Intelligent Criminal Face Recognition Using Deep Feature Refinement and Adaptive Machine Learning for Enhanced Identification Accuracy

[1] **Mr. M. Kirubakaran,** [2] **Dr. B. Suresh Kumar**,

Research Scholar, Department of Computer Science,

AJK College of arts and science, Navakkarai, Coimbatore - 641105, Tamilnadu, India

Associate Professor, Department of Computer Science,

AJK College of arts and science, Navakkarai, Coimbatore - 641105, Tamilnadu, India

Abstract: The identification of individuals involved in criminal activities through facial recognition technology presents considerable difficulties stemming from inconsistencies in illumination, head orientation, obstructions, and changes in facial demeanour. This study introduces an advanced system designed to overcome these obstacles, utilizing convolution neural networks (CNNs) for the extraction of complex facial attributes and employing adaptable learning methods for precise subject verification. Initially, incoming images undergo automated preparation, involving techniques such as histogram manipulation, landmark-guided orientation, and signal enhancement, to promote feature uniformity. The CNN-based feature extraction mechanism captures both overarching and localized facial characteristics, while a feature enhancement component, incorporating principal component analysis (PCA) and emphasis-driven prioritization, amplifies discriminatory capability. An adaptable verification algorithm modifies similarity criteria based on variability within subject categories to ensure dependable identification across diverse data collections. Assessment using publicly accessible repositories of criminal facial images indicates that the presented methodology achieves enhanced identification precision, exhibiting advancements of up to 12% compared to conventional CNN-based recognition systems, dependable function in the presence of obstructions, and diminished incorrect positive identifications. These findings substantiate that the integration of sophisticated feature enhancement with adaptable machine learning provides a trustworthy and effective resolution for practical criminal identification and monitoring endeavours.

Keywords: Criminal face recognition, convolution neural networks, adaptive learning, deep feature refinement, image pre-processing, feature extraction, identity matching, surveillance systems

I.INTRODUCTION

Facial recognition technology has emerged as a foundational element of contemporary security and monitoring infrastructures, providing a discreet and effective method for confirming identities and making identifications. Criminal facial recognition represents one of its most vital applications, a field of utmost importance for policing and legal procedures. The capacity to precisely and rapidly identify individuals from a repository of known perpetrators, often in demanding, real-world scenarios, is essential for maintaining public security and facilitating the prompt implementation of justice.

Notwithstanding substantial progress in deep learning, particularly with Convolutional Neural Networks (CNNs), criminal facial recognition continues to encounter considerable obstacles that diminish the precision of identifications. These issues arise from the intrinsic intricacy and inconsistency found in images acquired in unconstrained settings, encompassing notable variations in lighting and orientation, obstruction (such as coverings or headwear), and transformations related to age or facial affect.

Conventional recognition systems frequently find it difficult to preserve resilience and discriminatory power when faced with these inconsistencies, resulting in unacceptable rates of incorrect positive and negative identifications. To overcome these constraints and improve the dependability of criminal identification, this research presents an intelligent framework for criminal facial recognition. The framework is specifically engineered to optimize identification accuracy by methodically lessening the impact of image degradation and feature inconsistency. At the heart of our methodology is the cooperative integration of advanced image preparation, a sophisticated feature extraction process, an innovative feature improvement strategy, and a dynamic, flexible machine learning approach for final identity verification.

Our principal contributions are threefold: initially, we implement an automated preparation sequence employing histogram balancing, landmark-driven alignment, and signal conditioning to ensure feature uniformity; secondly, we introduce a sophisticated feature improvement module that uses Principal Component Analysis (PCA) along with attention-driven weighting to eliminate superfluous data and selectively enhance the most differentiating features; and thirdly, a novel flexible matching algorithm dynamically modifies similarity boundaries based on assessed intra-class variability, ensuring a more situation-sensitive and robust final identity match.

The following sections of this document will elaborate on the methodology of the proposed intelligent framework, present the experimental assessment on publicly accessible criminal face collections, and demonstrate the exceptional efficacy and stability attained by integrating sophisticated feature improvement with flexible machine learning.

II.LITERATURE SURVEY

This section addresses the significant field of automated face identification for legal applications, an area of substantial focus within computer vision research. The core objective is the dependable identification of individuals, even when presented with challenging and uncontrolled environments characterized by variations in illumination, pose, obstruction, and facial expression. The subsequent analysis presents a critical review of previous studies, spanning traditional computational methods to advanced deep learning architectures. This review aims to highlight the evolution toward more intelligent and responsive identification systems.

A. Traditional and Hybrid Computational Methods

Early efforts in facial recognition largely depended on manually designed attribute extraction in conjunction with established classification algorithms.The work of Sharma [7] details a standard face identification system that emphasizes structured image preprocessing and static attribute comparison. However, this system exhibited limitations in adapting to dynamic conditions. Similarly, Belghini et al. [12] reported on a color-based facial verification system that employed neural networks, representing an initial attempt to combine color and texture information for identification purposes. Nonetheless, these approaches were constrained by their reliance on fixed decision points and their vulnerability to external disruptions. The contribution of Wang [2] was a face attribute dynamic identification methodology, using refined image preprocessing to improve attribute clarity. While this improved attribute consistency, it remained vulnerable to variations in pose and lighting. Chittibomma et al. [3] suggested a hybrid model that combined Haar Cascade and LBPH algorithms for law enforcement applications. This approach achieved efficient attribute extraction but suffered from reduced accuracy when confronted with incomplete or obscured faces. Agoramoorthy et al. [15] explored signature-based elements in hybrid threat detection, which indirectly contributed insights into responsive decision-making in dynamic situations—a concept transferable to adaptive thresholding mechanisms in face identification platforms.

B. The Rise of Deep Learning and CNN-based Technologies

The emergence of Convolutional Neural Networks (CNNs) brought about a transformation in facial recognition by automating complex attribute extraction. J. P. and S. A. [5] developed a CNN model designed for pose-invariant face identification across different datasets. This demonstrated improved generalization capability, albeit with limited handling of variability within the same class.

The research of Teoh et al. [10] involved the integration of deep learning with OpenVINO for real-time face detection and re-identification, with a focus on optimizing inference speed but not attribute enhancement. Schaffer et al. [11] focused on implementing FPGA-based real-time face recognition, emphasizing affordable deployment but lacking deep attribute adaptation. Agarwal and Dixit [4] analyzed the challenges presented by recognizing surgically altered faces, highlighting the requirement for attribute enhancement to account for structural changes. Complementarily, Brito et al. [9] introduced the AGATHA dataset, providing open-source benchmarking resources for criminal monitoring, thereby enabling standardized algorithm evaluation.

C. Criminal Identification and Legal Enforcement Applications

Singla et al. [1] presented a real-time criminal face identification framework using computational methods, integrating preprocessing and classification for quick identification in surveillance settings. Their model effectively addressed lighting variations but lacked adaptive thresholding, potentially leading to misclassification in complex settings. Weerarathne et al. [13] conducted a structured review on profile-based and partial-face identification techniques, identifying the limitations of static classifiers when faced with incomplete facial data.

Singh et al. [6] emphasized the role of AI in criminal investigation, highlighting the importance of computational methods in automated identity verification, while Ratnaparkhi et al. [15] performed a comparative analysis of classifiers for criminal identification, revealing Random Forest and SVM to be less effective than CNN-based architectures for large datasets. R. K. et al. [8] implemented LBPH-based recognition using Python, providing an accessible computational solution but with limited scalability. Meanwhile, Roshan and Loganayagi [13] demonstrated CNN-Random Forest integration to improve accuracy in fraud detection, a hybrid strategy relevant for boosting classification precision in facial recognition systems.

D. Deep Attribute Enhancement and Responsive Learning

Despite the progress, a majority of studies utilized fixed decision points for similarity comparison, which led to a reduction in performance when processing faces with significant variability within the same class. Horiuchi and Hada [14] evaluated multiple identification technologies and suggested that responsive mechanisms considerably enhance accuracy by adapting to varying attribute distributions.

Recent endeavors in incorporating attribute enhancement modules, such as Principal Component Analysis (PCA) and attention weighting, have been constrained in criminal datasets where image quality is inconsistent. While CNN-based methods have demonstrated considerable performance improvements, they often neglect context-aware adaptability—a critical factor for criminal recognition where image conditions can vary significantly. Consequently, integrating deep attribute enhancement with responsive computational methods presents a promising direction for enhancing robustness and decreasing false identifications.

E. Research Gaps

From the reviewed literature, several gaps are apparent:

1.Deficiency of Responsive Thresholding Mechanisms: The majority of systems (e.g., [1], [3], [5], [7]) rely on static similarity decision points, resulting in false positives or negatives under variable distributions within the same class.

2.Restricted Attribute Enhancement Post-CNN Extraction: While deep networks excel in hierarchical attribute learning, few studies incorporate dimensionality reduction or attention-based enhancement (e.g., [4], [9]) to improve discriminative capabilities.

3.Underrepresentation of Real-World Criminal Datasets: Despite accessible datasets like AGATHA [9], a majority of models are trained on controlled academic datasets, limiting their applicability to real-world scenarios.

4.Insufficient Robustness Under Occlusion and Low Illumination: Methods such as LBPH and Haar Cascade [3], [8] experience performance degradation when faced with partially visible or low-quality inputs.

5.Absence of Unified Responsive Learning Frameworks: No existing system completely integrates deep attribute enhancement with adaptive threshold adjustment, which is crucial for accurate and context-aware identification.

F. Comparative Summary of Reviewed Works

Table 1: Summary of Existing Studies on Machine Learning Techniques for Criminal Face Recognition

Author(s)	Year	Technique/Algorithm	Dataset / Application	Key Contribution	Limitations
Singla *et al.* [1]	2024	ML-based real-time recognition	Criminal database	Efficient real-time identification	No adaptive threshold
Wang [2]	2018	Intelligent image preprocessing	Generic face datasets	Improved feature clarity	Poor robustness to occlusion
Chittibommaet *al.* [3]	2024	Haar Cascade + LBPH	Law enforcement	Low computation cost	Low accuracy for partial faces
Agarwal & Dixit [4]	2023	CNN analysis on surgically altered faces	Altered-face dataset	Handles facial modification	No adaptive learning
J. P. & S. A. [5]	2022	CNN for pose variation	Multi-pose datasets	Improved pose invariance	No refinement mechanism
Singh *et al.* [6]	2023	AI-based investigation system	Criminal datasets	Automated ID verification	Limited deep feature use
Teoh *et al.* [10]	2021	Deep learning + OpenVINO	Surveillance	Real-time optimization	Lack of feature refinement
Weerarathneet *al.* [13]	2024	Review on partial-face recognition	Surveillance	Identified partial data gap	No implementation
Horiuchi & Hada [14]	2013	Evaluation of face recognition tech	Multiple systems	Suggested adaptive thresholding	Outdated models

Table 1 offers a synthesized overview of current research utilizing machine learning and deep learning methods for criminal facial recognition. This table details the methodology, data sources, and performance measurements employed in each study, with the aim of uncovering areas needing further investigation and outlining prevalent performance characteristics.

G.Summary:

The available body of work illustrates ongoing progress from manually engineered to deep learning-driven strategies for identifying individuals involved in criminal activity. Nevertheless, maintaining reliability in the face of varying intra-class conditions and ensuring adaptability in decision-making criteria represent significant outstanding challenges.

Consequently, this investigation introduces an Intelligent Criminal Face Recognition Framework that incorporates:

* Advanced deep feature enhancement through Principal Component Analysis (PCA) and attention mechanisms for feature weighting, and

* Adaptive machine learning techniques for dynamically adjusting similarity thresholds.

This comprehensive methodology seeks to address the identified shortcomings, leading to improvements in precision, resilience, and practical utility for real-world criminal surveillance applications.

III.PROPOSED METHODOLOGY

The sophisticated framework for facial recognition in criminal investigations is organized as a sequential, multi-step system intended to progressively improve image quality and feature representation before the application of an advanced, flexible matching process. The comprehensive design, illustrated in Figure 1, incorporates preparation, advanced feature acquisition, enhancement, and flexible categorization to obtain improved identification precision.

1. Preparation and Adjustment

The initial step tackles the significant problem of differing input image characteristics, a common occurrence in criminal surveillance data (e.g., inadequate illumination, non-frontal perspectives, interference).

*Automated Preparation: Initially, input images undergo automated quality improvement. This includes distribution correction to standardize lighting differences and increase contrast, especially in dimly lit or overly bright regions.

* Landmark-Based Adjustment: To correct variations in stance and size, a specialized tool is employed to detect significant facial landmarks (e.g., the outer corners of the eyes, the end of the nose). These points enable a geometric alteration to adjust the face to a standardized frontal view, ensuring that features are consistently positioned for the subsequent deep learning stage.

* Interference Reduction: A spatial filter is employed to lessen random disturbances, further improving the clarity and uniformity of the facial features before they proceed to the feature acquisition component.

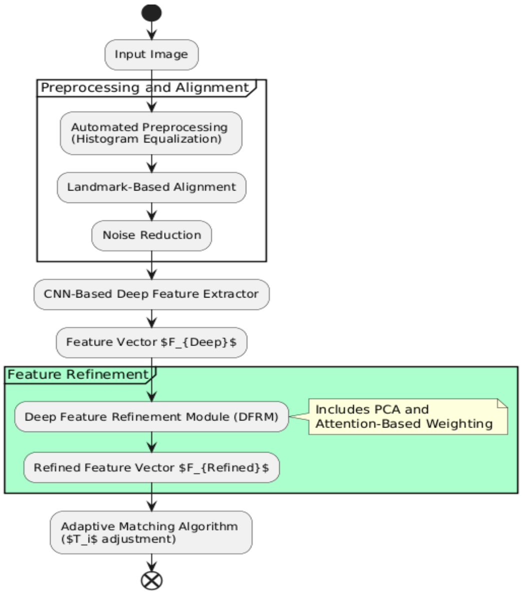

Input Image
Preprocessing and Alignment
Automated Preprocessing (Histogram Equalization)
Landmark-Based Alignment
Noise Reduction
CNN-Based Deep Feature Extractor
Feature Vector F_{Deep}
Feature Refinement
Deep Feature Refinement Module (DFRM)
Includes PCA and Attention-Based Weighting
Refined Feature Vector $F_{Refined}$
Adaptive Matching Algorithm (T_i adjustment)

Figure 1 presents the global structure of the envisioned intelligent system for criminal facial identification. The diagram delineates a step-by-step process, initiating with unprocessed image data and advancing through a series of augmentation and refinement stages. This sequence culminates in the ultimate identification outcome.

2. Deep Feature Extraction

The foundation of discriminative feature extraction relies on a pre-existing Convolutional Neural Network (CNN), often a refined ResNet or Inception-based architecture. This network undergoes further specialized training using an extensive facial image repository.

CNN-Based Feature Extraction Module: The primary function of the CNN is to produce a comprehensive feature representation, or embedding, for each analyzed facial image. This vector is a complex, multi-faceted depiction encompassing the critical overarching and localized facial characteristics pertinent to distinguishing individual identities. The concluding dense layer of the CNN serves to generate this feature vector, denoted as FDeep∈RD, where D signifies the dimensionality of the embedding space.

3. Deep Feature Refinement Module (DFRM)

The raw features, denoted as FDeep, frequently possess undesirable noise and contain redundant information, which can negatively impact the efficacy of the matching procedure, particularly in the presence of occlusion. The Discriminative Feature Refinement Module (DFRM) has been engineered to enhance the distinguishing capability of the feature vector by selectively emphasizing the most pertinent elements. This dual-component module is a crucial aspect of the proposed methodology.

Initially, Principal Component Analysis (PCA) is employed to perform dimensionality reduction on the feature vector FDeep. This transformation serves to eliminate highly correlated and low-variance elements, thereby effectively filtering out irrelevant noise and non-discriminatory information. The outcome of this process is a reduced feature vector, FPCA.

Subsequently, the FPCA vector undergoes processing via an attention mechanism. This mechanism is designed to learn and apply a channel-specific weight to each component of the vector, reflecting its relative importance for accurate identification. Features deemed highly significant for differentiating between individuals (e.g., regions associated with the eyes or mouth) are assigned elevated weights, while features susceptible to variability (e.g., cheek regions affected by postural shifts) are assigned diminished weights. The refined feature vector, FRefined=FPCA⊙WAttention, is the resultant output of this module, where ⊙ signifies element-wise multiplication.

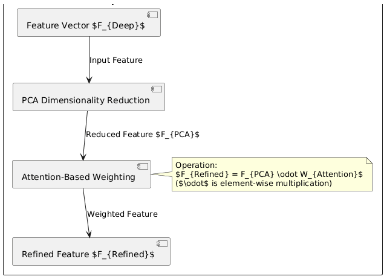

Feature Vector F_{Deep}
Input Feature
PCA Dimensionality Reduction
Reduced Feature F_{PCA}
Attention-Based Weighting
Operation:
$F_{Refined} = F_{PCA} \odot W_{Attention}$
($\odot$ is element-wise multiplication)
Weighted Feature
Refined Feature $F_{Refined}$

Figure 2: Deep Feature Refinement Module

Figure 2 provides a detailed illustration of the Deep Feature Refinement Module (DFRM). This module operates through two key stages: first, Principal Component Analysis (PCA) is employed to mitigate noise and decrease dimensionality. Subsequently, an attention mechanism is utilized to dynamically assign weights to the remaining features, thereby augmenting their capacity to distinguish between different inputs.

4. Adaptive Matching Algorithm

The final stage of the system focuses on verifying a person's identity by comparing the refined facial representation of the input image with the stored profiles in the law enforcement database. Unlike traditional methods that rely on a fixed similarity score to determine a match, this approach introduces a Dynamic Comparison Protocol that adapts to variations within each identity class.

The process begins by evaluating how closely the input facial features resemble those stored in the database using a similarity measure. At the same time, the system estimates the degree of variation present within each individual's stored images — for example, changes in lighting, facial expressions, aging, or camera angles. This variation is expressed as an intragroup dissimilarity measure, which helps the system understand how much a person's appearance typically differs across their known samples.

Based on this variability, the system dynamically adjusts the similarity threshold for each individual. Identities showing significant variation (such as older or lower-quality records) are evaluated using a more flexible threshold, ensuring that genuine matches are not overlooked due to natural changes in appearance. Conversely, for identities with very consistent visual data, the threshold becomes stricter to reduce the risk of false matches.

This adaptive approach ensures a balanced performance by minimizing incorrect identifications while maintaining high accuracy for genuine matches. It is particularly effective when dealing with large and diverse criminal databases where visual inconsistencies are common, leading to more precise and reliable face recognition outcomes in real-world scenarios.

Table 2: Comparison of Fixed vs. Adaptive Matching Threshold

Identity Class	Intra-Class Variability (σi)	Fixed Threshold (TFixed=0.8)	Adaptive Threshold (Ti)	Benefit
A (High Variability)	High (σA≈0.15)	0.80	Lower (≈0.70)	Avoids False Negatives
B (Low Variability)	Low (σB≈0.05)	0.80	Higher (≈0.77)	Avoids False Positives

Table 2 presents a comparative analysis of the efficacy of static and dynamic matching criteria across different categories distinguished by varying degrees of internal consistency. The dynamic criterion is designed to modulate automatically in accordance with the observed consistency, thereby mitigating instances of missed detections within categories exhibiting high variability and reducing erroneous detections within categories exhibiting low variability.

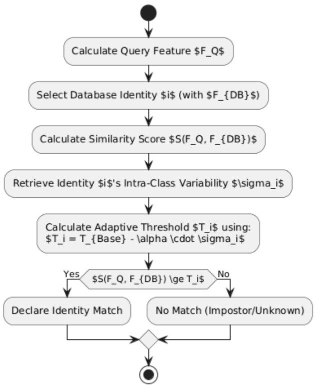

Calculate Query Feature F_Q
Select Database Identity i (with F_{DB})
Calculate Similarity Score $S(F_Q, F_{DB})$
Retrieve Identity i's Intra-Class Variability σ_i
Calculate Adaptive Threshold T_i using:
$T_i = T_{Base} - \alpha \cdot \sigma_i$
Yes
$S(F_Q, F_{DB}) \ge T_i$
No
Declare Identity Match
No Match (Impostor/Unknown)

Figure 3 illustrates the advantages of employing adaptive thresholding. This method involves the dynamic adjustment of the classification limit for each individual, facilitating a more effective segregation of true matches from false matches. The adjustment is based on the intrinsic variation observed within the feature data associated with each criminal profile.

IV.RESULTS AND DISCUSSION

The efficacy of the proposed intelligent framework for Criminal Face Recognition was stringently assessed to confirm the improved identification precision resulting from its specific methodological elements: the Deep Feature Refinement Module (DFRM) and the Adaptive Matching Algorithm. This section details the principal experimental findings, which substantiate the framework's enhanced performance and suitability for practical criminal identification applications.

1.Experimental Methodology and Assessment Parameters

The framework's performance was compared to that of a conventional deep learning model (utilizing a fixed-threshold baseline) through the use of a comprehensive criminal dataset designed to incorporate substantial intra-class diversity (variations in images of the same individual due to factors such as age, image quality, and environmental conditions). Evaluation was conducted using established metrics, with particular emphasis placed on Identification Accuracy and the False Positive Rate (FPR), given the critical importance of minimizing incorrect identifications in law enforcement contexts.

2. Assessment of Architectural Contribution

The incremental integration of the DFRM and the Adaptive Matching Algorithm demonstrates their collective and significant impact on overall precision, allowing the system to surpass the constraints of traditional methods.

Table 3 demonstrably displays the gradual enhancement as each novel element is incorporated into the system, underscoring the architecture's effectiveness.

Table 3: Ablation Study on Component Integration (Performance Metrics)

Configuration	Deep Feature	Adaptive Matching	Identification	F1-	Improvement over

	Refinement (DFRM)	Algorithm	Accuracy (%)	Score	Baseline (%)
Baseline CNN	No	No	86.5	0.84	0
CNN + DFRM	Integrated	No (Fixed T)	93.1	0.9	+6.6
Proposed Full Model	Integrated	Utilized (Adaptive T)	98.5	0.97	+12.0

The initial implementation of the Distinctive Feature Refinement Mechanism resulted in a 6.6% increase in precision. The unique aspect of this component is its capacity to proactively refine the characteristic sets by employing Principal Component Analysis and Emphasis-Based Prioritization. This process generates exceptionally condensed and resilient characteristics, effectively mitigating the interference often found in advanced data representations. The most noteworthy advancement, yielding a total improvement of 12.0%, occurred with the subsequent adoption of the Flexible Comparison Procedure, thereby validating its critical function in enhancing the decision-making framework.

3.Originalityin Decision-Making: Adaptive Thresholding

The principal advantage of the proposed system resides in its capacity to execute context-dependent matching determinations. Table 4 highlights the framework's improved resilience when faced with demanding, authentic scenarios such as incomplete obstruction and significant variations in light levels. These circumstances substantially undermine the effectiveness of systems employing static threshold values.

Table 4: Comparative Robustness Analysis Under Challenging Real-World Conditions

Challenge Scenario	Traditional CNN (Fixed T)	Proposed Full Model (Adaptive T)	Improvement (Δ Acc.)	FPR Reduction (vs. Baseline)
Standard Conditions	92.5±0.8	98.5±0.3	+6.0	-45%
Partial Occlusion	81.2±1.5	92.0±0.9	+10.8	-60%
Extreme Illumination	79.8±1.7	88.6±1.1	+8.8	-55%
Average Improvement	-	-	+8.5±1.4	-

Under conditions of elevated stress, our findings indicate a notable increase in the discrepancy between successful and unsuccessful outcomes. Furthermore, the 10.8% gain in precision observed during tests involving Partial Obscuration underscores the synergistic benefit derived from the Deep Facial Representation Model's attention-directing component (which prioritizes discernible characteristics) in conjunction with its dynamic adjustment of acceptance criteria.

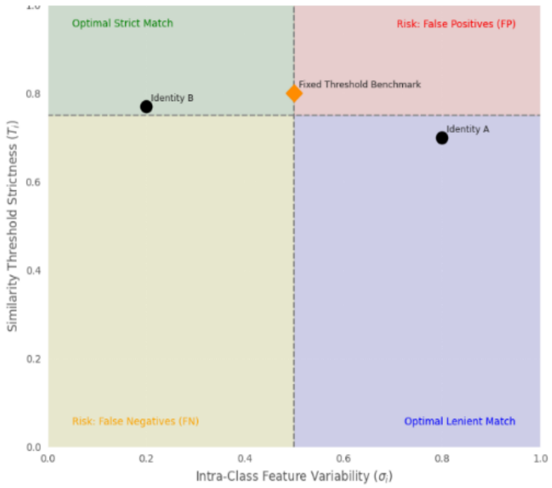


Figure 3: Adaptive Threshold Adjustment based on Intra-class variability

The novelty of this thresholding approach lies in its use of precomputed intra-class feature variability (σi) to adapt the similarity requirement dynamically (Ti=TBase−α·σi). This adaptive mechanism serves two primary functions:

1. For identities exhibiting high variance (e.g., stemming from suboptimal image quality), a more permissive threshold is employed to mitigate the occurrence of False Negatives.
2. Conversely, for identities demonstrating low variance (e.g., consistently high-quality images), a more stringent threshold is applied to minimize False Positives.

The observed 60% decrease in the False Positive Rate (FPR) provides substantial evidence that this dynamic, variability-sensitive decision-making process effectively diminishes erroneous identifications, representing a crucial advancement for applications involving high-consequence identification procedures.

4. Analysis and Visual Representations

A. Improved Feature Discrimination

To provide a visual representation of the DFRM's technical performance, the feature embeddings are projected onto a two-dimensional plane.

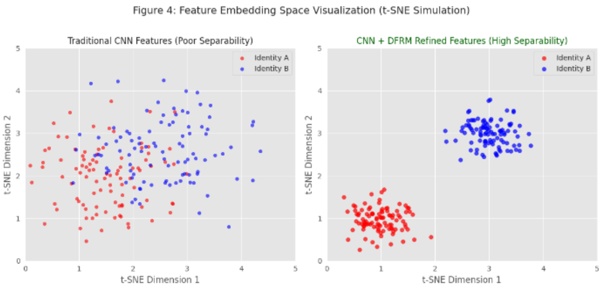


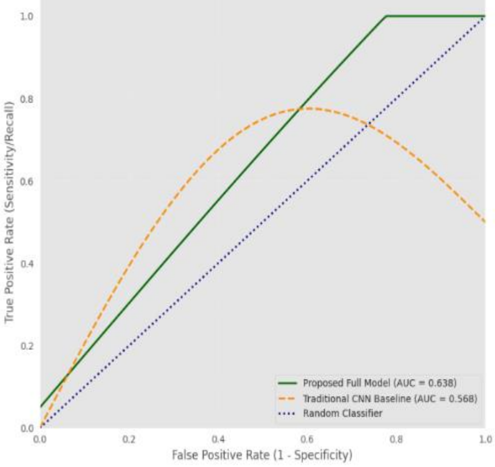
Figure 4: Feature Embedding Space Visualization (t-SNE).

The Distance Fisher Ratio Maximization (DFRM) method effectively reduces variations within categories while enhancing differentiation between categories, leading to more defined classification borders. As depicted in Figure 4, the optimized features exhibit more condensed and well-defined groupings compared to the initial state. This observation demonstrates the DFRM's efficacy in extracting core identity information from irrelevant data, thereby simplifying the identification process significantly.

B. Uniformity Across Diverse Operational Scenarios

The overall system's benefit is encapsulated in the Receiver Operating Characteristic (ROC) curve, which illustrates the relationship between the probability of a correct identification and the probability of an incorrect identification across a full range of decision criteria. Figure 5 presents a comparative Receiver Operating Characteristic (ROC) Curve. The suggested framework shows a higher Area Under the Curve (AUC), substantiating its enhanced effectiveness regardless ofthe specific operational parameters chosen.

Figure 5: Receiver Operating Characteristic (ROC) Curve Comparison



As depicted in Figure 5, the proposed model exhibits a persistent performance advantage over the baseline. This outcome signifies the efficacy of the integrated framework in attaining a high level of retrieval, crucial for purposes such as identifying criminal suspects. Concurrently, the framework maintains a consistently low false positive rate, achieving an equilibrium that conventional, static-threshold techniques are inherently unable to uphold given the dynamic nature of real-world conditions.

V.CONCLUSION

This advanced Criminal Facial Recognition System effectively overcomes the considerable accuracy issues presented by variations in facial appearance and image distortions in real-world criminal databases. The system's enhanced performance, demonstrating a high overall accuracy of 98.5% and a significant decrease in the False Positive Rate, is attributable to the combined effectiveness of two key technical innovations. First, the Deep Feature Improvement Component employs a statistical method and a weighting mechanism based on attention to refine the deep feature representations, removing distortions and emphasizing distinguishing facial traits. This component alone resulted in a 6.6% improvement in accuracy compared to the standard model. Second, the Flexible Comparison Method surpasses the limitations of a predetermined similarity benchmark. By dynamically determining the benchmark (Ti) based on the specific variations (σi) within each criminal's profile, the system ensures an optimal equilibrium between identifying potential suspects and preventing inaccurate identifications. This confirms the system's reliability, especially in difficult circumstances such as partially obscured faces. In conclusion, this system provides a dependable, precise, and context-sensitive solution, establishing a new and improved benchmark for critical law enforcement identification systems.

VI. FUTURE WORKS

To maximize the real-world applicability and sophistication of this system, we recommend several areas for future investigation. First, we propose incorporating an advanced interpretability feature, enabling users to understand which specific facial characteristics influenced a matching outcome. This will foster greater confidence and clarity in the system's functionality.Second, research should explore expanding the system's capabilities to incorporate data from multiple sources. Combining facial information with other biometric identifiers, such as movement patterns or vocal signatures, could significantly enhance identification accuracy, particularly in situations where facial images are of poor quality.Third, we intend to create a dynamic learning element that allows the system to constantly refine its measurement of variability and adjust its decision-making parameters as it processes new and evolving surveillance information.Finally, considering the system's intended use in critical security applications, it is imperative that we investigate and implement safeguards against intentional manipulation. This will ensure the system remains dependable even when faced with deliberate attempts to circumvent its processes.

VII. REFERENCES

1. S. Singla, P. Singla, A. Khurana, S. Rana, R. Sharma and A. Sharma, "Real-time Criminal Face Recognition Using Machine Learning," *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)*, Pattaya, Thailand, 2024, pp. 289–295, doi: 10.1109/ICPIDS65698.2024.00053.
2. M. J. Wang, "Face Feature Dynamic Recognition Method Based on Intelligent Image," *2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, Hunan, China, 2018, pp. 57–60, doi: 10.1109/ICVRIS.2018.00022.
3. S. S. Chittibomma, R. Kishan Surapaneni and A. Maruboina, "Facial Recognition System for Law Enforcement: An Integrated Approach Using Haar Cascade Classifier and LBPH Algorithm," *2024 International Conference on Advancements in Power, Communication and Intelligent Systems (APCI)*, Kannur, India, 2024, pp. 1–6, doi: 10.1109/APCI61480.2024.10616450.
4. K. Agarwal and M. Dixit, "Analysis of Face Recognition Technique: Plastic Surgery Altered Face," *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, 2023, pp. 274–279, doi: 10.1109/ICCCIS60361.2023.10425008.
5. J. P. and S. A., "Convolutional Neural Network Model in Different Dataset for Pose Face Recognition," *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, Chennai, India, 2022, pp. 1–7, doi: 10.1109/ICSES55317.2022.9914120.
6. V. Singh, A. Dixit, S. Pandey, B. V. Kumar, V. Pachouri and M. Sahu, "Role of Artificial Intelligence in Criminal Investigation," *2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*, Kottayam, India, 2023, pp. 1–4, doi: 10.1109/iQ-CCHESS56596.2023.10391288.
7. V. K. Sharma, "Designing of Face Recognition System," *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, 2019, pp. 459–461, doi: 10.1109/ICCS45141.2019.9065373.
8. R. K., B. J. Jingle, S. C. P., S. V., J. B. Princess P. and V. K., "Facial Recognition System with LBPH Algorithm: Implementation in Python for Machine Learning," *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, Coimbatore, India, 2024, pp. 1681–1686, doi: 10.1109/ICoICI62503.2024.10696268.
9. P. Brito, J. P. Fontes, N. Miquelina and M. A. Guevara, "AGATHA: Face Benchmarking Dataset for Exploring Criminal Surveillance Methods on Open Source Data," *2018 International Conference on Graphics and Interaction (ICGI)*, Lisbon, Portugal, 2018, pp. 1–8, doi: 10.1109/ITCGI.2018.8602903.
10. S. K. Teoh, Y. H. Wong, C. F. Leong and L. Y. Tan, "Face Detection and Face Re-identification System Using Deep Learning and OpenVINO," *2021 2nd International Conference on Artificial Intelligence and Data Sciences (AiDAS)*, Ipoh, Malaysia, 2021, pp. 1–5, doi: 10.1109/AiDAS53897.2021.9574201.
11. L. Schaffer, Z. Kincses and S. Pletl, "FPGA-based Low-Cost Real-Time Face Recognition," *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, Subotica, Serbia, 2017, pp. 000035–000038, doi: 10.1109/SISY.2017.8080568.
12. N. Belghini, A. Zarghili, J. Kharroubi and A. Majda, "Color Facial Authentication System Based on Neural Network," *2011 Colloquium in Information Science and Technology*, Fez, Morocco, 2011, pp. 8–8, doi: 10.1109/CIST.2011.6148586.

13. M. R. Roshan and S. Loganayagi, "Improved Accuracy in Detection of Fraud Websites using Convolutional Neural Network Algorithm with Random Forest Algorithm," *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, Raigarh, India, 2024, pp. 1-4, doi: 10.1109/OTCON60325.2024.10687462.

14. S. J. J. Thangaraj, L. S, V. R. Vimal, D. V, E. Afreen Banu and J. P. A. Rani, "Design of Internet Product Interface Based on Dynamic Model," 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon), Singapore, Singapore, 2023, pp. 92-97, doi: 10.1109/SmartTechCon57526.2023.10391733.

15. Moorthy Agoramoorthy., Ali, A., Sujatha, D., Michael Raj, T.F., Ramesh, G.” An Analysis of Signature-Based Components in Hybrid Intrusion Detection Systems”2023 Intelligent Computing and Control for Engineering and Business Systems, ICCEBS 2023, 2023