Leveraging Facial Recognition Technology in Criminal Identification

Arjun Menon, Kumari Shivani Singh, Raushan Kumar, Ritvik Sethi, Abha Kiran Rajpoot

Sharda University, Greater Noida, India

arjunmnn7@gmail.com, *kumarishivanisingh14@gmail.com*, *raushankumar606@gmail.com*, *ritviksethi56@gmail.com*, *abhakiran.rajpoot@sharda.ac.in*

Abstract

Detecting and identifying a criminal is a time-consuming and complex task. Criminals have become more astute in recent years, leaving no genetic evidence or fingerprint traces at the crime site. Using state-of-the-art facial identification technology is a quick and simple option. Surveillance cameras are being deployed at most buildings and traffic signals for monitoring reasons, thanks to advancements in security technology. Perpetrators, offenders, runaways, and lost individuals can all be identified using the camera's video recordings. This article aims to provide a brief survey of current improvements in face recognition, as well as a complete overview of several approaches to incorporating face detection in criminal identification based on various application scenarios. We also look at the evolution of facial recognition and where it is now in this study. It gives an overview of the internal architecture of a typical face detection system. It also highlights the obstacles that will be faced in instilling facial recognition as well as approaches to improve it while taking various trade-offs into account. It also identifies areas for future research in the incorporation of facial identification in a variety of sectors.

Keywords. Machine Learning, face recognition, neural networks, criminal identification, CCTV.

1. INTRODUCTION

Finding a criminal has proven to be a challenging task over the years. Previously, the whole approach was predicated on leads derived from evidence discovered at the incident site. Genetic evidence is simple to locate. Perpetrators, on the other hand, have developed and are now more skilled than ever at hiding their tracks and avoiding leaving any detectable trace. Facial recognition and surveillance are used in this case. The face is vital for social identity because each face is distinct owing to its distinctive features. Facial recognition for crime detection is a one-of-a-kind bio - metric approach that boasts excellent accuracy while being minimally invasive. It's a technique for naturally recognizing and checking an individual's distinguishing proof from video groupings or photographs utilizing the individual's face. The facial recognition system described in this article is a unique blend of the best facial recognition, classification, and feature extraction algorithms currently

available. MTCNN for recognition and FaceNet for embeddings have already been shown to be effective and state-of-the-art deep learning approaches.

Automated facial recognition is a technique in which a computer extracts important facial characteristics like the width of the nose or jawline, the space between both the eyes, the colour of the eyes, and so on. These traits come in handy when it comes to categorization and record matching. In this system, there are two important processes: detection and recognition. Facial recognition sets in motion two primary processes: training and assessment. The algorithm is fed a sample of pictures model trained on the training set. The facial recognition assessment phase compares the freshly obtained test image to the database [1].

The face is a crucial aspect of humans that reveals their distinct character, feelings, and age, as well as allowing for social interaction [2]. In recent years, biometric-based technologies, such as face recognition, have surfaced as being the most effective and reliable means of recognizing faces. Biometrics is a field that looks at a person's natural characteristics that are specific to the person, and this knowledge gathered might be beneficial in identification of a person [3]. While it is possible for individuals to deny the truth, biometric technologies – that is, inherent biological attributes such as fingerprints, faces and eyes – are relatively more reliable and incredibly hard to thieve since "the body never lies," and changing biometric features is incredibly challenging [4].

2. LITERATURE REVIEW

Nurul et al. [5] use CCTV video and compare the photos from the film with a police database if they don't uncover any fingerprints from the crime site. This technique is divided into five parts, the first of which is planning, wherein the why and how of the technique are examined. The prerequisite to design the system was considered in the second step of requirement analysis. The third step was design, in which they specified the system's workflow. The system is developed and tested using the Principal Component Analysis (PCA) Algorithm in the fourth and last significant stage. Maintenance is the final stage; this phase was skipped because the system was built in a controlled setting. The authors employed the PCA Technique to detect comparable features of photos accessible in the database with acquired images of CCTV for identifying criminals. The system will access a database containing the person's details in order to show the person's information if FRCI recognizes a face. Visual Studio Code is used to create the system interface, while MATLAB R2013b is used for database and code. Using the suggested approach, they were able to attain an accuracy of 80%.

Apoorva et al. [6] employed four phases, the first of which is real-time training using images, and the second of which is face identification using a Haar-classifier. The matching of surveillance camera captured photos with real-time images is the third phase, followed by the outcome section based on the comparison. For face detection, the authors use a Haar-classifier in OpenCV; Haar-cascading is one of the techniques for facial recognition. This algorithm

recognises many people and may be used to locate the suspects we're looking for. In comparison to the existing model, the suggested system has a very high accuracy. They also assured us that by using our Adhar database, we would be able to quickly identify Indians

and foreigners, as well as determine whether or not a person is a perpetrator. We may apply this approach by utilising the currently existing citizen database.

Rupali et al. [7] utilised the database containing passport information to determine if the passenger was an authorised passport holder. They're doing this with computer vision techniques and LBPH statistical models. For airport security purposes, this approach consists of six steps. First, capture a picture using a camera. Second, send the image to the Django server. Third, extract the LBPH feature set from the picture. Fourth, compare the image to a database using a classifier. Fifth, If a match is found, retrieve the user's information from the database. Lastly, email the user's predicted information to the administrator. They process LBPH pictures with webcam photos before applying classifiers and compare them to database images. This will also aid in catching offenders who travel from one nation to another, as well as detecting if the passenger has taken a bank loan, in which case the passenger's comprehensive information will be submitted to the police precinct for authentication.

Mohanty et al. [8] developed a web-based tool called Photo Sleuthing to identify soldiers from the American Civil War, which took place between 1861 and 1865. They said that locating a needle in a haystack is akin to this identifying mechanism. It contains a haystack structure, a narrowed haystack, and a needle in the haystack is found. Using a combination of automatic facial recognition and human knowledge, the team is able to complete their work. When the approach was first introduced, it assisted in the identification of unknown pictures, and the authors highlighted the ramifications for person identification pipelines. They demonstrate how the Photo Sleuthing pipeline has assisted in the identification of thousands of previously unknown photos while also encouraging long-term voluntary participation. Pate et al. [9] published an article in 2016 in which they employed the LEM method for facial identification to locate disappeared persons. The system’s productivity was 85 percent. Muyambo developed a face identification system in his work [10] in 2018 to discover missing individuals in Zimbabwe, which employed the LBPH approach to identify faces. The suggested technique achieved a 67.5 percent facial recognition rate. The LBPH algorithm is not affected by changes in brightness. Qasim et al. [11] have demonstrated a quick algorithm-based facial recognition system. Two datasets are used in this model: Unrestricted Facial Images (UFI) and Olivetti Research Laboratory (ORL). ORL comprises four hundred 92X92 pixel pictures, nine of which are used for training and one image is used for assessing each person. UFI has four hundred and one 128X128 pixel pictures, seven of which are utilized for training and one for assessing each individual. The captured picture is transformed to the HSV format, and then force field characteristics are retrieved. The three distance approaches used for classification are Manhattan, Euclidean, and Cosine. They obtained the best resolution and 99.9% accuracy for the datasets ORL and UFI by comparing these approaches.

A similar investigation of existing work by various creators has been summarised in Table 1.

Table 1. A comparative summary of existing related surveys.

Reference	Contribution
Nurul et al. [5]	Used CCTV footage to identify felons if fingerprints are not available and achieved 80% accuracy.
Apoorva et al. [6]	Used Haar-classifier in OpenCV for facial identification. This technology is capable of detecting many people.
Umbare et al. [7]	Used the passport database to determine whether or not the passenger was a verified passport holder.
Mohanty et al. [12]	Developed Photo Sleuthing to identify unknown portraits.
Pate et al. [13]	Used LEM method for face recognition to locate disappeared persons.
Muyambo et al. [14]	Used LBPH method to track down disappeared individuals in Zimbabwe. The LBPH algorithm is not affected by changes in brightness.
Qasim et al. [15]	Developed an algorithm that achieved an accuracy of 99%.

3. BASICS OF FACIAL RECOGNITION

Facial identification is a method for perceiving or approving a singular's ID by looking at their face. Facial acknowledgment programming can distinguish people in photos and recordings continuously. Police officials might use cell phones to distinguish people. Face identification softwares uses techniques to identify particular, distinguishing features on a being's face. These elements, for example, eye distance or jawline shape, are then changed into a numerical model and investigated with information from different countenances in a facial ID data set. The information about a specific face is in many cases called a face layout and is unmistakable from a photo since it's intended to recognize one face from multiple faces by just incorporating specific subtleties.

3.1. History of Facial Recognition

Facial recognition applications have been emerging since the 1960s, according to [12], which invented the idea of utilising a RAND tablet to coordinate facial characteristics. A gadget called as a RAND tablet was used because it gave the feature to input coordinates using a stylus. The stylus transmitted electromagnetic signals. RAND tablet was used to physically record the coordinates of nose, hair, eyes, mouth etc. facial features.

Goldstein et al. [13] took facial identification to a different level by using 22 specific facial traits such as hair colour, chin, nose elevation, skin colour, and so on. A vast amount of data on the human-assigned values of human faces was acquired. The original 34 features were

whittled down to 22 for which the data is reliable and consistent in terms of the participants who allotted the evaluation metrics. [14] & [15] introduced the world to eigenfaces and statistical techniques to face recognition in the late 1980s. Eigenfaces decrease dimensionality by projecting a sample/training data onto tiny feature faces using Eigenvalues and Eigenvectors. Principal Component Analysis is based on this concept (PCA). Face recognition was used for law enforcement for the first time in 2002. Since then, criminal identification has grown in importance as a facial identification application. [16] Creates a criminal identification system called "FRCI" using the dimensionality reduction approach Principal component analysis. The Haar-Features approach is used in [17], [18], and [19], as mentioned in [20]. The recognition time-frame in a Haar highlights framework is comprised of strong square shapes at the areas of specific elements. In a detection window at a certain position, a Haar-like feature evaluates neighbouring rectangular sections. Adriana et al. suggested a method in [21] that employs eighteen aspects, one of which being RGB, which is used in [22]. Le et al. [23] discusses the use of AdaBoost and ANN together to develop a hybrid model "ABANN" after neural networks became effective in dealing with computer vision tasks like facial identification in 2010. Many deep learning models have been used particularly for facial identification.

Table 2. History of Facial Recognition.

Year	Brief History
1960	Bledsoe coined the approach of using a RAND tablet for coordinating features on the face.
1971	Goldstein, Harmon and Lesk used 22 special facial features like the colour of hair, chin, nose elevation, skin colour etc.
1987	Sirovich and Kirby introduced the world to eigenfaces and statistical approaches to face recognition.
2001	For quick object identification, Viola and Jones employed a boosted cascade of basic characteristics.
2011	Le explains the usage of AdaBoost and ANN together to create a hybrid model "ABANN"
2015	Adriana Kovashka, Margaret Martonosi proposed a system which uses 18 features, one of them being RGB.
2017	Abdullah, Saidi and Rehman used dimensionality reduction technique Principal component analysis for creating a criminal identification system known as "FRCI"

3.2. Workflow of facial recognition system

Figure 1 depicts the fundamental stages required in face identification, which are discussed below:

- Taking an image: The picture that is taken is known as the test picture. With or without the subject's awareness, a closed-circuit camera might be used to capture the image.
- Face detection: The subject's features are detected from the whole picture collected in this stage.
- Features extraction: In this stage, the particular and unique features of the identified face are extracted in for the matching process between them with the matching photographs in this dataset.
- Matching: The resultant image is compared to the database pictures.
- Verification/identification: The final stage is to recognize the individual. A 1:N and 1:1 match is made for identification and verification respectively.

In face-acknowledgment frameworks, the distinguishing proof of the individual is the concluding phase after face recognition, and face to face matching is utilized to work with individual discerning. A face-recognition system was presented in one research as a way to identify a person. The technology worked by communicating between a stationary server and a mobile device, and it had a 95 percent accuracy rate. For the face detection identification, OpenCV Library techniques were employed. The face-detection skills of the utilised recognition algorithms are used to identify people.

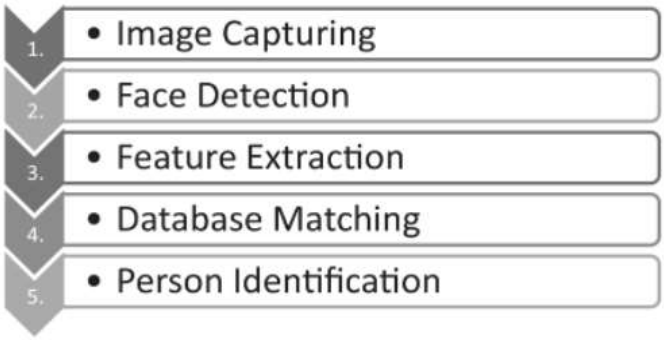

Figure 1. Workflow of facial identification.

4. APPLYING MTCNN AND FACENET FOR FACIAL RECOGNITION

To create a reliable facial recognition system, several strategies for detection, embedding, and recognition must be applied one after the other.

A. Multi-task Cascaded Convolutional Networks (MTCNN) - MTCNN demonstrates a method for detecting and aligning faces in photographs. It comprises a three-part CNN that can distinguish facial landmarks such as the nose, forehead, and eyes. MTCNN is divided into three phases. The image is first enlarged to build a pyramid of images so that detection for all sizes may be done, and then it is processed through a neural network known as P Net,

which outputs face coordinates and bounding box. Faces that are only partially visible are handled within the second step, and bounding boxes are produced using an R net. The P and R net results are quite close. In the third and final stage, an O net is used to provide three outputs: coordinates, landmarks on the face, and bounding box confidence levels. After each step, bounding boxes with low confidence are removed using a non-max suppression approach.

B. FaceNet - FaceNet was introduced in 2015 by a group of Google researchers. The job of face recognition, verification, and clustering was dealt with separately. FaceNet achieves very accurate results by using neural networks and a "triple loss function." The identified face is fed into the model, and the result is a face embedding, which is a vector with 128 components that reflect unique features in this face. A triplet loss function was utilised to train the deep CNN. It's based on the idea that feature vectors of similar faces are more similar than feature vectors of dissimilar faces. Machine learning techniques such as k-NN and SVM can be utilised for identification once the embeddings have been simplified.

4.1. Applying facial recognition in criminal identification

Criminal identification is the most vital responsibility for officers searching for criminals, but it is also the most complex and time-consuming because they must look for it everywhere. It will be more challenging in densely populated cities or public spaces. In certain circumstances, manual identification allows for the gathering of additional information about offenders. As a result, this study develops an automated criminal recognition system that detects offenders' faces. This will aid police in identifying and apprehending offenders in public areas. There are two methods for identifying criminals. Police personnel searching them in public locations use the Manual Identification System (MIS) to identify them. It takes a long time to offer sufficient attention, and it also has the potential to miss criminals since they will be warned by noticing officers and quickly flee the scene. Because the MIS is taking longer than expected, we will not be able to adequately pivot on every being. Talking about an automatic identification system (AIS), however, public inspection is not required. All of the processes in this system are automated here. The following are some key features of an automated criminal recognition surveillance system:

1. Criminal Enrolment: Criminal photographs with names attached to them are put to the criminal database so that the collected images may be compared to those in the database.
2. CCTV Interconnectivity: Cameras should be linked to the system that houses a criminal database and the application that runs on it.
3. Criminal Confirmation: If a person is located in a public location using this method, the criminal database may be used to determine who the culprit was.

4.2. Future scope of facial recognition in crime

Through the use of CCTV cameras located in several locations, an elegant face identification system may be automated to identify thieves. This technique may also be used to locate missing persons after natural disasters and other mishaps. This method may be enhanced to recognise many faces at once and to recognise faces in hazy or cropped photos. A criminal recognition system can also provide information about where the offender was seen utilising

camera locations. To offer extra facts about the offender, the database can include additional details such as age, crimes committed, linked persons last seen, and so on.

5. CONCLUSION

This article tackles the difficulty of using face recognition to detect criminals, which is a significant issue. In terms of data integrity, security, and traceability, traditional criminal identification has a number of flaws. Facial recognition automates the process, and it overcomes all of the disadvantages of traditional criminal identification. Because artificial intelligence powers face recognition technology, it may deliver outstanding results in detecting criminals. Even with the fact that most individuals strive to conceal their identities when engaging in illegal conduct by disguising their faces or covering their identities with scarves, masks, or other means. In these situations, AI uses deep learning techniques to identify the individual. Especially in comparison to other criminal systems such as biometrics or DNA, which require the criminal to leave a physical trace, facial identification may be able to issue a prompt more quickly (both in terms of detection and analysis of various image sources), making an increasing number of police departments around the world to adopt it.

REFERENCES

[1] P. M. and C. Iancu, "Automatic Face Recognition System for Hidden Markov Model Techniques," New Approaches to Characterization and Recognition of Faces, Aug. 2011, doi: 10.5772/17694.

[2] A. K. Agrawal and Y. N. Singh, "Evaluation of Face Recognition Methods in Unconstrained Environments," Procedia Computer Science, vol. 48, pp. 644–651, 2015, doi: 10.1016/j.procs.2015.04.147.

[3] R. Jafri and H. R. Arabnia, "A Survey of Face Recognition Techniques," Journal of Information Processing Systems, vol. 5, no. 2, pp. 41–68, Jun. 2009, doi: 10.3745/jips.2009.5.2.041.

[4] L. Introna and H. Nissenbaum, "Facial Recognition Technology A Survey of Policy and Implementation Issues," eprints.lancs.ac.uk, 2010. https://eprints.lancs.ac.uk/id/eprint/49012 (accessed Sep. 17, 2022).

[5] N. A. Abdullah, Md. J. Saidi, N. H. A. Rahman, C. C. Wen, and I. R. A. Hamid, "Face recognition for criminal identification: An implementation of principal component analysis for face recognition," 2017, doi: 10.1063/1.5005335.

[6] Apoorva P, Impana HC, Siri SL, Varshitha MR, Ramesh B. Automated criminal identification by face recognition using open computer vision classifiers. In2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) 2019 Mar 27 (pp. 775-778). IEEE.

[7] Umbare, Janhavi, Yadav, Pruthvi. 2020. Airport security using face-recognition. International Journal of Future Generation Communication and Networking. vol. 13, No. 3.

[8] Mohanty, Thames, Mehta, and Luther. 2019. Photo Sleuth: Combining Human Expertise and Face Recognition to Identify Historical Portraits. Conference: the 24th International Conference.

[9] Sumeet Pate. 2016. Robust Face Recognition System for E-Crime Alert. In International Journal for Research in Engineering Application and Management, Issue 1.

[10] Muyambo. 2018. An Investigation on the Use of LBPH Algorithm for Face Recognition to Find Missing People in Zimbabwe, International Journal Of Engineering Research & Technology (IJERT) Volume 07, Issue 07 (July 2018)

[11] Kian and Sara, "Force Field Feature Extraction Using Fast Algorithm for Face Recognition Performance", Iraqi Syndicate International Conference for Pure and Applied Sciences.

[12] Bledsoe.1960. Manual measurements.

[13] A.J. Goldstein, L.D. Harmon and A.B. Lesk, "Identification of human faces,"in proceedings of the IEEE, vol 59, pp. 748-760, May 1971.

[14] L.Sirovich and M.Kirby, "Low dimensional procedure for the characterisation of human faces," in Journal of the Optical Society of America A, vol 4, pp. 519-524, 1987.

[15] M. Turk and A. Pentland, "Eigenfaces for Recognition," in Journal of cognitive neuroscience, vol 3, pp. 71-86, Jan 1991.

[16] N. A. Abdullah, Md. J. Saidi, N. H. A. Rahman, C. C. Wen, and I. R. A. Hamid, "Face recognition for criminal Identification: An implementation of principal component analysis for face recognition," AIP Conference Proceedings 1891:1, Oct 2017.

[17] P. Kakkar and V. Sharma, "Criminal identification system using face detection and recognition," in International Journal of Advanced Research in Computer and Communication Engineering, vol 7, pp. 238-243, March 2018

[18] P.Apoorva, H.C. Impana, S.L. Siri., M.R.Varshitha and B.Ramesh, "Automated criminal identification by face recognition using open computer vision classifiers, " in 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 775- 778, 2019

[19] P. Chhoriya, "Automated criminal identification system using face detection and recognition", in International Research Journal of Engineering and Technology (IRJET) , vol 6, pp. 910-914, Oct 2019.

[20] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Computer Vision And Pattern Recognition, vol 1,pp. 511-519, Feb 2001.

[21] A. Kovashka and M. Martonosi, "Feature-based face recognition for identification of criminals vs. identification for cashless purchase".

[22] A. Chevelwalla, A. Gurav, S. Desai and S. Sadhukhan, "Criminal face recognition system," in International Journal Of Engineering Research & Technology (IJERT), vol 4, pp. 47-50, March 2015

[23] T. H. Le. 2011. Applying artificial neural networks for face recognition. Hindawi Publishing Corporation Advances in Artificial Neural Systems, vol 2011, pp. 1-16, 2011

Biographies

Arjun Menon is a final year student of B.Tech Computer Science at Sharda University. Currently he is working as a software engineer intern. His areas of interest are Machine Learning, Web development and Android Development.

Kumari Shivani Singh is a final year student of B.Tech Computer Science at Sharda University. Currently she is working as a software engineer intern. Her areas of interest are Machine Learning, Web development and Android Development.

Raushan Kumar is a final year student of B.Tech Computer Science at Sharda University. Currently he is working as a software engineer intern. His areas of interest are Machine Learning, Web development and Android Development.

Ritvik Sethi is a final year student of B.Tech Computer Science at Sharda University. Currently he is working as a software engineer intern. Her areas of interest are Machine Learning, Web development and Android Development.

Abha Kiran Rajpoot is an M.tech Graduate. Currently working as an Associate Professor in the department of Computer Science and Engineering at Sharda University. Her areas of interest are wireless sensor networks, soft computing and computer networks.