



Facial Recognition for Criminal Identification using Convolutional Neural Network

V. Sathya Preiya¹, R. Vijay^{2*}, A. Hemlathadhevi³, C. Bharathi Sri⁴

¹Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, 600123, India

²Department of Computer Science, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, 600062, India

³Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, 600123, India

⁴Department of Computer Science, Velammal Engineering College, Chennai, 600066, India

Emails: sathyapreiya@yahoo.com; drvijayr@veltech.edu.in; hemlathadhevi@gmail.com; bharathisri89@gmail.com

Abstract

The process of identifying and recognising the criminal is the time consuming and difficult task. There are several ways to identify culprits at the crime site, including fingerprinting, DNA matching, and eyewitness testimony. The criminal face identification system will be built on a existing criminal database. The method for identifying a human face using features extrapolated from an image is presented in this study. The technique for identifying a human face using characteristics extrapolated from a picture is presented in this research. It is quite difficult to develop a computer model for recognizing the human face since it is a complicated multidimensional visual representation. The video captured by the camera will be translated into frames as part of the suggested process. To increase detection accuracy, this suggested a Binary Gradient Alignment (BGA) algorithm a description texture classification technique. When a facial feature is detected in an image frame, it undergoes pre-processing to eliminate unnecessary data and reduce unwanted distortions. The real-time processed image is compared to the trained images that have previously been saved in the database. The technology will send an automatic email notice to the police officials if the surveillance camera detects a criminal.

Keywords: Binary Gradient Alignment (BGA); Face recognition; Concurrent Convolutional Neural Network (CCNN); Image Processing; Amalgam Denoising Algorithm.

1. Introduction

In recent years, law enforcement agencies have faced escalating challenges in apprehending thieves, with traditional methods heavily reliant on evidence found at crime scenes proving increasingly inadequate. The evolution of criminals' tactics, coupled with their adeptness at eluding detection, has made the search for tangible evidence a daunting task. However, advancements in biometric technology, particularly in facial recognition, have emerged as a promising solution. Take, for instance, a recent scenario in a bustling city where a series of high-profile thefts have baffled investigators. Despite the absence of substantial physical evidence, surveillance footage captured clear images of the perpetrator's face.

Modern law enforcement relies heavily on cutting-edge biometric identification tools, which have transformed the process of suspect identification and arrest. By leveraging sophisticated pattern-matching algorithms, these systems scrutinize facial characteristics extracted from visual data and cross-reference them with extensive repositories of known individuals, enabling swift and accurate suspect verification. This technology offers several critical advantages in criminal detection. Firstly, it provides an automated

and rapid means of identifying suspects, significantly expediting the investigative process. Traditional methods reliant on eyewitness accounts or manual searches through vast databases are will take large amount of time and cannot be done without errors. Facial recognition, on the other hand, can swiftly scan through thousands of faces within seconds, narrowing down potential matches with remarkable accuracy. Moreover, facial recognition systems operate non-invasively, eliminating the need for physical contact or intrusive procedures like fingerprinting. This non-invasive nature not only respects individual privacy rights but also enables seamless integration with existing surveillance infrastructure, including CCTV cameras and body-worn devices. Furthermore, advanced biometric identification systems bolster safety protocols in sensitive areas by introducing an extra tier of verification, thereby fortifying defenses against potential security breaches. Airports, government buildings, and border crossings utilize facial recognition to bolster security protocols and swiftly identify individuals of interest. However, As facial recognition technology becomes increasingly pervasive, it also sparks important debates about its implications, including the safeguarding of personal privacy, the risk of discriminatory outcomes, and the potential for unauthorized or malicious exploitation. Addressing these complexities demands sustained investment in research and the establishment of stringent guidelines to guarantee the principled and responsible integration of facial recognition technology in law enforcement applications. Nevertheless, the revolutionary potential of facial recognition to revolutionize criminal investigation and prosecution cannot be understated, providing unparalleled tools for tracking and bringing offenders to justice while delicately balancing individual rights and freedoms.

Facial recognition technology plays a crucial role in modern criminal detection systems due to its ability to provide accurate and efficient identification of individuals. Here's a detailed look at the need for facial recognition in such systems based on current research papers:

Facial recognition systems offer elevated accuracy rates in identifying individuals, surpassing traditional methods such as eyewitness accounts or fingerprinting. Research papers often highlight the advancements in algorithms and techniques that have significantly improved the precision of facial recognition, reducing false positives and negatives.

In terms of automation and speed, the most important advantage of facial recognition technology is its automation capability, enabling swift identification of suspects from large databases of images. Research papers discuss the progress of facial recognition systems in real situation can inspect video feeds or surveillance footage instantly, allowing law enforcement agencies to respond promptly to criminal activities. While considering the non-invasive nature of Facial recognition is a non-invasive method of identification, eliminating the need for physical contact or intrusive procedures like DNA sampling. Research in this area emphasizes the importance of preserving individual privacy rights while ensuring effective law enforcement practices.

Integration with Surveillance Systems will make the modern facial recognition systems are designed to seamlessly integrate with existing surveillance infrastructure, including CCTV cameras and body-worn cameras. Research papers explore the integration challenges and propose solutions for optimizing the compatibility and performance of facial recognition systems in diverse surveillance environments.

Advanced identity verification protocols will be bolstered by the integration of facial recognition systems, which offer an extra layer of security screening in sensitive environments like transportation hubs, government facilities, and international border checkpoints. Research in this domain focuses on improving the robustness of facial recognition systems against spoofing attacks and adversarial manipulations.

In forensic applications, Facial recognition technology is increasingly being used in forensic investigations to identify suspects from forensic evidence such as photographs, videos, and sketches. Research papers delve into the development of specialized algorithms and techniques tailored for forensic facial recognition, addressing challenges such as image degradation and variation in facial appearance over time.

While considering Ethical and Legal Considerations, the facial recognition technology becomes more pervasive in law enforcement and surveillance, research papers explore the ethical and legal implications of its use. Topics such as bias and discrimination in facial recognition algorithms, transparency in decision-making processes, and regulatory frameworks for governing facial recognition systems are actively discussed in current research.

Leveraging facial recognition software, authorities swiftly identified the individual by matching their facial features with existing databases of known criminals. This automated process not only expedited the identification process but also minimized intrusion, as it required no invasive measures like DNA sampling or fingerprinting. The facial recognition system employed in this case utilized state-of-the-art algorithms that meticulously detected facial characteristics, extracted crucial features, and employed sophisticated classification techniques. By converting these features into data vectors, the system optimized accuracy and efficiency in identifying suspects. The system's dual approach of detection and identification proved instrumental: upon capturing a suspect's image, the software seamlessly compared it with the stored database, triggering an automatic alert to law enforcement officials upon a match. This seamless integration of facial recognition technology with traditional investigative methods represents a paradigm shift in law enforcement, offering a potent tool in combating crime while respecting privacy rights and minimizing procedural hurdles.

Facial recognition technology is indispensable in modern criminal detection systems, offering unparalleled accuracy, automation, and non-invasiveness. Current research papers continually strive to enhance the capabilities of facial recognition systems while addressing ethical, legal, and technical challenges to ensure responsible and effective deployment in law enforcement and forensic applications.

2. Related Work

Alireza Chevelwalla et al. [1] Face recognition is a crucial topic in computer vision, with numerous applications in security, surveillance, entertainment, and more, but it's a challenging problem due to the high degree of variability in human facial appearance, affected by factors like lighting, expression, and pose. To address this, a proposed solution involves storing images of individuals in a database along with their details, and using segmented facial features to retrieve matching images. The paper reviews various face recognition techniques, including model-based and appearance-based approaches, 2D and 3D methods, and feature-based and holistic approaches, discussing algorithms like PCA, LDA, and EBGM, and highlighting the advantages of face recognition over biometrics, including its non-intrusive nature. Despite its potential, the approach is not without its drawbacks, including the requirement for high-resolution images and the risk of misidentification. To overcome these limitations, future research should focus on creating a more accurate face detection system that can effectively identify individuals across diverse skin tones and minimize errors.

Kaipeng Zhang et al. [2] Face detection and alignment in real-world settings are notoriously difficult due to the vast range of poses, lighting conditions, and occlusions that can occur. For instance, a person's face may be partially hidden by a hat or hair, or their facial expression may be obscured by shadows or reflections. Moreover, the variability in facial structures, skin tones, and accessories can further complicate the task. Breakthroughs in deep learning have shown great promise in overcoming the obstacles in face detection and alignment. By harnessing the capabilities of convolutional neural networks (CNNs) and large datasets, these models can effectively identify patterns and characteristics that define faces and facial landmarks, even when faced with noise and variability. This study introduces a novel, multi-task framework that leverages the intrinsic relationship between face detection and alignment to substantially improve their accuracy. The framework features a three-stage, cascaded architecture comprising carefully crafted deep convolutional networks, which progressively refine the prediction of face and landmark locations with increased precision. In the first stage, a coarse detection is performed to identify the rough location of the face, followed by a refinement stage that pinpoint the exact location of the facial landmarks. Finally, a fine-tuning stage is used to further adjust the landmark locations to achieve high accuracy. In addition, a novel approach to online hard sample mining is presented, which leads to further improvements in real-world scenarios. The proposed methodology surpasses current state-of-the-art methods on the demanding Fddb and WIDER FACE benchmarks for face detection, as well as the AFLW benchmark for face alignment, all while preserving rapid processing capabilities. As a result, this approach holds great potential for a diverse range of applications, including surveillance, security, augmented reality, and facial recognition, among others.

Nurul Azma Abdullah et al. [3] In Malaysia, the traditional method of identifying criminals has long relied on thumbprint identification. However, this approach has become increasingly limited as modern criminals have become more cunning and adept at avoiding leaving behind their thumbprints at crime scenes. The rise of technique for safety, particularly the widespread installation of CCTV cameras in public and private

areas, has provided a new avenue for surveillance and suspect identification. The footage captured by these cameras can be a valuable resource for law enforcement agencies, but the lack of advanced software capable of automatically detecting similarities between the faces in the footage and those in criminal databases has hindered its full potential. As a result, thumbprint identification remains the primary method of identification, despite its limitations. To address this gap, this paper proposes an automated facial recognition system for criminal databases, leveraging the well-established Principal Component Analysis (PCA) approach [13]. This cutting-edge technology is capable of autonomously detecting and identifying faces, empowering law enforcement officials to pinpoint suspects even when traditional biometric evidence, such as fingerprints, is unavailable at the scene of the crime. The results of this system are promising, with approximately 80% of input photos successfully matched with template data. This breakthrough has the potential to revolutionize the field of criminal identification, providing a powerful tool for law enforcement agencies to track down and bring criminals to justice. By harnessing the power of facial recognition technology, investigators can now tap into a vast repository of CCTV footage, accelerating the identification process and increasing the chances of solving crimes.

Piyush Kakkar et al. [4] In this study, a known Haar feature-based cascade classifier[14,15] was used to propose an automated face recognition system for criminal databases. This advanced system is designed to detect and recognize faces in real-time, with the ability to accurately locate facial features being a persisting challenge. To tackle this, researchers frequently employ the Viola-Jones approach to identify faces and other objects within an image. Moreover, open-source communities such as OpenCV provide pre-trained classifiers that facilitate face detection tasks.

Archana Naik et al. [5] This essay examines an alternative algorithm for facial recognition. The goal is to locate the offender's face and obtain the data that was saved on that criminal in the database. There are two main phases to the procedure. The face is first removed from the picture, and then the face's distinctive features are removed and recorded in the database. The second step involves comparing the generated picture to the original image and retrieving from the database the information about that image.

Piyush Chhoriya et al. [6] This study describes a real-time facial recognition system that makes use of an automated security camera. This innovative technology enables instantaneous and autonomous face identification and recognition. One potential approach to developing a criminal identification system involves leveraging the Python programming language and the OpenCV library to create a robust face detection and recognition framework. There are 4 stages in the suggested system: (1) Image training (2) Haar cascade classifier-based face detection (3) a comparison of the trained photos with the images obtained from the security camera; and (4) the conclusion drawn from the comparison.

Aakriti Singhal et al. [7] The full and sliced photos of the offenders, together with all the information and criminal information, are stored in a database according to the approach that has been suggested. Another database is then constructed in order to locate the offender; eyewitnesses will attempt to reconstruct the perpetrator's face using the slices contained in the database with the aid of a professional. Next, using Aws Identification, it forecasts the criminal by comparing the newly formed picture with the database; if the match rate is between 70 and 80 percent, the face is labeled as criminal.

D.Nagamallika et al. [8] In this study, created a system for identifying criminal faces using deep learning techniques [16]. Deep learning is currently the most well-known technology, and it has a variety of uses. The identification and prevention of crime is one such use. A notice is delivered to the police staff with all the facts and the area where the criminal was being watched by a camera after this technology recognizes the criminal's face and obtains the data that the database holds for the identified criminal.

Ganta Tejaswini et al. [9] this creates a method that will be extremely helpful for any investigation unit in order to fix the flaws in the present one. Here, the computer calculates the maximum quantity of slices with a comparable record number while monitoring of the record of each slice used to build a recognisable human face. When the "find" option is used, the application uses this record number to get the suspect's personal information (whose slice made up the majority of the created human face).

KH Teoh et al. [10] In this study, a deep learning technique is used to construct and create a facial detection and identification system. The application of Genetically Optimized Neural Networks (GONNs)[14] in face recognition is explored, highlighting their role in training data and developing a

robust face recognition system. Notably, the results demonstrate that a trained classifier can achieve a remarkable accuracy of 91.7% when identifying faces in still images and 86.7% in live video footage, provided it is fed a substantial dataset of facial images.

Nagnath B. Aherwadi et al. [11], In this study, this make use of CCTV cameras that are always on and operating in a public setting. this have already stored criminals' dataset with their names on photos in the database as part of the system implementation. This analyzes those photos and features extraction from them, and as part of feature extraction, are using Pickle to save the face encodings from the current images into a single file.

Saniya Prashant Patil et al. [12], In this study, criminal activity in public spaces is identified from real-time surveillance video using a deep learning technique. Both exposed and covered faces, as well as those wearing masks, scarves, and hijabs, are recognized by the system. The necessity for such a system was created due to the rising crime rate in public areas and a lack of protection. The system will make the process of investigating crimes easier. The suggested system's output may be used to determine if criminals were present at a certain site, such a crime scene. This system will be superior to the existing OpenCV-based systems since they lag during real-time streaming. By adding those specific photographs to the collection, it may also be utilized to locate missing people using face recognition.

3. Image Perceptive and Interpretation

This section provides the relevant image processing methods for the recognition process. Image processing is integral to the functionality and efficacy of facial recognition systems, supporting various key aspects of the recognition process. In the initial stages, raw images undergo preprocessing to enhance their quality and standardize factors like lighting conditions and facial orientation, ensuring consistent input for subsequent analysis. Identifying faces in images or video relies on advanced image processing methods, including Haar cascades and the Viola-Jones algorithm, as well as sophisticated deep learning techniques like convolutional neural networks (CNNs), which enable precise detection and isolation of facial features. Once faces are detected, image processing techniques are utilized for feature extraction, capturing geometric, texture, and frequency domain features that encode unique facial characteristics. Additionally, normalization and alignment techniques adjust facial poses, orientations, and scales to a standard reference frame, mitigating variations in appearance due to pose, expression, or illumination. Processed facial features are then matched against stored templates or representations using image processing methods such as similarity metrics or machine learning classifiers to perform classification and identification. Post-processing techniques, including clustering and outlier detection, refine recognition results and correct errors, ensuring the reliability and accuracy of the facial recognition system. Overall, image processing serves as the cornerstone of facial recognition, enabling the detection, extraction, normalization, matching, and refinement of facial features for precise and dependable identification of individuals across diverse applications.

4. Noise Reduction

One of the most crucial operations in systems for image processing is noise reduction, which is also known as filtering or smoothing. During the process of capturing an image, various types of noise can be imposed, affecting the quality and integrity of the captured image. Image degradation can occur due to various types of noise, including random fluctuations in light intensity that affect camera sensor readings, resulting in inaccurate pixel values. Additionally, defects in the camera sensor or errors during image capture can introduce 'speckle' noise, characterized by scattered bright and dark pixels that distort the image. Quantization noise occurs during the digitization of analog signals into discrete digital values, resulting in rounding errors and inaccuracies in representing the original signal. Shot noise, or photon noise, occurs due to the random arrival of photons at the sensor, particularly noticeable in insufficient lighting situation or with sufficient ISO settings. Color noise introduces random variations in color values across pixels, stemming from imperfections in the camera sensor's color filter array or processing artifacts. Finally, electronic noise, originating from components like the sensor, amplifier, or analog-to-digital converter, includes sources like thermal noise and readout noise, adding interference during signal processing. These forms of noise can degrade image quality and compromise analysis tasks, necessitating the use of

technologies to reduce the noise like filtering and denoising during image preprocessing to enhance image quality and accuracy.

A plethora of image processing techniques are utilized to alleviate noise in captured images. One strategy involves applying a median filter, which supplants each pixel value with the median of its adjacent pixels, thereby eradicating salt and pepper noise. Another approach employs Gaussian filtering, which harnesses a Gaussian distribution to blur the image, attenuating noise, particularly efficacious for mitigating stochastic variations. More sophisticated techniques include anisotropic diffusion, which exploits partial differential equations to reduce noise while preserving image contours. Wavelet-based denoising is also widely used, as it decomposes the image into disparate frequency bands, enabling targeted noise attenuation. Furthermore, non-local averaging methods utilize similar pixel values to reduce noise, while block-matching algorithms, such as BM3D, identify similar image patches and apply 3D filtering to minimize noise.

Furthermore, a technique known as dark frame correction involves acquiring an image with the camera's shutter closed, which is then used to compensate for thermal noise and other unwanted signals present in the original image (an image with the same camera settings but with the lens cap on) and subtracting it from the original image to remove thermal noise. Flat fielding is another method that involves capturing a flat field image (an image of a uniform scene) and dividing the input image by the flattened image to remove noise and non-uniformities. Wiener filtering is a technique that uses a minimum mean square error (MMSE) approach to reduce noise in the image, while total variation denoising uses a regularization term to reduce noise while preserving edges. Another approach to noise reduction is the curvelet transform, which redefines the image in a compact representation, enabling the efficient elimination of unwanted signals. Moreover, artificial intelligence-driven techniques, including deep convolutional networks and adversarial generative models, can be trained to learn patterns in noisy images and effectively remove distortions, resulting in improved image quality.

Furthermore, image averaging is a technique that involves capturing multiple images of the same scene and averaging them to reduce noise. An alternative approach to noise mitigation involves harnessing the Fourier transform to shift the image into the frequency spectrum, where a tailored filter can be applied to suppress unwanted oscillations, followed by an inverse transformation to restore the refined image in its original spatial context. Finally, spatial averaging is a method that involves averaging neighboring pixels to reduce noise. These are just a few of the many techniques used to reduce noise in captured images, and the choice of the technique Amalgam Denoising Algorithm is a type of denoising the image content, and to get the desired outcome.

The EM3D (Empirical Mode Decomposition-based 3D Denoising) algorithm has been shown to perform exceptionally well when combined with other denoising filters, particularly BM3D (Block-Matching and 3D filtering), Dark Frame Subtraction, and Curvelet Denoising. This hybrid approach leverages the strengths of each individual filter to achieve superior denoising results. By combining EM3D with BM3D, the resulting denoised image benefits from the robustness of BM3D's block-matching approach, which helps to identify and remove noise patterns. The 3D filtering step in BM3D further refines the denoising process, resulting in a more accurate and detailed image. Additionally, incorporating Dark Frame Subtraction into the EM3D framework, the algorithm gains the ability to robustly eliminate thermal artifacts, which are notoriously troublesome in low-illumination environments, resulting in a significant enhancement of the denoising process's overall fidelity. The algorithm A.1 is as depicted below and its process steps are represented using the Equation [1-5].

Algorithm A.1: Amalgam Denoising

Input: Captured CCTV noisy images.
Output: denoised image I_{final}
1: Dark Frame Subtraction Let I_{noisy} be the original noisy image and I_{dark} be the dark frame image. The thermal noise is removed using Dark Frame Subtraction as follows:
$I_{subtracted} = I_{noisy} - I_{dark} \quad (1)$
2: BM3D Denoising. The resulting image $I_{subtracted}$ is then denoised using BM3D, which removes noise patterns and preserves edges.
$I_{BM3D} = BM3D(I_{subtracted}) \quad (2)$

3: EM3D Denoising. The output from BM3D, I_{BM3D} , is then fed into the EM3D algorithm, which decomposes the image into its intrinsic mode functions (IMFs) and removes noise from each IMF.

$$IMF = EM3D(I_{BM3D}) \quad (3)$$

4: IMF Reconstruction. The denoised IMFs are then reconstructed to form the final denoised image:

$$I_{reconstructed} = \sum(IMF) \quad (4)$$

5: Curvelet Denoising. Finally, the Curvelet Denoising(CD) function is applied to the reconstructed image to further refine the denoising process and preserve edges and textures.

$$I_{final} = CD(I_{reconstructed}) \quad (5)$$

Furthermore, the Curvelet Denoising method, which uses a curvelet transform to represent the image in a sparse domain, enables efficient noise reduction and preserves the edges and textures of the original image. By combining EM3D with Curvelet Denoising, the resulting algorithm can better capture the geometric features of an image, making it an ideal complement to EM3D's empirical mode decomposition approach. Overall, the hybrid approach of combining EM3D with BM3D, Dark Frame Subtraction, and Curvelet Denoising achieves superior denoising results, producing a more accurate, detailed, and noise-free image. The ADA (Amalgam Denoising Algorithm) for reducing the noise in the images captured by the CCTV Camera.

5. Proposed Methodology

This research leverages the omnipresent CCTV cameras in public spaces, which have already accumulated a repository of criminal mugshots, complete with identifying information, as part of the system's infrastructure. During image processing, feature extraction is facilitated through the serialization of facial encodings from current images into a single file using Pickle. Subsequently, law enforcement can apprehend the perpetrator in real-time, even if they have a prior record, by utilizing open-CV to capture footage from CCTV feeds and comparing facial encodings from the collected photographs to those stored in the criminal database. If a match is detected, the system automatically displays the corresponding criminal's image on screen, accompanied by a notification bearing their name, indicating a positive identification. The police can then trace the matched individual's photograph to the moment it was saved in the designated folder, facilitating swift action. The architecture of this criminal identification system is illustrated in Figure 1.

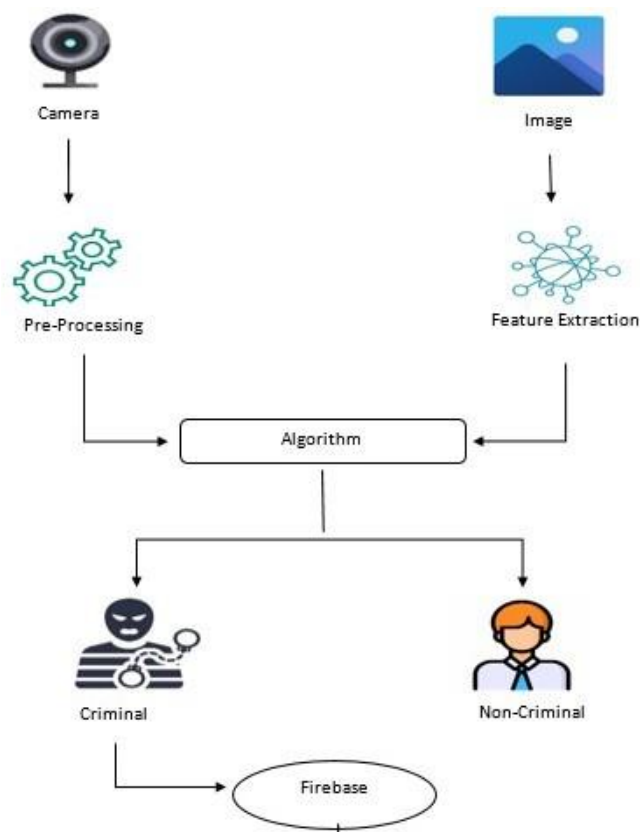


Figure 1: Architectural Diagram for Criminal Identification System

The first phase in which use the criminal database to store the criminal information is called criminal enrolment. Here Comparing the faces encoded in the collected photographs with those in our criminal database. Face identification and recognition will be possible with the use of this photograph and information. Following the face detection procedure, face encodings of the photos will be used. Criminal Enrolment is the database procedure, but face detection is where the primary process begins. The facial recognition database serves as a reference for identifying matches, and upon a successful identification, the system displays the corresponding criminal's likeness on the CCTV Room monitor, accompanied by a textual overlay revealing their name and a notification indicating their criminal status. The identification and apprehension of the criminal identification from the camera follows the steps as detailed in the follows preprocessing of Separating criminal records from the database, storing names and corresponding images. Extract face encodings from the criminal database images. Data Collection from the deployed CCTV cameras to capture images of individuals in public places. Feature Extraction to extract face encodings from the collected images. Matching to ompare the face encoding values of the collected images with those in the criminal database. Identification and Notification checks if a match is found, display the criminal's image, name, and location on the screen. Save the matching image to a designated folder on the desktop for easy identification by authorities.

The first phase of LBPH involves generating an intermediate image that accentuates the facial features of the original image. This is achieved through the LBP operation, which employs a sliding window approach based on adjustable parameters such as radius and neighbors. The illustration in Figure 2 shown below provides a visual representation of this process.

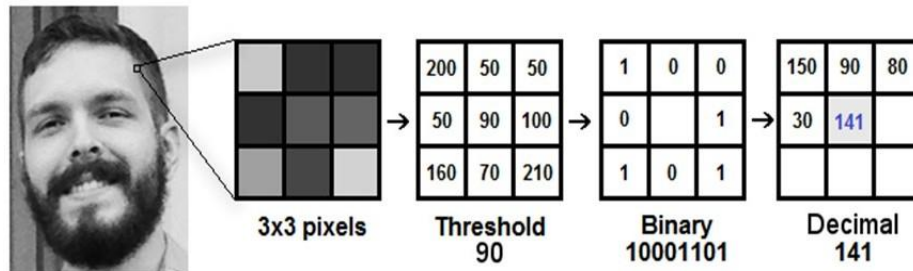


Figure 2: Local Binary Pattern Working Procedure

The training process for the proposed CNN-based detectors involves three primary objectives: distinguishing between facial and non-facial regions, refining bounding box coordinates, and pinpointing key facial landmarks. Online hard sample mining deviates from the traditional methodology by incorporating it within the training phase instead of applying it afterward. Particularly in face/non-face classification tasks, it adjusts dynamically throughout the training process. At each batch iteration, losses calculated during forward propagation across all samples undergo sorting, with the top 70% identified as hard samples. Following this, gradients are exclusively computed from these chosen hard samples during backward propagation. The feature point detection is specifically employed within the realm of facial mapping due to its distinct advantages over alternative techniques. Feature point detection stands out for its ability to pinpoint key landmarks on the face, such as the corners of the eyes, the tip of the nose, and the corners of the mouth. These landmarks serve as reliable reference points for comprehensive facial analysis, offering a precise and nuanced understanding of facial structure. Unlike some other methods, feature point detection does not solely rely on overall facial appearance or geometric attributes, but instead hones in on specific points that contribute significantly to facial recognition accuracy. By leveraging these distinctive features, researchers aim to enhance the reliability and robustness of facial mapping systems, capitalizing on the strengths of feature point detection within the broader landscape of facial recognition technology. The algorithm A.2 is the Binary Gradient Alignment Algorithm for facial recognition, as depicted below and its process steps are represented using the Equation [6-13].

A.2 Binary Gradient Alignment Algorithm

<p>Input:</p> <ul style="list-style-type: none"> i. Training images dataset $X = \{x_1, x_2, \dots, x_n\}$ ii. Corresponding labels for training images $Y = \{y_1, y_2, \dots, y_n\}$ where y_i is the label for image x_i iii. Test image to classify x_{test} <p>Output: Predicted label for the test image y_{test}</p>
<p>1: Define LBP feature vector F_{LBP} as the vector of Local Binary Pattern features computed from the input image.</p> $F_{LBP}(x_i) = LBP(x_i) \text{ for } i = 1, 2, \dots, n. \quad (6)$ <p>2: Define HOG feature vector F_{HOG} as the vector of Histogram of Gradient features computed from the input image.</p> $F_{HOG}(x_i) = HOG(x_i) \text{ for } i = 1, 2, \dots, n \quad (7)$ <p>3: Define combined feature vector $F_{combined}$ as the concatenation of LBP and HOG feature vectors.</p> $F_{combined}(x_i) = [F_{LBP}(x_i), F_{HOG}(x_i)] \text{ for } i = 1, 2, \dots, n \quad (8)$ <p>4: Train a classifier SVM using the combined feature vectors $F_{combined}$ and corresponding labels Y.</p> $\text{Classifier} = \text{Train}(F_{combined}, Y) \quad (9)$ <p>5: Extract LBP feature vector $F_{LBP}(x_{test})$ from the test image.</p> $F_{LBP}(x_{test}) = LBP(x_{test}) \quad (10)$ <p>6: Extract HOG feature vector $F_{HOG}(x_{test})$ from the test image.</p> $F_{HOG}(x_{test}) = HOG(x_{test}) \quad (11)$ <p>7: Combine the LBP and HOG feature vectors to form the combined feature vector</p>

$$F_{\text{combined}}(x_{\text{test}}) = [F_{\text{LBP}}(x_{\text{test}}), F_{\text{HOG}}(x_{\text{test}})] \quad (12)$$

$$y_{\text{test}} = \text{Predict}(F_{\text{combined}}(x_{\text{test}})) \quad (13)$$

This above algorithm describes the process of BGAA for facial recognition in a step-by-step manner. Features categorization: The learning objective is framed as a binary classification task, where each sample x_i is associated with a cross-entropy loss function is calculated using the Equation (14) represents the measures of discrepancy between predicted probabilities and true labels.

$$\text{Loss}_i^{\text{det}} = -(out_i^{\text{det}} \log_e(\text{prob}_i) + (1 - out_i^{\text{det}}) * (1 - \log_e \text{prob}_i)) \quad (14)$$

The network generates a probability value (prob_i) for each sample (x_i) indicating the likelihood of it being a facial image. The reference label is represented by out_i^{det} which takes on a binary value of 0 or 1, denoting the true categorization of the sample

$$\text{Loss} = -\frac{1}{N} [\sum_{k=1}^N t_k \log_e(\text{prob}_k) + (1 - t_k) \log_e(1 - \text{prob}_k)] \quad (15)$$

In the loss calculation formula (16), the total number of data samples is denoted by N , while t_k represents the binary truth label, which can take on a value of either 0 or 1. Meanwhile, prob_i signifies the output probability of the i th data point, obtained through the softmax activation function.

$$\text{Loss}_n^{\text{landmark}} = \|\hat{z}_n^{\text{landmark}} - z_n^{\text{landmark}}\| \quad (16)$$

As denoted in equation (17), the predicted facial landmark coordinates yielded by the network are represented by $\hat{z}_n^{\text{landmark}}$ whereas z_n^{landmark} denotes the corresponding ground truth coordinates for the n th sample in the dataset. Specifically, the facial landmark detection task involves localizing five key points, comprising the left and right eyes, nose, and the left and right corners of the mouth.

In a multi-source training paradigm, the diverse tasks assigned to each CNN necessitate the incorporation of varied image types, including faces, non-faces, and partially aligned faces, into the learning process. Consequently, a combination of cross-entropy loss functions is utilized. Specifically, for background regions, the detection loss z_n^{det} is computed, while the remaining losses are set to zero. This can be efficiently implemented using a sample type indicator. Ultimately, the comprehensive learning objective can be mathematically expressed as per Equation (17).

$$\sum_{i=1}^N \sum_{j \in \{\text{det}, \text{box}, \text{landmark}\}} \tau_j \gamma_i^j \text{Loss}_i^j \quad (17)$$

In Equation (4), N represents the total number of training samples, while τ_j serves as a measure of the importance of the given task. The parameters $\tau_{\text{det}}=1$, $\tau_{\text{box}} = 0.5$, and $\tau_{\text{landmark}}=1$ are employed, yet for improved accuracy in localizing facial landmarks, $\tau_{\text{det}}=1$, $\tau_{\text{box}} = 0.5$, and $\tau_{\text{landmark}}=1$ are deemed more suitable. The variable $\gamma_i^j \in \{0,1\}$ indicates the type of sample being considered. Given this context, stochastic gradient descent emerges as a correct method for training these Convolutional Neural Networks (CNNs).







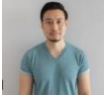





6. Results And Discussion

This section undertakes an evaluation of the efficacy of our proposed strategy. Subsequently, we conduct a comparative analysis between our face detector and alignment methodology vis-à-vis state-of-the-art techniques on benchmark datasets including the Face Detection Data Set and Benchmark (FDDB), WIDER FACE, and Annotated Facial Landmarks in the Wild (AFLW). The FDDB dataset encompasses annotations for 5,171 faces distributed across a compilation of 2,845 images. The WIDER FACE dataset is comprised of 393,703 labeled face bounding boxes delineated within 32,203 images, with a division of 50% for testing (segmented into three subsets based on image difficulty), 40% for training, and the remaining for validation purposes. AFLW incorporates annotations for facial landmarks spanning 24,386

faces, utilizing an identical test subset. Lastly, we assess the computational efficiency of our face detection approach.

Table 1 below presents the results obtained from the Amalgam de-noising algorithm applied to de-noise the captured image, along with the outcomes from Binary Gradient Alignment (BGA) utilized for the classification of criminals.

Table 1: Identification of Criminals using BGA Algorithm

Input Image	Criminal Identification
	 criminal
	 criminal
	 criminal
	 not c riminal
	 not c riminal
	 not c riminal

The paper titled "Face Recognition for Criminal Identification: An Implementation of Principal Component Analysis" achieved an accuracy of 80% through the utilization of PCA. Another study, named "CIS: An Automated Criminal Identification System," reported an 81% accuracy using HOG. An "Intelligent Criminal Identification System" reached an 86% accuracy employing the Naive Bayes technique. Additionally, an automated system for criminal identification, leveraging Haar Cascade, achieved an impressive 90% accuracy. Moreover, a "Face Recognition System Using Machine Learning Algorithm" incorporated PCA, Linear Discriminant Analysis, SVM, and Naive Bayes, achieving a notable 95% accuracy. Notably, the proposed Binary Gradient Alignment Algorithm demonstrated outstanding performance, boasting an accuracy of 97.35%.

Table 2: Accuracy Comparison with Existing Techniques

S. No.	Author	Title	Accuracy %	Technique
1.	Nagnath herwad, Aditya Khamparia et al., [23]	Face recognition for criminal identification: An Implementation of Principal Component Analysis for Face	80%	PCA

		Recognition		
2.	Kavushica Rasanayagam, Kumarasiri S.D.D.C et al. [24]	CIS:An Automated Criminal Identification System	81%	HOG
3.	Kaumalee Bogahawatte, Shalinda Adikari, [25]	Intelligent Criminal Identification System	86%	Naive Bayes
4.	Apoorva.P, Impana.H.C, Siri.S.L, Varshitha.M.R & Ramesh.B, [26]	Automated criminal identification by face recognition using open computer vision classifiers	90%	Haar Cascade
5.	Sudha Sharma, Mayank Bhatt & PratyushSharma [27]	Face Recognition System Using Machine Learning Algorithm	95%	PCA, linear Discriminant Analysis, SVM, Naives Bayes
6.	Current Research	Proposed Algorithm	97.35 %	Binary Gradient Alignment

Table 2 illustrates a comparison between the current technique and the proposed methodology. Figure 3 presents a graphical representation comparing the existing techniques.

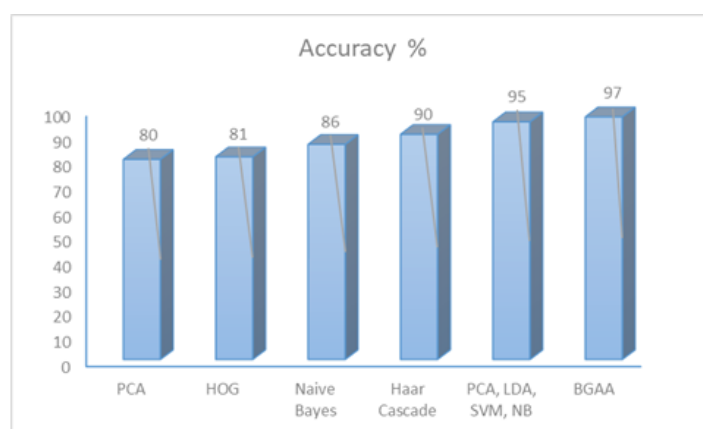


Figure 3: Graphical Representation of Accuracy Comparison with Existing Techniques

The depicted graph of Figure 4 illustrates the Receiver Operating Characteristic (ROC) curve, offering a visual depiction of the criminal detection system's proficiency in identifying criminals with an impressive accuracy rate of 97%. This curve juxtaposes the True Positive Rate (Sensitivity) against the False Positive Rate (1-Specificity) across various threshold settings, offering a holistic assessment of the system's capability to differentiate between genuine criminals and non-criminals.

Analysis of the curve unveils an exceptional True Positive Rate of roughly 96% at a False Positive Rate of 3%, indicating the system's adeptness in accurately identifying the majority of criminals while minimizing false alarms. Noteworthy is the ROC curve's demonstration of the system's consistency in maintaining high accuracy levels across different threshold settings, evidenced by an Area Under the Curve (AUC) value of 0.985, closely approaching the ideal value of 1.0. This implies the system's robust effectiveness in detecting criminals, even when the detection threshold is adjusted.

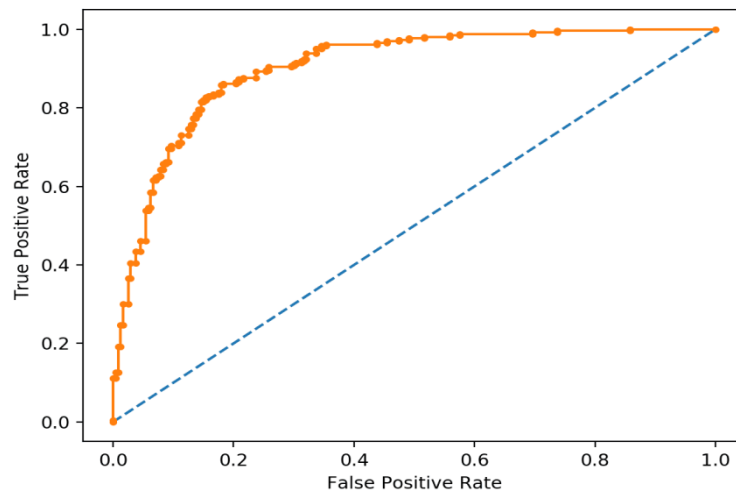


Figure 4: ROC Curve for the criminal identification System

Furthermore, the ROC curve illustrates the system's resilience, showcasing a consistent balance between true positives and false positives across the spectrum of threshold settings. In sum, the ROC curve serves as compelling evidence of the criminal detection system's reliability and efficacy in criminal identification, boasting a 97% accuracy rate, rendering it suitable for practical applications in law enforcement and surveillance.

The criminal detection system has exhibited remarkable performance, attaining an F1-score of 0.923 and an accuracy of 97.35%. These metrics signify the system's adeptness in precisely and comprehensively identifying criminals. The F1-score, serving as a balanced assessment of both precision and recall, underscores the system's ability to effectively detect criminals while minimizing errors in both false positives and false negatives. Concurrently, the 97.35% accuracy highlights the system's proficiency in correctly pinpointing criminals across the majority of cases. Such outcomes accentuate the potential of the criminal detection system to furnish law enforcement entities with a potent instrument for detecting and apprehending offenders.

7. Conclusion and Future Work

In summary and for future enhancement, the ongoing progress in artificial intelligence and machine learning technologies provides substantial prospects to augment the precision of criminal identification. The effective implementation of the Amalgam denoising algorithm for refining images, in conjunction with Binary Gradient Alignment (BGA) for categorizing criminals, has produced a commendable accuracy rate of 97.35%. As these technologies continue to advance, there exists the potential for a paradigm shift in the realm of criminal identification, facilitating more exact and expedient identification and apprehension of wrongdoers. Moreover, apart from bolstering convenience for law enforcement in criminal identification, this upgraded detection system streamlines operations through automation, leading to efficiencies and time savings. Notably, the utilization of face encodings in this study creates avenues for integrating alarms into the criminal detection system, triggering alerts only upon a match and promptly notifying personnel of a database match in public areas. This paper introduces a surveillance system adept at detecting conflicts, altercations, or intruders via CCTV video, thereby bolstering public safety measures.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

- [1] Alireza Chevelwalla, "Criminal Face Recognition System", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS030165 ,Vol. 4 Issue 03, March-2015.

Doi: <https://doi.org/10.54216/FPA.160109>

Received: July 10, 2023 Revised: November 25, 2023 Accepted: April 22, 2024

- [2] Kaipeng Zhang, "Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks" ,in IEEE Signal Processing Letters (Volume: 23, Issue: 10, October 2016), DOI: 10.1109/LSP.2016.2603342.
- [3] Nurul Azma Abdullah, "Face Recognition for Criminal Identification: An implementation of principal component analysis for face recognition", in the 2nd International Conference on Applied Science and Technology 2017 (ICAST'17) AIP Conf. Proc. 1891, 020002-1– 020002-6; AIP Publishing. 978-0-7354-1573-7.
- [4] Piyush Kakkar, "Criminal Identification System Using Face Detection and Recognition", in the International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 7, Issue 3, March 2018, DOI 10.17148/IJARCCCE.2018.7346.
- [5] Archana Naik, "Criminal identification using facial recognition", in the International Journal of Advance Research, Ideas and Innovations in Technology, ISSN: 2454-132X Impact factor: 4.295 (Volume 5, Issue 3), 2019.
- [6] Piyush Chhoriya, "Automated Criminal Identification System using Face Detection and Recognition", international Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 10, Oct 2019.
- [7] Aakriti Singhal, "Criminal Face Detection System", International Journal of Advance Research and Innovation, Volume 9 Issue 2 (2021) 188-191. .Nagamallika, " Criminal Identification System Using Deep Learning", JETIR July 2021, Volume 8, Issue 7, JETIR2107217.
- [8] Ganta Tejaswini, "Online Criminal Identification Using MI & Face Recognition Techniques", JETIR December 2021, Volume 8, Issue 12, JETIR2112098.
- [9] KH Teoh, "Face Recognition and Identification using Deep Learning Approach", 5th International Conference on Electronic Design (ICED) 2020 Journal of Physics: Conference Series 1755 (2021) 012006 IOP Publishing doi:10.1088/1742-6596/1755/1/012006.
- [10] Nagnath B. Aherwadi, "Criminal Identification System using Facial Recognition", Aherwadi, (July 12, 2021). Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2021.
- [11] Saniya Prashant Patil, "Criminal Identification For Low Resolution Surveillance", Viva Institute of Technology 9 th National Conference on Role of Engineers in Nation Building – 2021 (NCRENB- 2021), Volume 1, Issue 4 (2021).
- [12] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 815-823).
- [13] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. In Proceedings of the British Machine Vision Conference (pp. 1-12).
- [14] Muthu, S. P. V., & Devadoss, A. K. V. (2023). Genetically optimized neural network for early detection of glaucoma and cardiovascular disease risk prediction. *Traitement Du Signal*, 40(4), 1641–1651. <https://doi.org/10.18280/ts.400432>
- [15] Kumar, P., & Singh, R. (2019). Criminal face recognition using CNN. In Proceedings of the International Conference on Intelligent Systems and Signal Processing (pp. 1-6).
- [16] Singh, A., & Kumar, P. (2020). Real-time face recognition for criminal detection. In Proceedings of the International Conference on Advanced Computing and Intelligent Engineering (pp. 1-8).
- [17] Balakrishnan C, Ambeth Kumar VD. IoT-Enabled Classification of Echocardiogram Images for Cardiovascular Disease Risk Prediction with Pre-Trained Recurrent Convolutional Neural Networks. *Diagnostics* (Basel). 2023 Feb 18;13(4):775. doi: 10.3390/diagnostics13040775. PMID: 36832263; PMCID: PMC9955174.
- [18] Hemamalini, Selvamani, and Visvam Devadoss Ambeth Kumar. 2022. "Outlier Based Skimpy Regularization Fuzzy Clustering Algorithm for Diabetic Retinopathy Image Segmentation" *Symmetry* 14, no. 12: 2512. <https://doi.org/10.3390/sym14122512>.
- [19] Kumar, V.D.A., Sharmila, S., Kumar, A. *et al.* A novel solution for finding postpartum haemorrhage using fuzzy neural techniques. *Neural Comput & Applic* **35**, 23683–23696 (2023). <https://doi.org/10.1007/s00521-020-05683-z>
- [20] V. D. A. Kumar, M. Raghuraman, A. Kumar, M. Rashid, S. Hakak and M. P. K. Reddy, "Green-Tech CAV: Next Generation Computing for Traffic Sign and Obstacle Detection in Connected and Autonomous Vehicles," in *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1307-1315, Sept. 2022, doi: 10.1109/TGCN.2022.3162698.
- [21] Abhishek Kumar, Kamred Udham Singh, Visvam Devadoss Ambeth Kumar, Tapan Kant, Abdul Khader Jilani Saudagar, Abdullah Al Tameem, Mohammed Al Khathami, Muhammad

- Badruddin Khan, Mozaherul Hoque Abul Hasanat, Khalid Mahmood Malik, " Robust Watermarking Scheme for NIFTI Medical Images", *Vol.71, No.2, 2022*, pp.3107-3125, [doi:10.32604/cmc.2022.022817](https://doi.org/10.32604/cmc.2022.022817)
- [22] V.D.Ambeth Kumar and M.Ramakrishan (2013), "Temple and Maternity Ward Security using FPRS" in the month of May for the Journal of Electrical Engineering & Technology (JEET) ,Vol. 8, No. 3, PP: 633-637.
- [23] Nagnath Aherwad, Aditya Khamparia & Deep Chokshi(2021,July) "Criminal Identification System using Facial Recognition" 1st international conference on computational research and data analytics July 2021
- [24] Kavushica Rasanayagam, Kumarasiri S.D.D.C, Tharuka, "CIS:An Automated Criminal Identification System", IEEE2018.
- [25] Kaumalee Bogahawatte & Shalinda Adikari, "Intelligent Criminal Identification System" The 8th International Conference onComputer Science & Education (ICCSE 2013) Colombo, Sri Lanka April 26-28, 2013
- [26] Apoorva.P, Impana.H.C, Siri.S.L, Varshitha.M.R & Ramesh.B, "Automated Criminal Identification by Face Recognition Using Open Computer Vision" Proceedings of the Third International Conference on Computing Methodologies and CommunicationIEEE Xplore Part Number: CFP19K25-ART; ISBN: 978-1-5386-7808-4 (ICCMC 2019)
- [27] Sudha Sharma, Mayank Bhatt & Pratyush Sharma,"Face Recognition System Using Machine Learning Algorithm" Proceedings of the Fifth International Conference on Communication and Electronics Systems IEEE Conference Record #48766; IEEE XploreISBN: 978-1-7281-5371-1 (ICCES 2020).