond to intra-personal variations that are not relevant for face recognition task. The Fisherfaces algorithm ensures maximum and minimum variances *between* (across the users) and *within* (with the users) classes respectively. Mathematically, the *between class* and *within class* are expressed in Equations (1) and (2) accordingly.

$$S_w = \sum_{j=1}^{c} \sum_{i=1}^{n} (X_t^j - \mu_j)(X_t^j - \mu_j)^T \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Where X_t^j, is the i^{th} sample of class j, μ_j is mean of class j, c is number of classes, and n is number of samples in class j. while the between class scatter matrix is given by:

$$S_b = \sum_{j=1}^{c} (\mu_j - \mu)(\mu_j - \mu)^T \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

Where μ represents the mean of all classes, with the goal being to maximise the between class measure and minimise the within class measure.

Interestingly, another algorithm known as Local Binary Patterns Histograms (LBPH) combines Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG) to create a simple but effective method of representing images, while using an easy to understand vector (Deeba & Ahmed, 2019). Foremost, to detect faces in images, the images have to be converted to grayscale. That is, for each pixel $P_{i,j}$, a vector equivalent is derived containing the values for colours red, green and blue. Subsequently, Equation (3) is used to convert the face image to grayscale.

$$G_{i,j} = (0.2989, 0.5870, 0.1140)^T . P_{i,j} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

Where $G_{i,j}$ represents the corresponding pixel in the generated y-scale image. The LBPH algorithm is based on the local-binary-operator. This operator is utilised for local binary characteristics by taking into consideration the LPB that could reduce the local and special characteristics of an image (Deeba & Ahmed, 2019). Thus, the binary ratio of intensities of the pixel at the centre and the pixels in its neighbourhood is called LBP. Equation (4) represents the mathematical description of LBP.

$$LPB(P_c - q_c) = \sum_{m=0}^{7} s(t_m - t_c)^{2^t} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

Where the centre pixel shown by t_c and (pc, qc) represents the surrounded eight pixels. This proves very useful in determining the face features in the face matrix features extracted from the images. Also, it is against this face features that the values of the centre pixel are compared to generate a binary code. Likewise, LBPH algorithm proved to be advantageous over Fisherfaces and eigenfaces in terms of dealing with images having poor lighting (Zarei, 2018) and possessing improved facial recognition with little resolution (Ahmed, Guo, Ali, Deeba, & Ahmed, 2018).

Similarly, Halvi, Ramapur, Raja, and Prasad (2017) proposed a fusion-based facial recognition system using one dimensional transform domains. The researchers proposed a method by which two-dimensional face images are converted into one dimension (1D). One dimensional Discrete Wavelength Transform (DWT) and Fast Fourier Transform (FFT) are utilised to extract features of face images. Subsequently, these characteristics are then compared between the already stored and test images through Euclidian Distance (ED). Better results are obtained by using some performance parameters derived from

ED. As a matter of fact, a detailed analysis revealed that the proposed method has highest success rate, but lowest equal error rates when compared with existing facial recognition methods, thus indicating a better performance. However, the researchers observed that future research would require implementing the algorithm on relevant hardware for real time applications. This is an important observation, because certain limitations can only be detected when a software is fully deployed on to hardware.

Also, Zafar *et al.*, (2019) proposed a facial recognition system using Bayesian convolutional neural networks for resilient surveillance systems. The researchers worked extensively to enhance the efficiency of facial recognition systems by minimizing false positive. The researchers noted that the effectiveness of a facial recognition method relied primarily on its ability to work with images having low quality and its efficacy to extract relevant features. To this end, the capability of Deep Convolution Neural Networks (DCNNs) to extract important features from unprocessed images makes it a desirable facial recognition algorithm.

Accordingly, the results obtained by Zafar *et al.*, (2019) showed that deep learning (DL)-based approaches are quite suitable, because feature extraction and representation are performed without much intervention using back-propagation method on supplied data. Also, the researchers also proved that although deep convolutional neural network (DCNN)-based techniques showed outstanding outcome in facial recognition by discovering intricate features in large datasets, they observed an uncertainty in the prediction of the output class. Particularly, the uncertainty can be mitigated by employing Bayesian convolutional neural networks, thereby becoming a valuable approach for reducing false positives. Nonetheless, the researchers noted that DL-based approaches may not perform well under unstrained environments owing to the fact that the method involves human intervention in the selection and representation phases, which might not be ideal for all scenarios.

In addition, Sukhija, Behal and Singh (2016) proposed the use of genetic algorithm (GA) to handle facial recognition. The algorithm employed the idea of genomes or chromosomes to evolve a recognition procedure for face images. The proposed GA is based on Darwin theory of evolution, which is characterised by a search mechanism and selection technique for chromosomes (individuals) that have better adaptation and good chances of survival. These strong individuals survive and have their traits passed to the next generation. This concept, on which genetic algorithm is based ensures increased speed in cases of large search spaces whereby conventional algorithms become inefficient. Interestingly, GA produces better result, because it produces collection of solutions, rather than one.

Furthermore, the proposed GA algorithm was compared against other known facial recognition algorithms like Linear Discriminate Analysis (LDA) and PCA algorithms. The comparison was conducted using face images drawn from already benchmarked datasets that were retrieved from University of Manchester Institute of Science and Technology (UMIST), Olivetti Research Laboratory (ORL) and Indbase. The results as shown in Figure1, revealed that the recognition rate for GA was better than that of LDA and PCA. Also, due to optimality principle of GA, which is not available in LDA and PCA, it was able to reduce the training images of the three datasets.

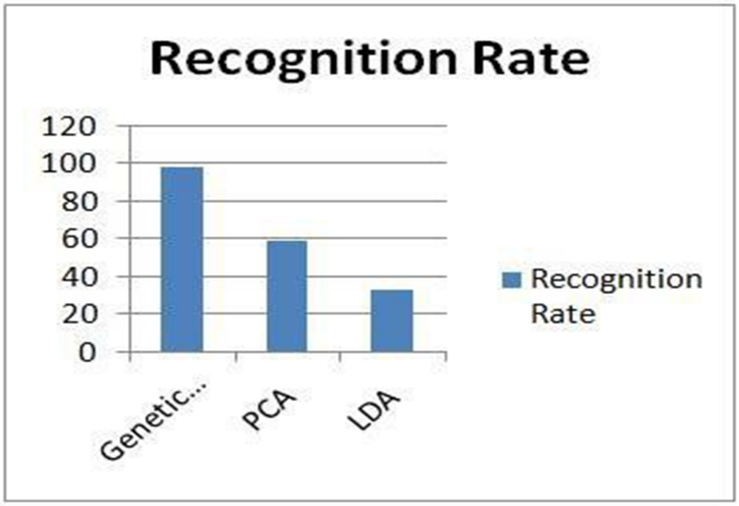

Figure 1: comparison of GA against PCA and LDA (Source: Sukhija, 2016)

3.2 Review of Facial Recognition Systems for Criminal Detection

Abdullah *et al.*, (2017) developed a system to assist law enforcement officers in identifying criminals in public places, especially in situations where criminals did not leave fingerprints at the crime scene. The researchers used PCA to accomplish facial recognition and Haar-cascades for face detection. The researchers took advantage of existing CCTV mounted across Malaysia to create a system, whereby video feeds across these cameras are compared against face records of known criminals. Figure 2 presents system architecture of the proposed system, which after implementation recorded 80% accuracy. However, their system, which was developed for unregulated environments relied on the existence of well populated face records of criminal, unfortunately this fails to factor in first time offenders.

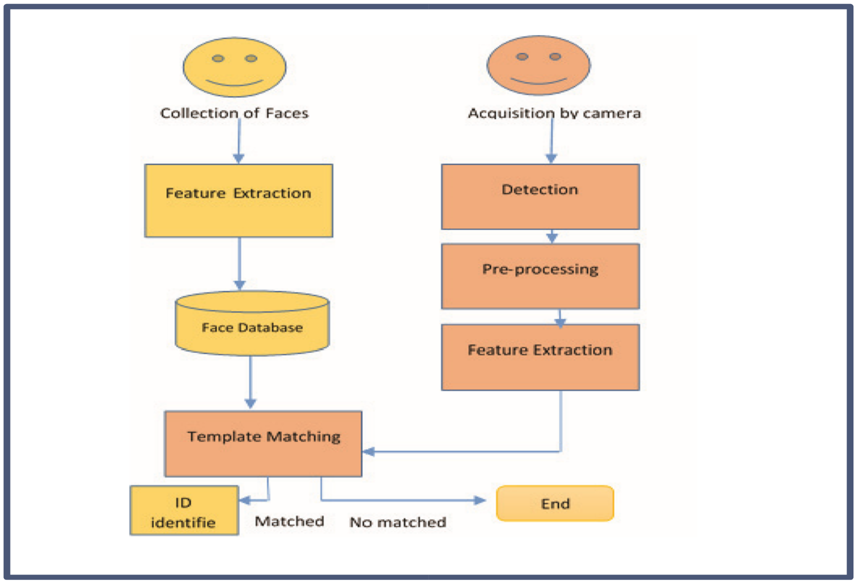

Figure 2: System Architecture of FRCI. (Source: Abdullah *et al*., 2017)

Also, Kumar *et al.*, (2018) designed a suspect identification system using facial recognition in public environments. The suspect identification system used LBPH algorithm for facial recognition and Haar-cascades classifier for face detection. The system allowed tracking of criminals, suspect and general individuals by simply providing pictures of the individuals against which comparison is made with feed from strategically positioned cameras. The system architecture and the performance evaluation result (false acceptance rate and false rejection rate) are shown in Figure 4 and Figure 5 respectively. Nevertheless, due to the system's on input pictures against, which comparison is made, the system was limited in dealing with undocumented criminals.

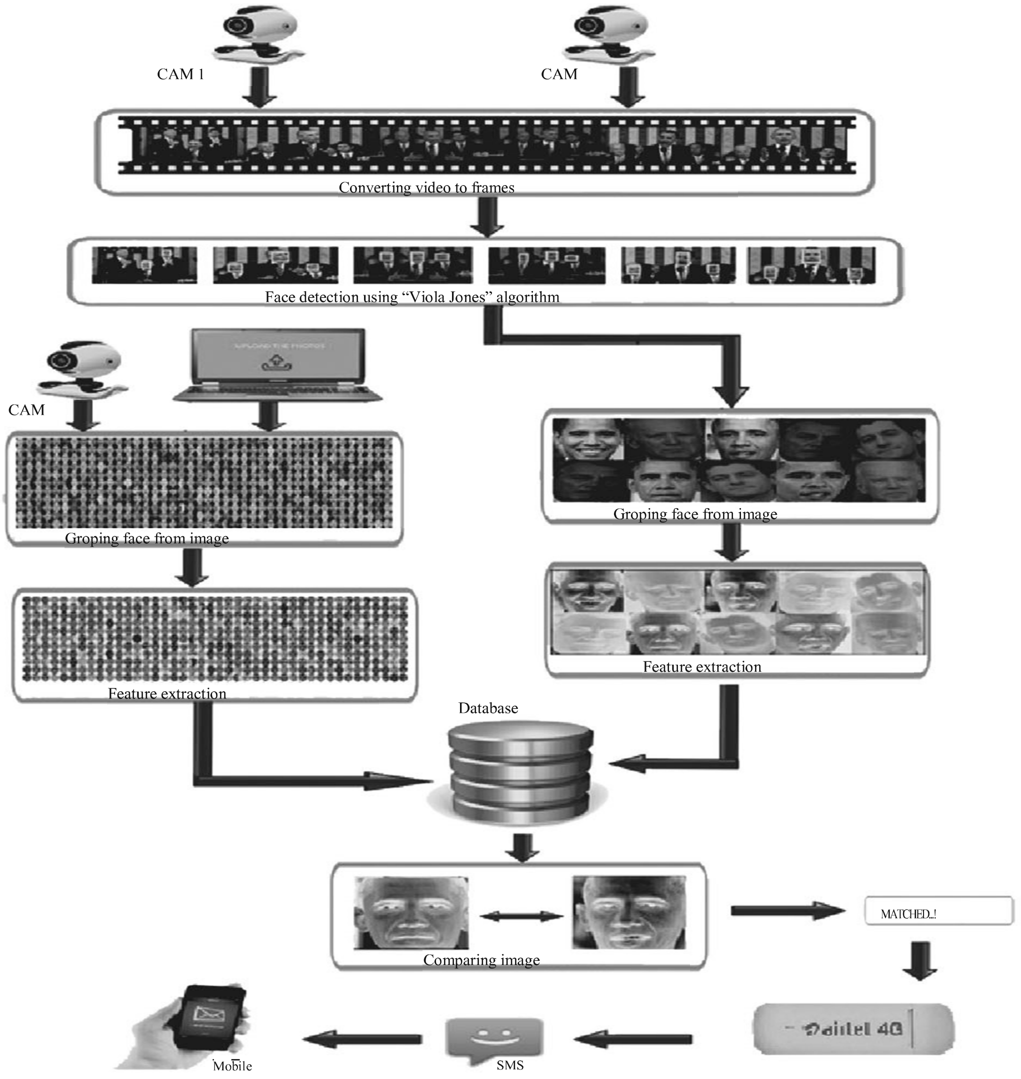

Figure 3: system Architecture of suspect identification system (source: Kumar *et al.*, 2018)

Online: ISSN 2645-2960; Print ISSN: 2141-3959

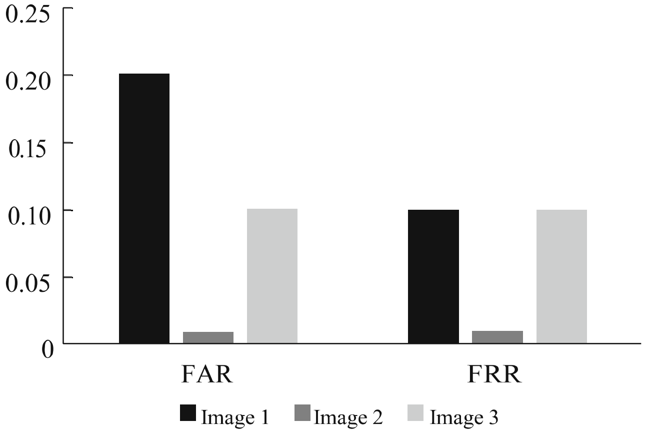

Figure 4: Test Results (source: Kumar *et al.*, 2018)

Similarly, Kakkar and Sharma (2018) implemented a criminal identification system using Haar-cascade classifiers. The algorithm adopted by the researchers looked for specific Haar features in an image. The classifiers allow a *face candidate*, which is a rectangular part of the original copy of the image to move to the next step of the recognition algorithm when Haar features are found. Mostly, the size of the sub window is set to 24 x 24 pixels and the window is usually scaled so as to get varieties of different face sizes. Thereafter, the algorithm will use the window to scan the whole face image and each section within the image represents a face candidate. Next, faces of known criminals are saved in a database and compared against still images or video streams in order to detect if an individual is a criminal or not. However, the system failed to cater for cases of undocumented criminals or first-time offenders.

In addition, Nguyen, Sheng and Lakshamanan (2019) designed and developed a smart security system with facial recognition using neural networks in restricted (regulated) environment. The researchers aimed at controlling access into homes by employing facial recognition methodology. Significantly, the study improved the classifier model via social media and human interaction. This improvement was achieved using a deep learning framework called TensorFlow. As illustrated in Figure 5, the system architecture employed cloud server for the facial recognition activities.

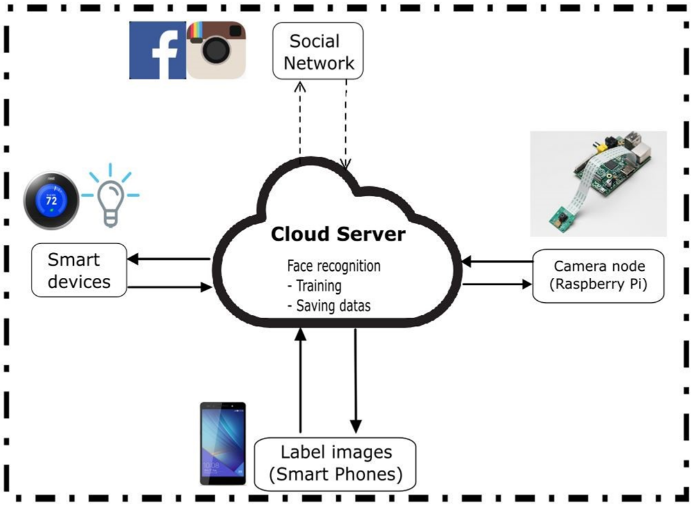

Figure 5: Smart security system using facial recognition (source: Nguyen *et al.*, 2019)

Specifically, cloud server was utilised to atone for the computational expense that comes with training the neural network. The cloud server node receives data from the camera nodes, stores and then trains the data after data acquisition. The cloud server also has a web-based server collecting data from Facebook and saving all data to storage. The authors included a module to allow the home owner to control the smart devices and change permission level for different users using a smart phone. Based on this granted access level, different users will able to control different smart devices. Whenever a new person is detected, the cloud server sends an alert to the smartphone. The owner can then label the person or take necessary actions in case of any security breach. The researchers trained the proposed model using Visual Geometry Group (VVG) dataset and Labelled Faces in the Wild (LFW) datasets. Afterward, the result of their system was compared with other algorithms as detailed in Table 1. Nonetheless, the use of cloud server may serve as a limitation in locations where internet service is lacking.

Table 1: Performance evaluation (source : Nguyen *et al.*, 2019)

Models	**Accuracy**
SOF model	0.9318 ± 0.0140
Facenet paper	0.9963 ± 0.009
Eigenface	0.6002 ± 0.0079
Human, cropped	0.995

4. Analysis of Existing System

Altogether, several systems have been proposed and developed over the years to unravel the faces of criminals through facial recognition methodologies. Generically, analysis of the existing systems revealed that most of them comprised of one or more CCTV cameras and a database against which face comparison is performed. Hence, the existing systems have similar workflow that can be summarised as follows:

i. Receive images of criminals from various sources.
ii. Detect faces and extract feature from criminal images using face detection algorithms.
iii. Store faces in a database with a label.
iv. Train the model of facial recognition algorithm and chose appropriate confidence value.
v. Receive video feed from strategically positioned CCTV cameras and compare faces in feed for a possible match against criminal database.
vi. Notify appropriate authorities through messaging systems like SMS or email.

Individually, each of the proposed systems explored and adopted one or more algorithms to implement each step in the workflow and their approaches centred on different environment of interests. For instance, the systems developed by Abdullah *et al.*, (2017), Kakkar and Sharma (2018) and Kumar *et al.*, (2018) focused on facial recognition in public places, while, the system developed by Nguyen, Sheng and Lakshamanan (2019) served as authentication mechanism for registered individuals in a private environment.

Likewise, this analysis further exposed the need for research efforts to define and discriminate the environments into which each of the facial recognition system was meant to operate. More importantly, the development of a system that will operate in semi-regulated environment (an environment that is neither public nor exclusively private) will be desirable. Indeed, such system will be able to serve dual purposes of identifying known and unknown faces for authentication and criminal detection respectively.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

5. Proposed Design and Methodology

Remarkedly, the outcome of literature review and subsequent analysis of existing systems on face detection and recognition necessitated the need to classify the operational environments of criminal recognition systems. Again, the two preceding sections justified the need for system that could aid in recognising criminals in different operational environments.

5.1 Classification of Operational Environment

As emphasised in the preceding section, knowing the environment and the purpose for deploying facial recognition system is of paramount importance. Therefore, this study discriminates operational environments into three broad categories namely; ***regulated***, ***unregulated*** and ***semi-regulated*** environments. The classification of these domains of application of the systems is dependent on the availability of prior data about people entering and exiting the environments.

i. **Regulated environment** refers to an environment in which all the individuals entering and exiting a facility are registered or known to the system and access is granted to only these registered individuals. In this case, facial recognition systems are majorly used for access control, rather than detecting criminal within security facility. Hence, such systems restrict access to vital assets and provide facial evidence of criminal when security breaches occurred.

ii. **Unregulated environment** refers to public places like stadia, train stations, shopping malls, academic institutions, public functions etc, whereby none or vast majority of those entering and exiting the environment are unknown to the system. That is, data about these entities, including their facial images are not preloaded into the database to detect already tagged criminal.

iii. **Semi-regulated environment** on the other hand refers to environments whereby some of the people entering and exiting are known while others are unknown. Example of these environments are banking halls, customer experience or service centres etc. Thus, the database to support facial recognition system in such environments will be partially filled with facial data of both regular users and known criminals. One major requirement for any criminal detection and recognition system in semi-regulated environment, is the additional module that will populate the database with new faces and tag the new faces appropriately. Essentially, the module will aid recognition of first-time offenders and assist law enforcement agents in tracking and investigating the movement of individuals, suspects or confirmed criminals.

5.2 Proposed Facial Recognition System for Semi-Regulated Environment

The proposed system will be deployed in semi-regulated environments in order to create a system that will detect the presence of known criminals, unknown individuals and known individuals. Particularly, it will ensure proper documentation of criminals for investigative purposes. The implementation of the system comprises of computer that receives and process video feeds from strategically positioned and networked CCTV cameras. Likewise, the database of known criminal and suspected criminals will be maintained and automatically updated to meet the dynamic nature of facial repository for semi-regulated environment. Above all, an unusual combination of deep learning and LBPH algorithms would be used in the system for optimal performance.

More so, the system would send appropriate message to notify security operatives once a known criminal is detected within an environment. Therefore, Figure 6 represents high-level design of the system using the flowchart, whereas, Figure 7 presents a detailed block diagram of same system. In addition, the

Online: ISSN 2645-2960; Print ISSN: 2141-3959

system would provide interfaces for users to monitor criminals, configure necessary thresholds, maintain all algorithms, manage face repository, generate appropriate security reports etc.

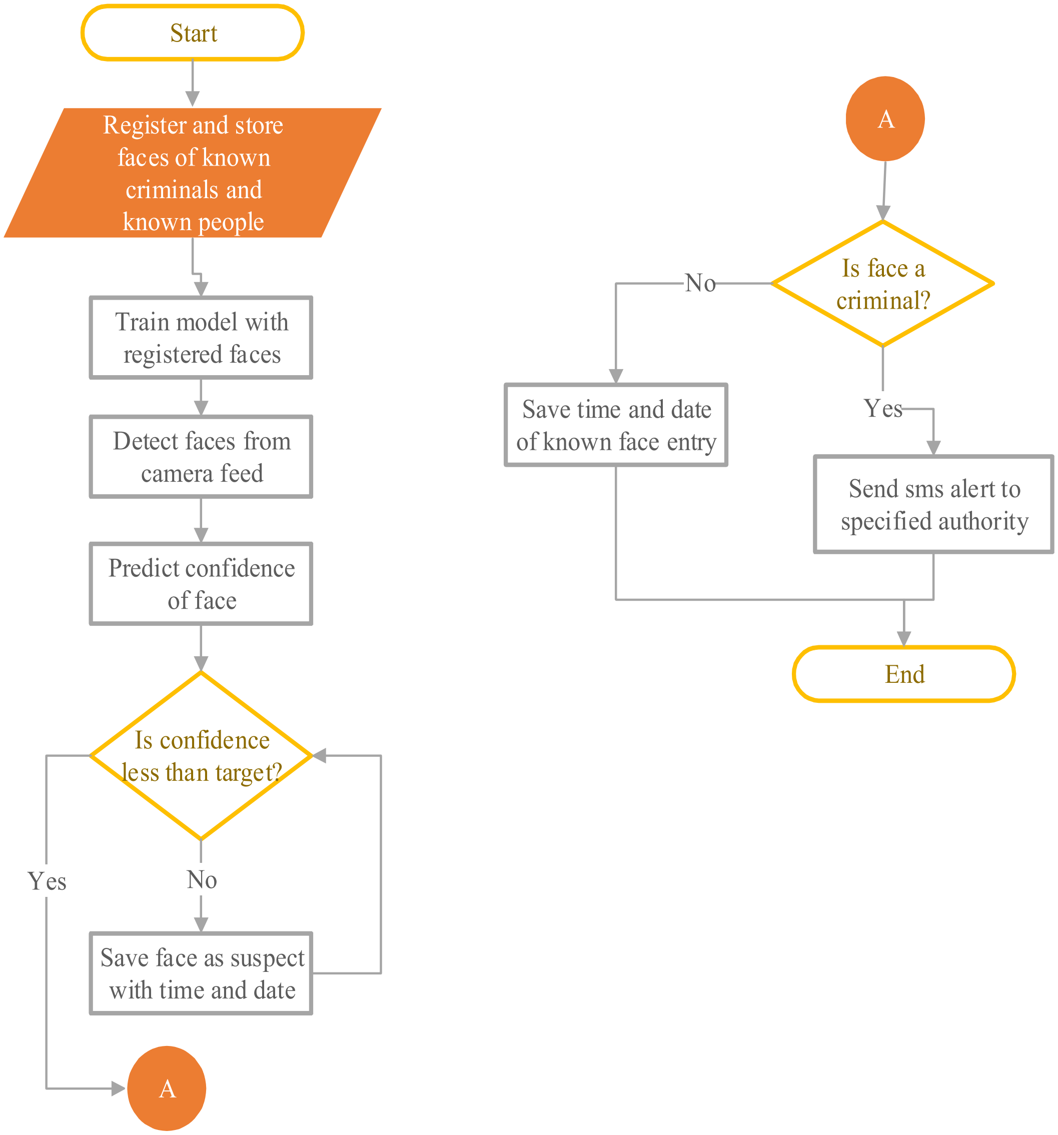
Start
Register and store faces of known criminals and known people
Train model with registered faces
Detect faces from camera feed
Predict confidence of face
Is confidence less than target?
Yes
No
Save face as suspect with time and date
A
A
Is face a criminal?
No
Yes
Save time and date of known face entry
Send sms alert to specified authority
End

Figure 6: Flowchart of proposed facial recognition system for semi-regulated environment

Online: ISSN 2645-2960; Print ISSN: 2141-3959

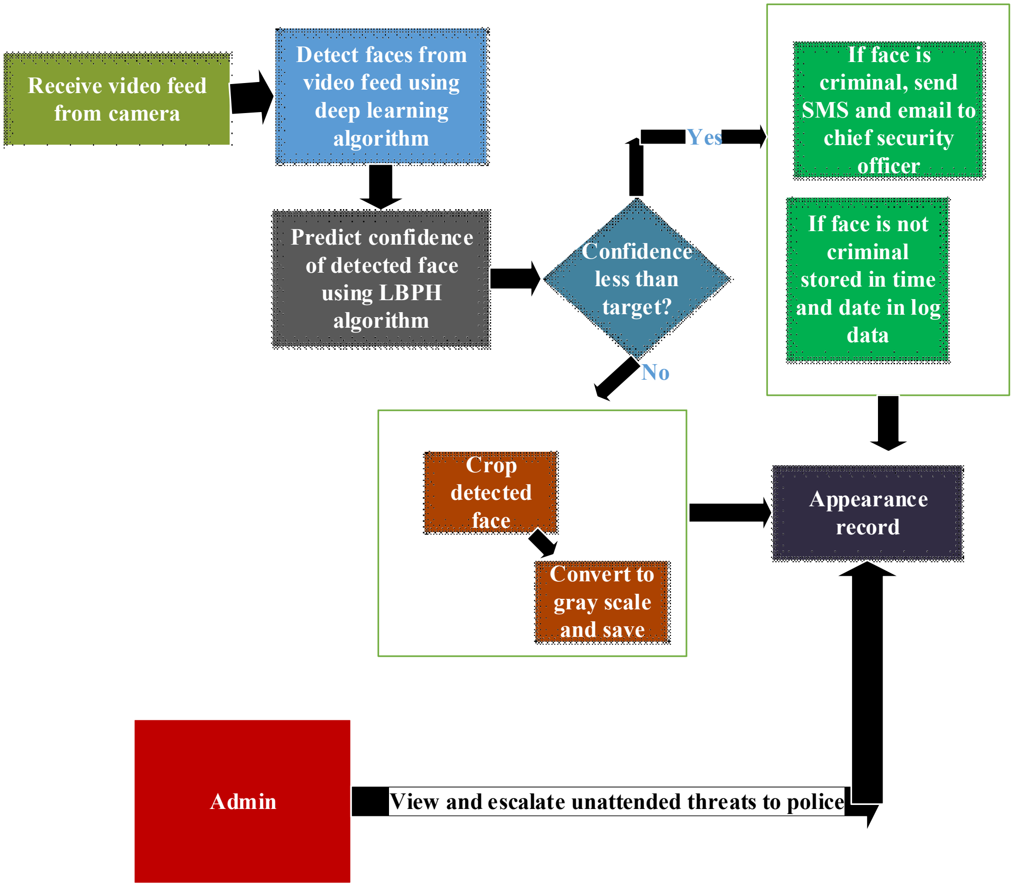
Receive video feed from camera
Detect faces from video feed using deep learning algorithm
Predict confidence of detected face using LBPH algorithm
Confidence less than target?
Yes
No
If face is criminal, send SMS and email to chief security officer
If face is not criminal stored in time and date in log data
Crop detected face
Convert to gray scale and save
Appearance record
Admin
View and escalate unattended threats to police

Figure 7: Block diagram of proposed facial recognition system for semi-regulated environment

6. Conclusion and Future Works

Certainly, insecurity is a grave concern to everybody, as it continues to plague our societies and constantly requires innovative ways to unravel the mysteries behind some topical crimes. Thus, several approaches have been proposed and implemented to address some criminal acts using facial recognition algorithms and systems. These previous studies adopted one or more face algorithms and approaches. Interestingly and for the first time we categorised the operational environments of existing studies into regulated, unregulated and semi-regulated after careful systematic analysis. Primarily, the categorisation allowed for description of each environment for proper understanding and documentation to aid the design and development of facial recognition systems for respective environment.

Furthermore, the possibility of combining traditional and deep learning algorithms for facial detection and recognition in semi-regulated environment was explored to support crime investigations. Thus, this research enunciated the fundamental components for advanced use of facial recognition systems to alert security agencies about presence of criminals and suspects in semi-regulated environment. Therefore, future research efforts in this direction will be directed to implementing and evaluating the performance of the proposed facial recognition system, which was designed for criminal recognition in semi-regulated environment.

Reference

Abdullah, N. A., Tun, U., Onn, H., Chuah, C. W., Tun, U., Onn, H., … Onn, H. (2017). Face recognition for criminal identification : An implementation of principal component analysis for face recognition Face recognition for criminal identification. *https://doi.org/10.1063/1.5005335*

Ahmed, A., Guo, J., Ali, F., Deeba, F., & Ahmed, A. (2018). LBPH based improved face recognition at low resolution. *2018 International Conference on Artificial Intelligence and Big Data, ICAIBD 2018*, 144–147. https://doi.org/10.1109/ICAIBD.2018.839618

Chevelwalla, A., Gurav, A., Desai, S., & Sadhukhan, P. S. (2015). Criminal face recognition system. *International Journal of Engineering Research & Technology (IJERT) 4(03)*, 47–50.

Daniel, S., Al, H., & Hartnett, M. (2018). Face recognition : From traditional to deep learning methods. *arXiv:1811.00116v1*.

Deeba, F., & Ahmed, A. (2019). LBPH-based enhanced real-time face recognition. *International Journal of Advanced Computer Science and Applications*. *10*(5), 274–280.

Diwate, R. B., & Ingole, S. G. (2016). Different face recognition techniques : A survey. *International Journal for Research in Technological Studies*, 2(5). 2348-1439.

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

Kakkar, P., & Sharma, V. (2018). Criminal identification system using face detection and recognition. *International Journal of Advanced Research in Computer and Communication Engineering*, *7(3)*. 238–243. https://doi.org/10.17148/IJARCCE.2018.7346

Karamizadeh, S., Abdullah, S. M., Manaf, A. A., Zamani, M., & Hooman, A. (2013). An overview of principal component analysis. *Journal of Signal and Information Processing*, *04*(03), 173–175. https://doi.org/10.4236/jsip.2013.43b031

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*. *28(3)*, 410–420. https://doi.org/10.1134/S1054661818030136

Li, H., & Zhu, X. (2016). Face recognition technology research and implementation based on mobile phone system. *12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*. (pp. 972–976). IEEE.

Malathi, R., & Raj, J. R. (2016). An integrated approach of physical biometric authentication system. *Procedia - Procedia Computer Science*, *85*(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. *International Journal of Advance Research, Ideas and Innovations in Technology*. *5*(3). 1936-1940.

Nguyen, T., Sheng, W., & Lakshamanan, B. (2019). A smart security system with face recognition. *arXiv:1812.09127*.

Olszewska, J. I. (2016). Automated face recognition: challenges and solutions. *IntechOpen*. 59-79. http://dx.doi.org/10.5772/66013

Peters, J. F. (2017). *Foundations of computer vision: Computational geometry, visual image structures and object shape detection, Springer, Cham*. https://doi.org/10.1007/978-3-319-52483-2

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology and Public Policy*, *18*(1), 135–159. https://doi.org/10.1111/1745-9133.12419

Ran, R., Lavanya, S., & Poojitha, B. (2018). IoT based home security system using raspberry Pi with email and voice alert. *International Journal of Advanced Research in Computer Science and Software Engineering, 8(4)*, pp. 119-123.

Saini, R., Saini, A., & Agarwal, D. (2014). Analysis of different face recognition algorithms. *International Journal of Engineering Research & Technology (IJERT). 3(11)*, 1263–1267.

Sukhija, P., Behal, S., & Singh, P. (2016). Face recognition system using genetic algorithm. *Procedia - Procedia Computer Science*, *85*(Cms), 410–417. https://doi.org/10.1016/j.procs.2016.05.183

Tiwari, T., Tiwari, T., & Tiwari, S. (2015). Biometrics based user authentication. *American Journal of Engineering Research (AJER), 4(10)*, 148–159.

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*. 1-10. https://doi.org/10.1186/s13640-019-0406-y.

Zarei, S. (2018). *Face recognition methods analysis*. *1*(1), 1–12.

Zareiforoush, H., Minaei, S., Alizadeh, M. R., & Banakar, A. (2015). Potential applications of computer vision in quality inspection of rice: A review. *Food Engineering Reviews*, *7*(3), 321–345. https://doi.org/10.1007/s12393-014-9101-z