International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

Face Detection and Recognition for Criminal Identification System

Prof. Kiran Yesugade[1], Apurva Pongade[2], Shruti Karad[3], Divya Ingale[4], Shravani Mahabare[5]
[1-5]Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune, India
Email ID: *kiran.yesugade@bharatividyapeeth.edu[1], apurvapongade564@gmail.com[2], shrutikarad20@gmail.com[3], divyaingale01@gmail.com[4], shravanimahabare13@gmail.com[5]*

Abstract
This project showcases a powerful Face Detection and Recognition system intended to improve law enforcement skills by speeding up the identification of suspects in criminal cases. The system uses scalable databases and real-time computation, however instead of using traditional web sources for face detection. Accuracy and dependability are ensured by using the LBPH algorithm for face recognition and the Haar-cascade classifier for feature detection. The smtplib library allows the system to send a Gmail notification when it finds a matching face. The system that has been built contributes to public safety initiatives by improving law enforcement operations and demonstrating versatility for different face detection circumstances. The outcomes show how successfully the system can detect faces in real-time circumstances. The system achieves great performance by creating dynamic datasets and integrating algorithms. Integrating Gmail improves law enforcement response by facilitating prompt contact of identified suspects. This study highlights the role that surveillance technology plays in public safety and crime prevention, and it provides law enforcement authorities with useful solutions. Furthermore, the uses of this facial recognition and detection technology go beyond police enforcement. It can expedite attendance tracking and improve security in access control systems. Because of its adaptability, it can be used in a variety of industries and is expected to have a significant impact.

Keywords: *LBPH algorithm; real-time computation; scalable database; smtplib library*

1. Introduction
Electric The advent of advanced technology has transformed numerous sectors, including security and law enforcement, with Face Detection and Recognition systems becoming pivotal in modern surveillance and identification processes. This project focuses on developing a highly accurate system tailored to the needs of law enforcement, aiming to expedite the identification of suspects in criminal cases. Traditional methods of suspect identification, often manual and prone to errors, are increasingly inadequate in addressing contemporary security challenges. The development of this Face Detection and Recognition system marks a significant advancement in security technology, providing a reliable and efficient solution for identifying suspects in criminal cases. Its broader applications, coupled with careful consideration of ethical issues, highlight its potential for widespread adoption and its contribution to enhancing public safety. This project underscores the transformative impact of intelligent surveillance systems in meeting modern security challenges, paving the way for more effective crime prevention and response strategies. This tailored approach ensures data relevancy and quality, which are critical for the system's performance. The initial step involves converting color frames to grayscale images, simplifying the data and enhancing detection accuracy. At the core of this project is the development of custom datasets for face detection, diverging from the common reliance on online sources. custom datasets and advanced algorithms, this system provides a more efficient and reliable alternative to conventional approaches, ultimately enhancing public safety. The proposed system leverages real-time processing and scalable databases, offering a robust solution to these challenges. By integrating grayscale images reduce

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

complexity and improve processing speed, which is essential for real-time applications. The Haar-cascade classifier, a machine learning-based approach, is employed for feature detection. Trained on a set of positive and negative images, it effectively identifies facial features under varying conditions. Following detection, the Local Binary Patterns Histogram (LBPH) method is used for recognition due to its robustness and accuracy. This method analyzes local image features, creating a histogram that represents the face, which is then compared with stored histograms in the database. Real-time processing capability is a critical feature of this system, as timely identification of suspects is crucial for law enforcement operations. The system's scalable database architecture ensures efficient handling of large data volumes, allowing for expansion and adaptation to meet growing needs without compromising performance. A key component of the system is its notification mechanism, which alerts authorities upon detecting a match. By integrating the smtplib library, the system can send automated Gmail notifications, ensuring prompt communication. This feature enhances the system's practical utility by facilitating swift action and maintaining efficient communication within law enforcement agencies. Beyond law enforcement, this technology can be adapted for various applications, such as enhancing security in access control systems and streamlining attendance management. These additional applications demonstrate the system's versatility and broad potential impact across different sectors. This project also addresses the ethical considerations associated with deploying face recognition technology, emphasizing the importance of privacy and security. The system incorporates data encryption, secure storage, and access controls to protect individuals' information. Transparency and accountability measures are implemented to ensure the technology is used responsibly and ethically, aligning with legal and societal standards.

2. Literature Survey

A deep neural network and machine learning algorithm are employed in the face detection system, which may also be used as a basic criminal identification system. A camera module is one of the hardware requirements, primarily for CCTV. The main objective of the study is to map distinctive features like lips, hair, and beards. There are two crucial stages to face recognition. 1. Verification of face 2. Recognition of an individual's visage [1]. Face detection plays a major role in face identification, but it also contributes other features. Face-net is the library used for face identification, and face extraction is included. The feature is trained using Deep CNN [2]. The study suggests a novel approach that makes use of elements for real-time criminal identification [3]. In the story, missing children and criminals are identified through the use of web scraping and facial recognition technology. It classifies individuals into groups using a Haar cascade classifier, after which it determines if a certain face is criminal [4,5]. OpenCV is used to extract features from images. Web scraping is employed for training, and a feature 9 can recognize many faces in a single photo, which improves the application's speed and reliability [6]. An investigation into facial recognition for criminal identification in surveillance footage brought to light the importance of video graphics technology in identifying criminals hiding behind the crime scene [7]. The system combines CNN and DNN algorithms for neural recognition [8]. The project compares the dataset with match data frames to produce a result based on the classification method. [9] The application of a criminal detection system predicated on an offender's prior criminal activities is illustrated in the study. The model tags face from the wild dataset using the CNN algorithm to perform neural recognition in the simulator. The automatic system is searching for the perpetrator [10]. The mapping of photos with the database is the main purpose of the proposed system. CCTV cameras are frequently utilized to take the image [11]. The model's accuracy is roughly 87%, however accuracy loss becomes a significant issue when it comes to verification [12]. The database of the prototype features redundant names, which could result in duplicate entries with names associated with criminal activity [13]. This study makes use of the Labeled Faces in the Wild dataset and the CNN approach [14]. The main goal of the proposed approach is to develop a reliable facial alignment

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

and detection system for criminal identification [15]. The system makes use of FaceNet and Multi-task cascaded convolution neural networks to fully use the power of convolution neural networks [16]. The goal of this project is to apply deep learning to improve terrorist and criminal detection. It uses CNNs to recognize faces, emotions, ages, and genders, and LeNet to identify suits. IMDb is the dataset, and Keras on Tensor Flow is utilized for categorization. For efficiency, AWS is used for training. The goal of the project is to increase security forces' ability to identify suspects more accurately and efficiently [17]. In order to help with incidents such as child abuse or rioting, the study presents an automated technique for identifying persons based on Relatively Permanent Pigmented or Vascular Skin Marks (RPPVSM) observed on non-facial body areas. It achieves high identification accuracies on a variety of subjects by combining skin segmentation, matching algorithms, and RPPVSM detection. For Asian participants with fewer RPPVSM, a fusion approach using inferred vein patterns improves identification even more. This technique is the first of its kind for forensic situations' automated identification utilizing non-facial skin markings [18]. This research provides an automated surveillance camera-based real-time facial recognition system. The system consists of face detection with a Haar-classifier, real-time image training, comparison with previously trained photos, and result presentation. The system uses OpenCV's Haar cascade technique for face detection in order to identify people who are on a watch list. It has a high degree of accuracy and rapid multi-face recognition. The suggested approach proposes to distinguish between citizens and foreigners using India's Aadhar database, assisting in criminal investigations [19]. The development of algorithms for automatically identifying criminals' faces is described in this paper. Several face identification techniques are covered, including 3D shape models, Eigen face, Fisher face, Local Binary Pattern, and active appearance. Utilizing data augmentation for enhanced training performance, the Local Binary Pattern Histogram approach is used to face recognition. Features like eyes, nose length, cheek, lips, etc. are extracted using the Haar cascade. With the use of a web camera to capture grayscale photographs of people, the system can identify and detect people, transferring this data to WhatsApp after the classifier has been trained with these images [20].

3. Proposed System

The proposed method utilizes Haar-Cascade for face detection and the LBPH algorithm for face recognition to automatically identify criminal faces. The Python module TKinter was used to build the Graphical User Interface (GUI) for this system, making it the quickest and easiest way to design such an application. The system uses criminal datasets and labels to train photographs in databases and cameras. When the criminal's face is detected, it sends a message to the registered email-ID. The system architecture is depicted in Figure no.1. The next section explains each stage in detail. [21]

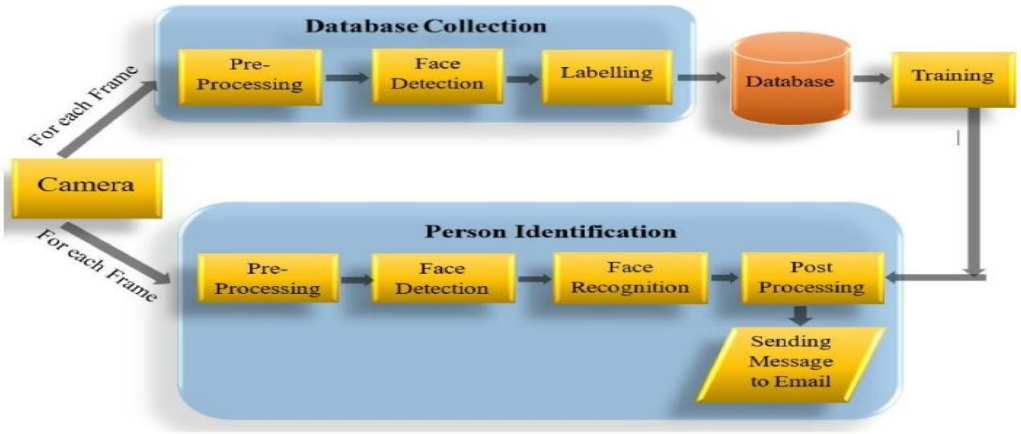

Figure 1 System Architecture

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

The criminal identification and recognition system has a complete architecture that incorporates machine learning to streamline the identification process. The design is divided into two major components: database collecting and individual identification. The first element of database gathering begins with the acquisition of facial photographs obtained while registering the criminal. These photos are pre-processed, with each image cropped to focus on the face and transformed to greyscale to simplify the data and reduce computational complexity. Following that, face detection techniques are used to recognize and isolate facial features in the photos. Once recognized, these photographs are labelled with the relevant identifiers, such as the Id number followed by the individual's image number, to form a tagged dataset. This curated dataset is then saved in a database and used to train a machine learning model intended for facial recognition. The system's second component is responsible for identifying individuals. When a person appears in front of a camera, their face is collected and goes through the identical preprocessing steps: cropping and conversion to greyscale, followed by face detection to extract facial features. The processed image is then fed into the pre-trained facial recognition algorithm. This model compares the new image to a stored database of known faces to detect probable matches. If a match is found, the system moves on to the post-processing step, where all pertinent information on the identified individual is compiled. The system then utilizes the SMTP library to send a notification email to a predetermined email address, informing the recipient about the identified criminal. This architecture offers a fast, accurate, and quick criminal identification procedure by utilizing machine learning for real-time facial recognition and automated alerting.

4. Algorithm

The system's pseudocode is as follows:

- Convert each frame to grayscale from RGB.
- Use the Haar Cascade classifier to detect faces.
- Run the LBPH algorithm on the ROI to retrieve features.
- If no faces are detected, return none.
- If a face is detected and, in the database, capture the image.

5. Datasets

In our project, as shown in Figure 2 we collect 600 images of a single person for training the model. When a person is registered as a criminal or missing, a unique ID is generated in a database for that individual. This ID is then provided to the face data model to create the face data for that person. Each image of a person is stored as 'user.id_number.image_number' (e.g., user.3.10) in jpg format, saved in grayscale. This approach ensures that each image is uniquely identifiable and linked to the person's ID, facilitating efficient data management and retrieval during the training and recognition phases. Before storing the images in grayscale format, we apply a preprocessing technique to enhance the images' quality and reduce noise. This preprocessing involves converting the images to grayscale, which removes color information and retains only the luminance information. Storing images in grayscale reduces the complexity of the data, as it requires only a single channel compared to the three channels (red, green, and blue) in colored images. This simplification makes the training process more efficient and less computationally intensive, especially when dealing with a large number of images. Additionally, grayscale images require less storage space, which is beneficial for managing and storing a large dataset of images efficiently.

Figure 2 Images Stored in Dataset

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

6. Methodology

The system is evaluated using real-time video, with some faces recognized as known and others as unfamiliar. After recognizing and verifying the photograph, the identified face's information is sent over E-mail.

6.1. Pre-Processing and Face Detection.

First, transform the frame from color to grayscale. The haar cascade classifier recognizes faces and detects characteristics in photos using trained cascade functions. With the use of edge, line, and other haar features. The Haar-Classifier system was implemented with the OpenCV library, which includes the class. Large photographs or images with multiple sizes and features require numerous computations, most of which are irrelevant. AdaBoost selects the best image from a big collection of photographs.

6.2. Face Recognition

LBPH approach is used because it is reliable. It also provides a simple way to distinguish between front and side faces. Compared to Eigenfaces and Fisherfaces, this method accurately describes facial traits in images. Combining LBP with the histogram of gradients (HOG) descriptor increases detection performance. This technique improves performance by locally characterizing images within datasets. When an unknown image is changed, it performs similarly to an equivalent approach for comparing images within datasets and displaying results. It outperforms other algorithms in various environments and lighting situations. The first phase of the LBPH method involves highlighting facial traits to create an intermediate image that better describes the original. The algorithm uses a sliding window approach based on radius and neighbour's characteristics, refer Figure 3.

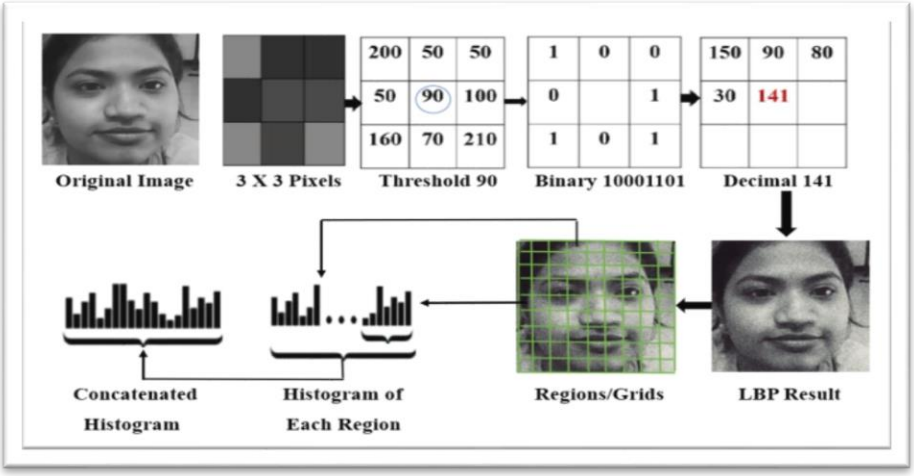

Figure 3 LBPH Algorithm Process

Initially, the frame is transformed to a 3x3 pixel matrix. The median pixel serves as a threshold value. A matrix's values are set to 1 when a neighboring pixel exceeds the median pixel. Otherwise, the values are set to zero. Now obtaining binary values in a clockwise direction. Convert the binary value to a decimal integer and replace it with the matrix's median pixel value. The image is transformed to an LBP (Local Binary Pattern) and divided into numerous grids for histogram extraction. After that, each histogram is concatenated to form a larger histogram. The new, larger histogram reflects the original features. This method will repeat for each new image, resulting in a new histogram.

6.3. Post Processing

Using Euclidean distance, the new histogram is compared to the dataset histograms to identify the individual in the image. The histogram with the lowest confidence, or shortest distance, is chosen. The ID for a histogram is extracted when the confidence level is low. The approach is recognized if the confidence level is lower than the threshold. Once a person is in the datasets, their information is

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

sent to E-mail. Higher confidence labels indicate undetermined status. As shown in Figure 4 this technology automatically identifies criminal faces, making identification easier.

Figure 4 Person Identification Result

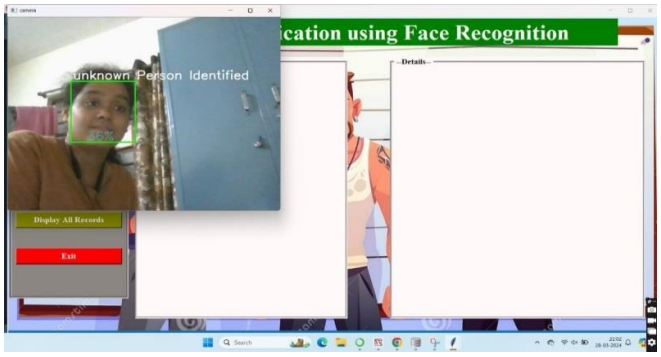

Figure 5 Unknown Person Identification Result

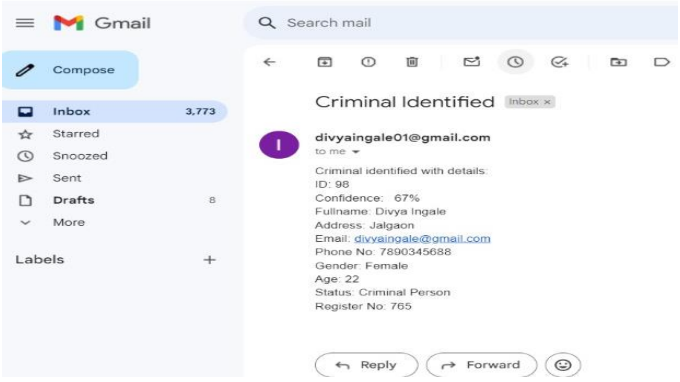

Figure 6. Result Sent to E-Mail

7. Result and Discussion

When a face is discovered in a surveillance camera kept in the database, Email will be notified. Importing the smtplib library file allows you to send information using Email as shown in Figure 6. The camera will mark faces that are not in the database as unknown as shown in Figure 5. The camera will detect two more faces. This simple technology sends the details we have taken while registration that are id, confidence is calculated by algorithm, full name, address, email id, phone no, gender, age, status, registration no.

Conclusion

The creation of the Face Detection and Recognition system signifies a major progress in law enforcement technology, offering a dependable and effective tool for recognizing suspects immediately. Using custom datasets, the system achieves high accuracy and performance with the Haar-cascade classifier for detection and the LBPH method for recognition. The combination of instant processing abilities and a strong notification system guarantees quick and efficient communication, improving the speed of law enforcement responses. This project meets the current requirements of law enforcement and shows possibilities for wider use in different security and access control situations. In general, the advancement of the system highlights how advanced surveillance technologies can improve public safety and operational efficiency.

References

[1]. Escobar, H., Cuevas, E., Toski, M. I., Ramirez, F. J. C., & Pérez-Cisneros, M. (2023). An Agent-Based Model for Public Security Strategies by Predicting Crime Patterns. IEEE Access, 11, 67070-67085.

[2]. Andrew Fredrick Nyoka, Kelvin Sauli Godfrey, Happines Gideon Mwakilembe, Leonard Jonas Mugendi, Oscar David Mbita, Adramane Assoumana, Dawson Ladislaus Msongaleli, “Reliable Face Identification System for Criminal Investigation,” in 11th International Symposium on Digital Forensics and Security (ISDFS), pp. 2023.

[3]. M Saravanan, K. Kowsalya, “Real-Time Criminal Face Identification Based on Haar-Cascade and Lbph, with Automatic Message Delivery to Whatsapp,” in IEEE 2nd Mysore Sub Section International Conference (MysuruCon), pp. 2022.

[4]. Shafia and Manzoor Ahmad Chachoo, “Social Network Analysis based Criminal Community Identification Model with Community Structures and Node Attributes,”

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

in Proceedings of the Fourth International Conference on Smart Systems and Inventive Technology, pp. 2022

[5]. Md. Faruk Abdullah Al Sohan, Nusrat Jahan Anannya, Afroza Nahar, Kazi A Kalpoma "Preliminary Findings: Use of CNN Powered Criminal Identification System," in Proc. of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering, pp. 2022

[6]. Swati Jagtap, Nilkanth B.Chopade, Sanjay Tungar, "An Investigation of Face Recognition System for Criminal Identification in Surveillance Video," in 6th International Conference On Computing, Communication, Control And Automation, pp. 2022

[7]. Sanika Tanmay Ratnaparkhi, Dr. Pooja Singh, Aamani Tandasi, Dr. Nidhi Sindhwani," Comparative Analysis of Classifiers for Criminal Identification System Using Face Recognition" in IEEE in 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), pp. 2021

[8]. Raj Kumar R, Shyam Sundar A, Ruban Haris B, Ragul K, Cloudin S, "Identification of Criminal and Non-Criminal Face Using Deep Learning and Image Processing," in International Conference on System, Computation, Automation and Networking (ICSCAN), pp. 2021.

[9]. Aamani Tandasi, Sanika Tanmay Ratnaparkhi, Shipra Saraswat, "Face Detection and Recognition for Criminal Identification System," in 11th International Conference on Cloud Computing, Data Science & Engineering, pp. 2020.

[10]. Imran Shafi, Sadia Din, Zahid Hussain, Imran Ashraf, Gyu Sang Choi,"Adaptable Reduced-Complexity Approach Based on State Vector Machine for Identification of Criminal Activist on Social Media," in IEEE, pp. 2021

[11]. Vaishali B, Dr. S.John Justin Thangaraj, "Innovative Facial Expression Identification for Criminal Identification using Unsupervised Machine Learning and Compare the Accuracy with CNN Classifiers," in International Conference on Business Analytics for Technology and Security (ICBATS), pp. 2022.

[12]. Yimin Yang, Zhaochong Wang, Zongshen Jiang, "An Improved Tri-training based Named Entity Identification Approach for Legal Knowledgebase of Properties Involved in Criminal Cases," in 7th Annual International Conference on Network and Information Systems for Computers (ICNISC), pp. 2021.

[13]. Gurlove Singh, Amit Kumar Goel, "Face Detection and Recognition System using Digital Image Processing," in Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020) IEEE Xplore, pp. 2020.

[14]. S. Ayyappan, Dr. S. Matilda, "Criminals and Missing Children Identification Using Face Recognition and Web Scrapping," in IEEE, pp. 2020

[15]. Ghazvini, A., Abdullah, S. N. H. S., Hasan, M. K., & Kasim, D. Z. A. B. (2020). Crime spatiotemporal prediction with fused objective function in time delay neural network. IEEE Access, 8, 115167-115183.

[16]. Apoorva.P, Impana.H.C, Siri.S.L, Varshitha.M.R, Ramesh.B." Adoptability of Open-Source Face Recognition (FR) on Automated Criminal Identification System for Law Enforcement in the Philippines: A Systematic Review" in IEEE in Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019) IEEE Xplore, pp. 2019

[17]. Apoorva.P, Impana.H.C, Siri.S.L, Varshitha.M.R, Ramesh.B, " Automated Criminal Identification By Face Recognition Using Open Computer Vision Classifiers," in Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019) IEEE Xplore, pp. 2019.

[18]. Kavushica Rasanayagam, Kumarasiri

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1950- 1957
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0267

S.D.D.C, Tharuka W.A.D.D., Samaranayake N. T, Dr.Pradeepa Samarasinghe, Samanthi E.R. Siriwardana, "CIS: An Automated Criminal Identification System," in IEEE, pp. 2018.

[19]. Arfika Nurhudatiana, Adams Wai-Kin Kong, "On Criminal Identification in Color Skin Images Using Skin Marks (RPPVSM) and Fusion with Inferred Vein Patterns," in IEEE Transactions on Information Forensics and Security, pp. 2015.

[20]. Anil K. Jain and Brendan Klare, "Matching Forensic Sketches and Mug Shots to Apprehend Criminals," in IEEE Computer Society, pp. 2011.