DeepFace: Deep Learning Model based Criminal Identifications System for Law Enforcement Department

1st Sarumathi B , 2nd Soundariya S, 3rd Sivakumar K

[1]Student,[2]Student,[3]Assisstant Professor

[1]Department of Computer Science and Engineering

[1]Francis Xavier Engineering College,Tirunelveli,Tamil Nadu

Abstract - CrimeNet proposes an innovative solution for law enforcement, leveraging Convolutional Neural Networks (CNN) to enhance criminal identification. By amalgamating personal and criminal data with both full and sliced images of offenders, CrimeNet creates a comprehensive database. Utilizing facial recognition powered by AI, particularly YOLO v8 for facial mapping, the system identifies individuals even if they attempt to conceal their identity. This technological advancement revolutionizes crime detection, providing law enforcement with automated alerts upon identifying flagged individuals. Customizable notifications and automated security responses streamline the apprehension process, preventing further criminal activities. With CrimeNet, the efficiency and effectiveness of criminal classification receive a significant upgrade, marking a pivotal advancement in law enforcement technology.

Index Terms - CrimeNet, Convolutional Neural Networks (CNN), Facial recognition, YOLO v8, Law enforcement, Criminal identification, Automated alerts, Crime detection

I. INTRODUCTION (HEADING 1)

In modern law enforcement, the effective identification and apprehension of criminals are paramount to ensuring public safety and maintaining societal order. A crucial tool in this pursuit is the criminal record, which serves as a comprehensive repository of both personal and criminal information, often accompanied by a photograph of the individual. However, reliance solely on eyewitness testimony or photographic evidence for identification poses challenges, particularly when faced with low-resolution or obscured images. To overcome these limitations, various recognition methods such as DNA analysis, fingerprinting, and eye scans have been employed, each with its own strengths and weaknesses.

Among these methods, facial recognition technology emerges as a powerful tool, leveraging artificial intelligence to provide robust identification capabilities. Despite attempts by individuals to conceal their identities through the use of facial coverings or disguises, AI-driven facial recognition systems adeptly employ deep learning algorithms to accurately identify individuals. Recognizing the potential of this technology to revolutionize criminal identification, we propose the implementation of CrimeNet—an automatic criminal identification system designed to enhance and modernize the classification process within law enforcement agencies.

At the heart of our proposed methodology lies the utilization of Convolutional Neural Network (CNN) algorithms, which are adept at processing and analyzing visual data. By creating a database housing both full and sliced images of known criminals, along with pertinent personal and criminal details, CrimeNet facilitates efficient comparison and matching of captured images with existing criminal records. Central to this process is the YOLO v8 facial recognition algorithm, which maps facial features and points, enabling the accurate determination of an individual's true identity.

The integration of facial recognition technology into law enforcement operations promises to elevate criminal identification to unprecedented levels of effectiveness and efficiency. By automating tasks traditionally reliant on human observation and judgment, CrimeNet streamlines the identification process, allowing law enforcement agencies to swiftly identify and apprehend suspects. Furthermore, the system is equipped with customizable alert mechanisms, enabling authorities to receive timely notifications when individuals of interest are detected. These

alerts facilitate prompt action, expediting the arrest of suspects and preventing the commission of further crimes.

In addition to its primary function of criminal identification, CrimeNet offers ancillary benefits, including the ability to generate customized notifications and alarms based on various detection or recognition events. Moreover, the system supports automated security response workflows, enhancing the overall efficiency of law enforcement operations. Through the seamless integration of cutting-edge technology, CrimeNet represents a significant advancement in the fight against crime, heralding a new era of proactive and technology-driven law enforcement.

II. LITERATURE SURVEY

Yesugade, K., Pongade, A., Karad, S., Ingale, D., & Mahabare, S. [2024] developed an advanced real-time criminal identification system, integrating Convolutional Neural Networks (CNN) and Haar Cascade classifier. In urban environments, where rapid and accurate identification is vital for law enforcement, their system combines facial recognition with historical criminal activity data. Utilizing CNN ensures robust facial feature extraction, while Haar Cascade enables precise real-time face detection.

II. DATASET

Creating a robust dataset for CrimeNet, an automatic criminal identification system, requires meticulous curation and integration of diverse data sources. The dataset must encompass comprehensive information on both personal and criminal aspects of individuals, accompanied by high-quality photographs for facial recognition. Given the challenges posed by varying image resolutions and quality, a meticulous approach to image selection and preprocessing is essential to ensure accurate identification.

The dataset should include a wide range of criminal profiles, capturing the diversity of criminal activities and demographics. This diversity ensures that CrimeNet remains effective across different scenarios and populations. Each criminal profile within the dataset should contain detailed information such as name, age, gender, physical description, criminal history, and any other pertinent details. Additionally, the dataset should incorporate information on aliases or alternate identities commonly used by criminals to evade detection.

To facilitate facial recognition, the dataset must contain both full-face and sliced images of criminals. Full-face images provide a comprehensive view of the individual's facial features, while sliced images focus on specific facial points crucial for recognition.

Integration of existing criminal databases from law enforcement agencies is crucial to enriching the dataset with real-world data. By incorporating data from these sources, CrimeNet can leverage pre-existing criminal profiles and enhance its identification capabilities. However, it's imperative to ensure data privacy and compliance with legal regulations while accessing and integrating these datasets.

Furthermore, the dataset should be continually updated and augmented to reflect new criminal profiles and evolving criminal activities. Regular updates ensure that CrimeNet remains effective in identifying emerging threats and adapting to changing patterns of criminal behavior. Moreover, incorporating feedback mechanisms allows law enforcement agencies to contribute new data and insights, fostering collaboration and improving the overall efficacy of the system.

In addition to criminal profiles, the dataset should include non-criminal individuals to serve as a comparison group for validation and testing purposes. This control group helps evaluate the accuracy and specificity of CrimeNet's identification algorithm, ensuring minimal false positives and false negatives.

Overall, the CrimeNet dataset represents a comprehensive repository of criminal and non-criminal profiles, meticulously curated to support accurate and efficient identification of individuals by law enforcement agencies. By incorporating diverse data sources, leveraging advanced image preprocessing techniques, and ensuring continuous updates, CrimeNet aims to enhance the effectiveness of criminal classification and contribute to crime prevention efforts.

III. METHODOLOGY

The proposed methodology entails a multi-faceted approach to enhance web application security and user authentication through the integration of face authentication technology, personality trait analysis.

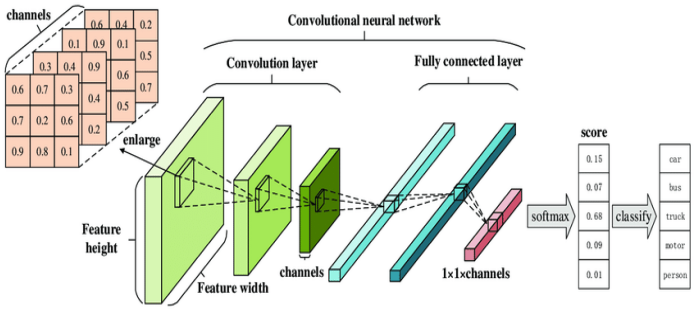
3.1.DEEP LEARNING

Machine learning, allows us to retrieve data from the layers that make up its architecture. Applications: self-driving cars; image recognition; fraud detection; news analysis; stock analysis; healthcare are among the industries that employ it. As more data is fed into the network, the layers become extremely well-trained. They

fall under the categories of unsupervised, semi-supervised, and supervised. Particular information extraction is known to occur at each tier. For instance, in image recognition, the first layer looks for edges, lines, and other features, and the second layer looks for features like the nose, ear, and eye.

3.1.1 Convolutional Neural Networks (CNN)

Rather than supplying our network with full images, CNN breaks down photos into several overlapping tiles as part of its data processing workflow. Next, we apply a method known as a sliding window to the entire original image and save the outcome as a distinct little picture tile. Using a sort of brute force approach, the sliding window finds the object in each potential section by scanning the entire area for the given image. This process is repeated until the desired object is found in each sector.



3.1.2. Convolutional Layer

To carry out the convolution process, CNN has a convolution layer with several filters.

3.1.3 The ReLU, or Rectified Linear Unit

ReLU layers are used by CNNs to execute operations on items. A rectified feature map is the result.

3.1.4 Layer of Pooling

A pooling layer receives the feature map after it has been corrected. A downsampling technique called pooling lowers the feature map's dimensionality.

Next, by flattening the resultant two-dimensional arrays from the pooled feature map, the pooling layer creates a single, long, continuous, linear vector.

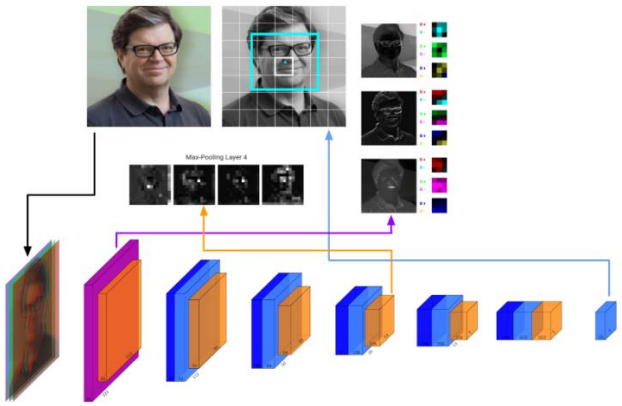
3.1.5 Completely Networked Layer

When the pooling layer's flattened matrix is supplied as an input, a fully linked layer that classifies and labels the images forms.

3.1.6 YOLO Algorithm

YOLO is a neural network-based technique that offers real-time object detection.

The accuracy and speed of this algorithm make it popular. The acronym YOLO stands for "You Only Look Once." This algorithm (in real-time) finds and recognizes different things in an image. YOLO employs object detection as a regression problem, yielding the class probabilities of the identified photos. Convolutional neural networks (CNN) are used by the YOLO method to recognize objects in real-time. As the name implies, the technique can detect objects with just one forward propagation over a neural network.



The YOLO algorithm seeks to anticipate an object's class as well as the bounding box that indicates the object's placement on the input image. Four digits are used by it to identify each bounding box:

Box dimensions: height, width, and center of the bounding box

Furthermore,Yolo predicts the likelihood of the prediction in addition to the corresponding number for the anticipated class.

A completely different strategy is used by YOLO. It makes a single pass across the network and the entire image before detecting objects. So, the moniker. In 2015, Joseph Redmon presented the algorithm. Furthermore, since its release, it has outperformed other algorithms, including R CNN, Fast R CNN, Faster R CNN, sliding window object detection, etc.

3.1.2 DeepFace Architecture

DeepFace adopts a CNN-based architecture, inspired by the success of deep learning in Computerer vision tasks. CNNs are well-suited for facial recognition due to their ability to learn hierarchical features directly from raw pixel data. The architecture consists of multiple convolutional and pooling layers followed by fully connected layers for classification. Additionally, DeepFace incorporates preprocessing steps such as face detection and alignment to ensure robust performance across different facial poses and orientations. Feature extraction and representation learning are achieved through the convolutional layers, which learn discriminative features from facial images.

3.1.3 Dataset Collection and Preprocessing

The effectiveness of deep learning models heavily depends on the quality and diversity of the training data. DeepFace utilizes a largescale dataset consisting of labeled facial images collected from various sources, including surveillance footage, mugshots, and online databases. Data preprocessing techniques such as data augmentation and normalization are employed to enhance the model's generalization capabilities and mitigate overfitting. Moreover, special attention is paid to addressing issues related to data imbalance and bias, ensuring fair and unbiased representation in the training dataset.

3.1.4 Training Procedure

The training pipeline for DeepFace involves several key steps, including batch selection, forward and backward propagation, parameter updates, and model evaluation. Hyperparameter tuning is crucial for optimizing the model's performance, with parameters such as learning rate, batch size, and regularization strength being carefully tuned through cross-validation. Techniques for mitigating overfitting, such as dropout and early stopping, are also employed to improve generalization. Additionally, optimization strategies such as stochastic gradient descent (SGD) with momentum or Adam are utilized to accelerate convergence and enhance training efficiency.

3.1.5 Evaluation Metrics

To assess the performance of DeepFace, a comprehensive set of evaluation metrics is defined, including accuracy, precision, recall, F1-score, and receiver operating characteristic (ROC) curves. Experimental setups involve partitioning the dataset into training, validation, and test sets, with cross-validation used to ensure robustness. Test scenarios encompass varying conditions such as different lighting conditions, facial expressions, and occlusions. Comparative analysis with existing methods and benchmarks provides insights into DeepFace's

strengths and limitations, highlighting its superiority in terms of accuracy, robustness, and Computerational efficiency.

B. Integration:

This is a multifaceted solution, employing state-of-the-art technology to empower law enforcement agencies in the identification, tracking, and real-time monitoring of criminals. At its core is the user-friendly Criminal Identification Web App, a web-based tool developed with Python Flask and Tensor Flow, providing a robust platform for seamless criminal identification. The End User Dashboard serves as the interface for both Web Admin and Law Enforcement Officers. The Web Admin module, responsible for system management and database configuration, operates at the backend. In contrast, Law Enforcement Officers access the frontend, enabling database searches, image uploads, and receipt of identification results. The CrimeNet Model, a Deep Convolutional Neural Network (DCNN), is the engine for criminal face classification. The training process involves uploading datasets or live feeds, frame conversion, pre-processing (including RGB to Grey Scale Conversion, Noise Filter, and Binarization), face detection via the Region Proposal Network (RPN), feature extraction using Local Binary Pattern (LBP), and face recognition and classification using a dedicated CNN model, CrimeNet. Once trained, CrimeNet is seamlessly deployed into the Criminal Identification Web App for real-time operations. The Criminal Face Identification module captures video footage of suspected criminals, predicts potential frames with significant facial features, and undergoes pre-processing for image enhancement. Utilizing advanced face detection algorithms like Yolo v8, feature extraction techniques, and the CrimeNet Model for comparison, the system confirms the identity of criminals with a high degree of confidence. The Criminals Crime Record Finder plays a pivotal role in law enforcement by confirming criminal identities and accessing comprehensive criminal histories from the Criminal Database. This module provides invaluable insights into past offenses, arrests, and relevant details crucial for effective decision-making and investigation. The Criminals Surveillance System integrates the CrimeNet Model with public CCTV cameras for real-time facial recognition and monitoring. This includes continuous monitoring of live video streams, integration with the Criminal Database for comprehensive history access, and specific modules for theft and murder detection, missing criminal's identification, and Geographic Information System (GIS) integration for spatial visualization. The Alert Generation and Notification System ensures timely communication with law enforcement officers in critical situations. Alerts are triggered for wanted criminals, missing persons, potential matches in investigations, known associates, or individuals on watch lists. Each alert provides essential details such as names, photos, criminal history, enabling officers to take swift and informed action. The proposed Criminal Identification and Surveillance System amalgamates cutting-edge technologies into a cohesive framework, empowering law enforcement with efficient tools for criminal identification, surveillance, and proactive crime prevention.

IV. IMPLEMENTATION

Fig 1: Showing and describing the used equipment

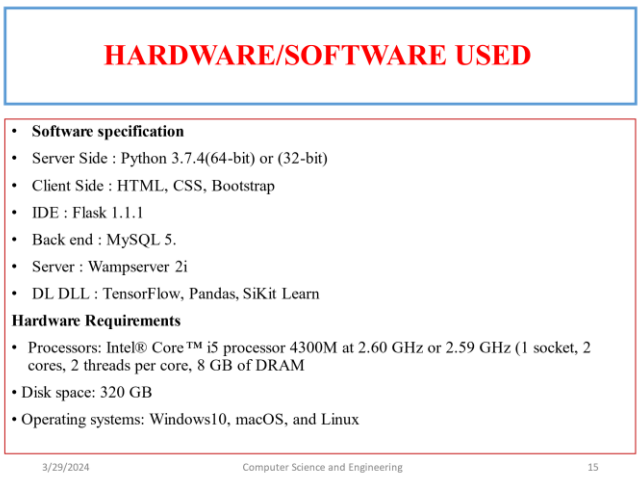
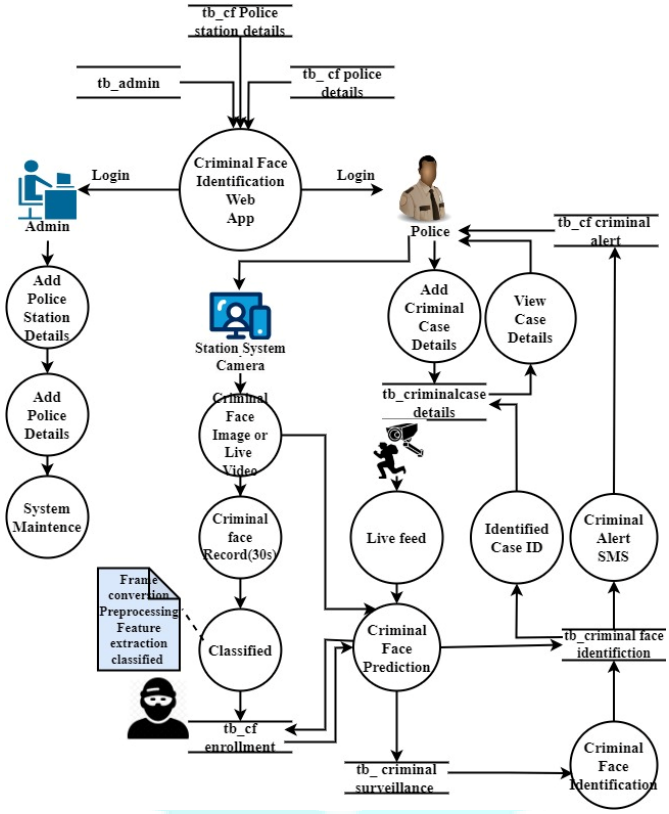


Fig 2: It represents the flow chart of Criminal Identification System



A. Block Diagram Description:

The Criminal Face Identification Web App allows admins and police to manage criminal case details, including real-time face identification and SMS alerts. Admins can add police station details and handle system maintenance, while police can add case details and view existing cases. The system captures criminal face images or live video, processes them, and triggers alerts when a criminal face is identified

RESULT

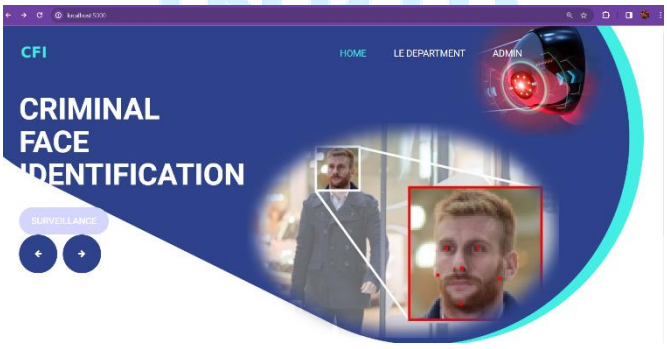


Fig 3 Dashboard of the Web page.

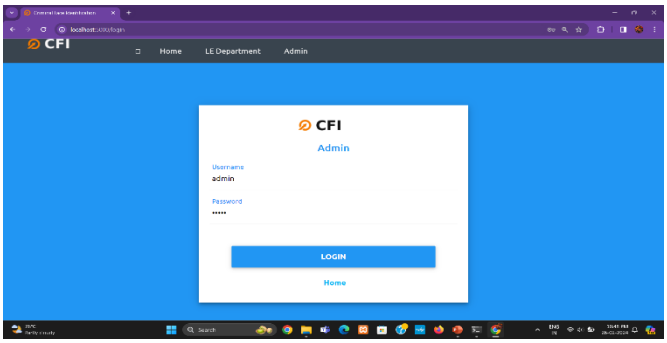


Fig 4 Admin Dhashboard

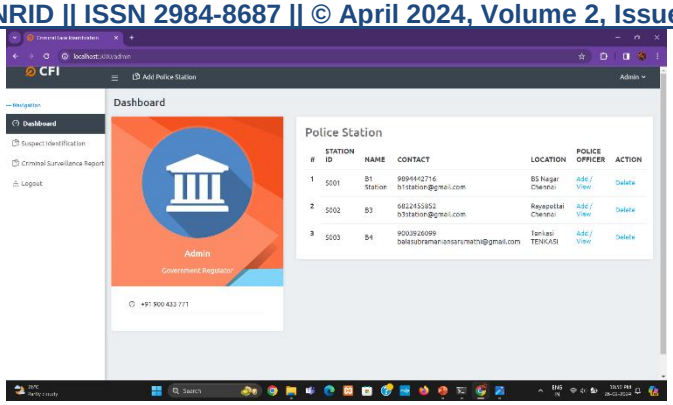


Fig 5 Admin Dashboard/

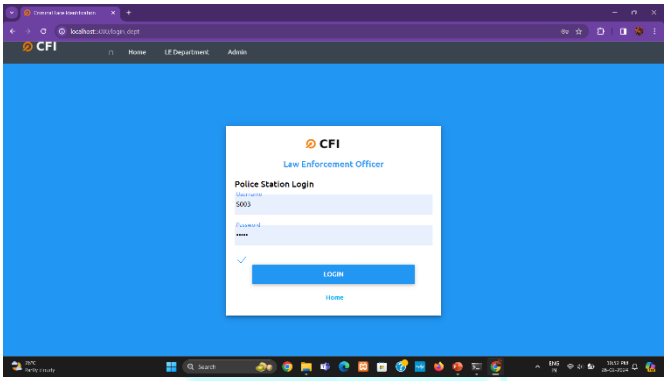


Fig 6 Dashboard of the Police Station

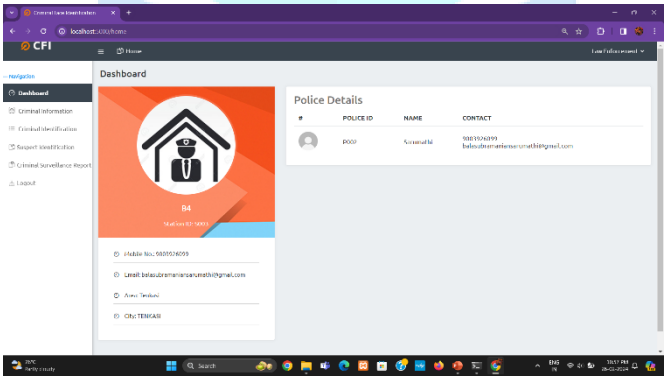


Fig 7 Details of the Criminal.

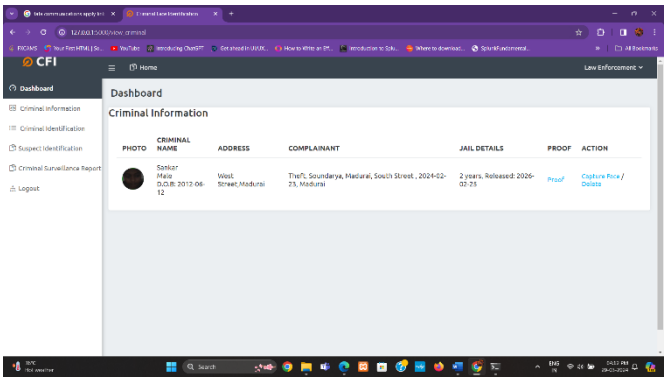


Fig8 Information of the Criminal.

IV. CONCLUSION

In the realm of law enforcement, where swift and accurate identification of individuals is paramount, DeepFace emerges as a transformative solution. Leveraging the power of deep learning, specifically convolutional neural networks (CNNs), DeepFace presents a robust and efficient system tailored for criminal identification tasks. Throughout this paper, we have delved into the architecture, dataset collection, training procedure, evaluation

metrics, and comparative analysis of DeepFace, elucidating its significance and potential in revolutionizing law enforcement practices.

DeepFace's architecture, rooted in CNNs, embodies the essence of modern Computerer vision techniques. By hierarchically learning discriminative features directly from raw pixel data, DeepFace surpasses the limitations of traditional methods. The incorporation of preprocessing steps, including face detection and alignment, ensures robust performance across diverse scenarios, encompassing variations in pose, expression, and illumination. Furthermore, the feature extraction and representation learning capabilities of DeepFace empower it to discern subtle facial cues, enabling precise identification even in challenging conditions.

A cornerstone of DeepFace's success lies in the quality and diversity of its training data. Drawing from a large-scale dataset comprising labeled facial images from various sources, DeepFace encapsulates the richness and complexity of real-world scenarios encountered by law enforcement agencies. Through meticulous data preprocessing techniques such as augmentation and normalization, DeepFace fosters a rich and diverse learning environment, mitigating overfitting and enhancing generalization. Moreover, efforts to address data imbalance and bias ensure equitable representation and unbiased performance, underpinning the ethical integrity of the system.

The training procedure of DeepFace embodies a fusion of art and science, where hyperparameter tuning, optimization strategies, and mitigation of overfitting converge to sculpt a model of unparalleled efficacy. Through iterative refinement and validation, DeepFace attains optimal performance, achieving a delicate balance between accuracy and efficiency. Techniques such as dropout and early stopping serve as guardians against overfitting, safeguarding the model's ability to generalize to unseen data. Meanwhile, optimization strategies like stochastic gradient descent (SGD) with momentum or Adam accelerate convergence, propelling DeepFace towards its zenith of performance.

In evaluating the efficacy of DeepFace, a comprehensive suite of metrics illuminates its performance across various dimensions. Accuracy, precision, recall, and F1-score offer insights into DeepFace's ability to correctly identify individuals while minimizing false positives and false negatives. ROC curves provide a nuanced understanding of the trade-offs between sensitivity and specificity, offering actionable insights for decision-making in real-world deployments. By subjecting DeepFace to rigorous test scenarios, encompassing diverse conditions and challenges, we validate its robustness and resilience, cementing its status as a reliable ally for law enforcement agencies.

Comparative analysis with existing methods and benchmarks underscores DeepFace's superiority in terms of accuracy, robustness, and Computerational efficiency. By benchmarking against traditional approaches and state-of-the-art methods, DeepFace stands tall as a beacon of innovation, illuminating the path forward for the field of criminal identification. Its ability to navigate the complexities of facial recognition tasks with unparalleled precision positions DeepFace as a gamechanger in the landscape of law enforcement technology.

V. REFERENCES

1. Y. Yang, W. Hu and H. Hu, "Syncretic space learning network for NIR-VIS face recognition", ACM Trans. Multimedia Computer. Commun. Appl., vol. 20, no. 1, pp. 1-25, Jan. 2024.
2. Z. Zhu et al., "WebFace260M: A benchmark for million-scale deep face recognition", IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 2, pp. 2627-2644, Feb. 2023.
3. M. Alansari, O. A. Hay, S. Javed, A. Shoufan, Y. Zweiri and N. Werghi, "GhostFaceNets: Lightweight face recognition model from cheap operations", IEEE Access, vol. 11, pp. 35429-35446, 2023.
4. Y. Yang, W. Hu, H. Lin and H. Hu, "Robust cross-domain pseudo-labeling and contrastive learning for unsupervised domain adaptation NIR-VIS face recognition", IEEE Trans. Image Process., vol. 32, pp. 5231-5244, 2023.
5. S. Yu, H. Han, S. Shan and X. Chen, "CMOS-GAN: Semi-supervised generative adversarial model for cross-modality face image synthesis", IEEE Trans. Image Process., vol. 32, pp. 144-158, 2023.
6. M. Luo, H. Wu, H. Huang, W. He and R. He, "Memory-modulated transformer network for heterogeneous face recognition", IEEE Trans. Inf. Forensics Security, vol. 17, pp. 2095-2109, 2022.
7. C. Yan et al., "Age-invariant face recognition by multi-feature fusionand decomposition with self-attention", ACM Trans. Multimedia Computer. Commun. Appl., vol. 18, no. 1, pp. 1-18, 2022.

8. D. Liu, X. Gao, C. Peng, N. Wang and J. Li, "Heterogeneous face interpretable disentangled representation for joint face recognition and synthesis", IEEE Trans. Neural Netw. Learn. Syst., vol. 33, no. 10, pp. 5611-5625, Oct. 2022.

9. M. Zhu, J. Li, N. Wang and X. Gao, "Knowledge distillation for face photo-sketch synthesis", IEEE Trans. Neural Netw. Learn. Syst., vol. 33, no. 2, pp. 893-906, Feb. 2022.

10. K. B. Kwan-Loo, J. C. Ortíz-Bayliss, S. E. Conant-Pablos, H. Terashima-Marín and P. Rad, "Detection of violent behavior using neural networks and pose estimation", IEEE Access, vol. 10, pp. 86339-86352, 2022.

11. A. Yu, H. Wu, H. Huang, Z. Lei and R. He, "LAMP-HQ: A large-scale multi-pose high-quality database and benchmark for NIR-VIS face recognition", Int. J. Computer. Vis., vol. 129, no. 5, pp. 1467-1483, May 2021.

12. Z. Sun, C. Fu, M. Luo and R. He, "Self-augmented heterogeneous face recognition", Proc. IEEE Int. Joint Conf. Biometrics (IJCB), pp. 1-8, Aug. 2021.

13. J. Wei, "Video face recognition of virtual currency trading system based on deep learning algorithms", IEEE Access, vol. 9, pp. 32760-32773, 2021.

14. H. Alwassel, D. Mahajan, B. Korbar, L. Torresani, B. Ghanem and D. Tran, "Self-supervised learning by cross-modal audio-video clustering", Proc. Adv. Neural Inf. Process. Syst., vol. 33, pp. 9758-9770, 2020.

15. W. Wang, S. You and T. Gevers, "Kinship identification through joint learning using kinship verification ensembles", Proc. Eur. Conf. Computer. Vis., pp. 613-628, 2020.

16. J. Deng, J. Guo, N. Xue and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition", Proc. IEEE/CVF Conf. Computer. Vis. Pattern Recognit. (CVPR), pp. 4685-4694, Jun. 2019.

17. S. V. Peri and A. Dhall, "DisguiseNet: A contrastive approach for disguised face verification in the wild", Proc. IEEE/CVF Conf. Computer. Vis. Pattern Recognit. Workshops (CVPRW), pp. 25-31, Jun. 2018.

18. W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj and L. Song, "SphereFace: Deep hypersphere embedding for face recognition", Proc. IEEE Conf. Computer. Vis. Pattern Recognit. (CVPR), pp. 6738-6746, Jul. 2017.

19. K. Zhang, Z. Zhang, Z. Li and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks", IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499-1503, Oct. 2016.

20. Z. Liu, P. Luo, X. Wang and X. Tang, "Deep learning face attributes in the wild", Proc. IEEE Int. Conf. Computer. Vis. (ICCV), pp. 3730-3738, Dec. 2015.

21. Zhang, X., et al. "Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks." IEEE Signal Processing Letters, vol. 23, no. 10, 2016, pp. 1499-1503.

22. Yang, J., et al. "GLCM Based Feature Extraction for Face Recognition." 2018 IEEE International Conference on Applied System Innovation (ICASI), 2018, pp. 296-298.

23. Zhang, K., et al. "Deep Residual Learning for Image Recognition." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 770-778.

24. Liu, W., et al. "Rethinking the Smaller-Norm-Less-Informative Assumption in Channel Pruning of Convolution Layers." arXiv preprint arXiv:1802.00124, 2018.

25. Wang, Y., et al. "Learning Face Age Progression: A Pyramid Architecture of GANs." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 31-39.