P-ISSN: 2709-6254	Journal of Development and Social Sciences	Jan-Mar 2024, Vol. 5, No.1
O-ISSN:2709-6262	https://doi.org/10.47205/jdss.2024(5-I)54	[585-597]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

Comparative Study of Forensic Face Recognition and Fingerprint during Crime Scene investigation and the role of Artificial Intelligence tools in Forensics

[1]Shabana Kausar*, [2]Rizwana Khanzada and [3]Mohammad Abbas Sherazi

1. PhD Scholar, Dadabhoy Institute of Higher Education Karachi and Lecturer at Institute of Law University of Sindh Jamshoro, Sindh, Pakistan
2. PhD scholar Molecular biology (Liaquat Medical university of health science Jamshoro) Medical technologist/ forensic DNA analysts LUMHS, , Sindh, Pakistan
3. BS Forensic Biology LUMS Jamshoro, Sindh, Pakistan

***Corresponding Author:** adv.shabanakausar@gmail.com

ABSTRACT

Surprisingly, the high accuracies previously reported, exceeding 95%, dropped significantly when faced with the more demanding conditions of the forensic scenario, plummeting to as low as 65%. In essence, while facial recognition systems have shown impressive performance in ideal conditions, our study indicates a substantial decrease in accuracy when faced with the complexities and challenges typical of real-world forensic scenarios, highlighting the need for further advancements to bridge this gap. Recent advancements in machine learning and computer vision have shown facial recognition systems achieving accuracies that surpass human performance in controlled settings but fingerprint analysis is proved more accurate in all aspects. To investigate this, we created a large-scale synthetic facial dataset and designed a controlled facial lineup that mimics conditions encountered in real forensic situations. This approach allowed us to systematically assess facial recognition under various challenging real-world conditions. Using both our synthetic dataset and a well-known dataset of actual faces, we tested the accuracy of two widely used neural-based facial recognition systems. Comparative and Analytical method is applied for present Research. Artificial intelligence could help humans in accuracy and speeding up the process of investigation.

KEYWORDS: Artificial Intelligence, Crime Scene, Evidence, Facial Recognition, Fingerprints, Forensic, Investigation

Introduction

Forensic face recognition involves using facial features or characteristics to identify individuals for legal or investigative purposes. It relies on analyzing facial images or videos obtained from various sources, such as surveillance cameras, photographs, or video footage, to match or compare against known databases or other images to establish identity (Jatoi, 2021).

The process generally involves: Image Acquisition: Obtaining facial images or videos from crime scenes, surveillance footage, or other sources. Feature Extraction: Identifying and extracting key facial features like the distance between the eyes, nose shape, jawline, etc. This may involve using algorithms to create a facial template or representation. Database Comparison: Comparing the extracted features against databases of known individuals, which could include mugshots, official identification records, or other sources. Matching and Analysis: Algorithms compare the extracted features with the database to find potential matches or similarities. The analysis may involve statistical models or machine learning algorithms to determine the likelihood of a match (Kaipeng, 2016).

Verification/Validation: Human experts typically verify the results to confirm matches or similarities and provide expert testimony in legal proceedings if necessary. Forensic face recognition has its challenges, including variations in lighting, facial expressions, image quality, and angle differences. Despite technological advancements, it's not always foolproof and is often used in conjunction with other evidence-gathering techniques for a more comprehensive investigation. Ethical considerations and the potential for biases in algorithms are also important factors to consider in forensic face recognition. Therefore, its application requires careful scrutiny and validation to ensure accuracy and fairness in legal and investigative contexts.

Literature Review

Facial Recognition through CCTV Footage: Facial recognition using CCTV footage involves the application of facial recognition technology to analyze and identify individuals captured on closed-circuit television (CCTV) cameras. CCTV cameras are commonly used for surveillance in (Duncan, 2018) public spaces, commercial establishments, and other areas to monitor activities and enhance security. The process of facial recognition with CCTV footage typically involves these steps:

- **Footage Collection:** CCTV cameras capture video footage in specific areas. These cameras continuously record activities, and the footage may contain individuals' faces.
- **Face Detection:** Software algorithms are used to detect and locate faces within the recorded video frames. This step involves identifying facial features such as eyes, nose, mouth, and other distinguishing characteristics.
- **Feature Extraction:** Once faces are detected, the system extracts facial features or creates a digital representation of the face, often referred to as a facial template or signature. These templates encode key facial characteristics for comparison.
- **Database Comparison:** The extracted facial templates are compared against a database of known individuals, which could consist of a watchlist, criminal databases, or other records containing facial information.
- **Matching and Analysis:** Algorithms compare the extracted facial features with the database entries to find potential matches or similarities. The system calculates the likelihood of a match based on similarity scores (Bacci & Davimes, Facial Comparison: Current Status, Limitations, and Future Directions., 2021).
- **Verification/Review:** Human operators or experts often review the results to confirm matches and assess the accuracy before taking any action or making conclusions based on the recognition results. Facial recognition based on CCTV footage has raised concerns about privacy, potential misuse, and ethical considerations regarding mass surveillance. There are also challenges such as varying lighting conditions, angles, image quality, and the potential for false positives or errors, which can impact the accuracy of identification (Group, 2019).

Regulations and policies regarding the use of facial recognition technology in public spaces continue to evolve, considering the balance between security needs and individuals' rights to privacy and protection from unwarranted surveillance (Steyn, et al., 2018).

Artificial Intelligence and Facial Recognition: Artificial intelligence (AI) significantly enhances forensic facial recognition by improving accuracy, efficiency, and scalability. Here's how AI contributes to this field:

- **Advanced Algorithms:** AI algorithms, especially deep learning and neural networks, excel in learning intricate patterns and features from facial data. They can identify

and extract facial features more accurately, even in complex conditions like varying lighting, angles, and facial expressions.

- **Enhanced Accuracy:** AI-based facial recognition systems continuously improving through training on large datasets. They can learn from diverse facial characteristics, reducing false positives and negatives. AI works minutely on details and on pixels of available images therefore its more reliable than other sources.
- **Speed and Efficiency:** AI enables swift processing of large volumes of facial data from CCTV footage or image databases, reducing the time required for analysis and identification. AI also works on online traffic data and enhance the range of available options before forensic experts (Bacci & Davimes, Facial Comparison: Current Status, Limitations, and Future Directions., 2021).
- **Feature Extraction:** AI algorithms can extract detailed and nuanced facial features, allowing for more precise matching and comparison against databases of known individuals (Urbanova, 2016).
- **Adaptability to Variability:** AI models can adapt to variations in facial appearance due to aging, disguises, or different facial expressions, improving their ability to recognize individuals over time.
- **Integration with Other Technologies:** AI-powered facial recognition can be integrated with other technologies like object detection, scene analysis, and natural language processing, providing a more comprehensive understanding of events or situations.
- **Improving Forensic Investigations:** AI can assist forensic experts by rapidly processing and analyzing vast amounts of facial data, aiding in identifying suspects or missing persons.

However, challenges persist, including ensuring the fairness and accountability of AI algorithms, addressing biases within the datasets used for training, and maintaining ethical standards in the use of facial recognition technology for forensic purposes. Over all, AI's role in forensic facial recognition continues to evolve, offering promising advancements in accuracy and efficiency while raising important ethical and privacy considerations that require careful management and regulation.

Material and Methods

Researcher relied on already online previous researches done by various authors and analytical method is employed for this paper. The facial images showcased in Figures 1 and 2 of this paper belong to the corresponding author and are sourced from the Wits Face Database's sample images. These images are publicly available and can be reproduced under an open access license governed by the Creative Commons Attribution License. This license allows unrestricted utilization, distribution, and reproduction in any format or medium, given that appropriate citation of the original work is included. Access to these images is available through the supplementary materials accompanying the Wits Face Database's data note.

Algorithm of facial Recognition step by step: Facial recognition algorithms are computational methods used to identify and authenticate individuals by analyzing their facial features. Here's a simplified explanation of how they generally work:

- **First step: Face Detection:** The algorithm first locates a face within an image or video frame. This step involves identifying patterns that resemble a human face, such as the arrangement of eyes, nose, mouth, and their spatial relationships.
- **Second Step: Feature Extraction:** Once a face is detected, the algorithm extracts specific features from the face, often represented by numerical values. These features

can include the distance between the eyes, the shape of the nose, the contours of the face, etc. Various techniques like eigenfaces, local binary patterns, or deep learning methods are used to extract these features.

- **Third Step: Feature Comparison:** The extracted facial features are then compared to a database of known faces or templates to find a match. This comparison is typically done by measuring the similarity or dissimilarity between the extracted features and the stored features using mathematical algorithms.
- **Fourth Step: Classification or Recognition:** Based on the comparison results, the algorithm determines whether the face matches any of the faces in the database. If it finds a match above a certain threshold level of similarity, it identifies the individual associated with that matched face.
- **Update and Learning:** Some facial recognition systems continually update and improve their recognition accuracy by learning from new data. This can involve retraining the algorithm with new images or fine-tuning its parameters based on its performance. Facial recognition algorithms have applications in various fields, including security, law enforcement, access control, and digital authentication. However, ethical considerations about privacy, consent, and potential biases in these systems are crucial as the technology advances.

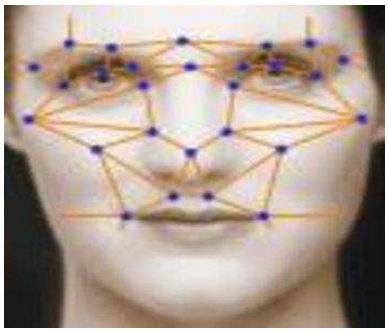

Fig.1 Image sample for Facial recognition

Fingerprint matching process step by step:

Fingerprint matching involves a series of steps to compare and determine whether two fingerprints are from the same individual. Here's a simplified explanation:

- **First Step: Image Acquisition:** The process begins by capturing an image of the fingerprint. This can be done using various methods, including optical scanners or capacitive sensors. The fingerprint image obtained is typically a grayscale representation showing the ridges and valleys.
- **Second Step: Preprocessing:** The captured image undergoes preprocessing to enhance its quality and make it suitable for analysis. This step involves removing noise, adjusting contrast, enhancing ridge structures, and standardizing the image size and orientation.
- **Third Step: Minutiae Extraction:** Fingerprint matching primarily relies on identifying minutiae points, which are specific points where ridges end, split, or change direction. Algorithms analyze the fingerprint image to extract minutiae such as ridge endings, bifurcations, and ridge dots (Wayman, 2022).
- **Fourth Step: Feature Extraction:** Once the minutiae points are identified, their characteristics are quantified and encoded. Information about the position, direction, and relationship between minutiae points is stored as a unique fingerprint template or fingerprint representation.

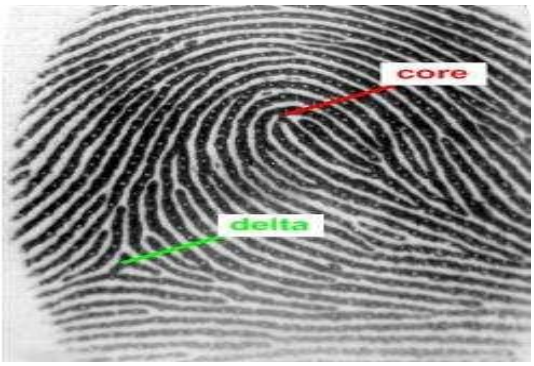

Fig.2 Image sample for Finger Print Recognition

- **Fifth Step: Matching:** The extracted features or templates of the fingerprints to be compared are then compared against each other(Jain, 2014). Matching algorithms evaluate the similarity or dissimilarity between the minutiae points, usually using mathematical techniques like pattern matching or correlation.
- **Sixth Step: Scoring and Decision:** A similarity score is generated based on the comparison. If the score surpasses a predefined threshold, the fingerprints are considered a match, indicating that they likely belong to the same person. Otherwise, they are considered different (Noyes E, 2017).
- **Final Step: Verification or Identification:** In verification scenarios, the goal is to confirm whether a fingerprint matches a specific reference fingerprint (one-to-one comparison). In identification scenarios, the objective is to search a database to find a match for an unknown fingerprint (one-to-many comparison) (Rupinder Saini, 2014).

Fingerprint matching is widely used in various fields, including law enforcement, access control, forensics, and identity verification due to its uniqueness and reliability. The accuracy of the process relies on the quality of the captured image, the effectiveness of the feature extraction algorithms, and the matching criteria used.

Role of Artificial intelligence in facial Recognition and Fingerprint Analysis:

Artificial intelligence (AI) plays a significant role in advancing facial recognition and fingerprint analysis technologies, improving accuracy, efficiency, and robustness (Bacci & Davimes, Facial Comparison: Current Status, Limitations, and Future Directions., 2021). Here are examples of AI's role in these areas:

Role in Facial Recognition

- **Feature Extraction and Recognition**: AI-based algorithms, particularly deep learning models like Convolutional Neural Networks (CNNs), excel at learning intricate patterns in facial features. They're capable of extracting high-level representations of faces, allowing for more accurate recognition (Stephan, Caple, Guyomarc'h, & Claes, 2019). *Example:* Face Net and VGG Face are deep learning models trained to generate face embeddings (numerical representations) that enable accurate face recognition even with variations in pose, lighting, and facial expressions.
- **Improved Accuracy**: AI enables facial recognition systems to adapt and improve over time by learning from large datasets (Ashby, 2017). They can continuously refine their recognition capabilities, reducing errors and false positives/negatives. *Example:* Systems like Amazon Rekognition and Microsoft Azure Face API utilize AI for face

detection, verification, and identification, constantly improving their accuracy through machine learning (Arabina, June 2009).

- **Ethical Considerations**: AI also helps address ethical concerns by attempting to minimize biases in facial recognition systems. Efforts are made to train models on diverse datasets and develop algorithms that are less prone to racial, gender, or cultural biases. *Example:* IBM developed a dataset called Diversity in Faces (DIF) to reduce biases in facial analysis systems by incorporating a more diverse range of facial images (Bacci, Steyn, & Briers, Performance of forensic facial comparison by morphological analysis across optimal and suboptimal CCTV settings., 2021).

Role of AI in Fingerprint Analysis:

a. **Minutiae Detection and Matching**: AI algorithms aid in accurately detecting minutiae points on fingerprints and matching them effectively, improving the speed and precision of identification. *Example:* Automated Fingerprint Identification Systems (AFIS) like NEC's Integra-ID 5 use AI-powered algorithms for fast and accurate matching of fingerprints in forensic investigations and identity verification.

b. **Enhanced Pattern Recognition:** AI enhances the ability to recognize complex patterns and structures in fingerprints, making it possible to analyze partial or distorted prints more effectively. *Example:* Cognitec's Face VACS-DB Scan leverages AI to identify faces in large image databases, including forensic applications where degraded or partial face images need to be matched (Facial Image Comparison Feature List for Morphological Analysis, 2018).

c. **Real-time Processing**: AI enables faster processing and matching of fingerprints, allowing for rapid identification and verification in various applications (Noyes E, 2017). *Example:* MorphoTrak, now part of IDEMIA, uses AI-driven fingerprint identification technologies in law enforcement and civil applications to quickly match prints against large databases.

AI's role in facial recognition and fingerprint analysis continues to evolve, driving improvements in accuracy, speed, and ethical considerations, making these technologies more reliable and versatile for various applications.

d. **Accuracy Comparison:** When it comes to the use of artificial intelligence (AI) in forensic evidence analysis, the reliability of facial recognition and fingerprint recognition can be influenced by various factors:

e. **Training Data and Algorithms:** Facial Recognition: AI-driven facial recognition systems rely on vast datasets of facial images for training. The accuracy and reliability of facial recognition can depend on the quality and diversity of these datasets. AI algorithms can learn to recognize patterns in faces, but their accuracy can be affected by variations in lighting, angles, expressions, and potential changes in appearance (Facial Image Comparison Feature List for Morphological Analysis, 2018).

f. **Fingerprint Recognition**: AI-driven fingerprint recognition systems also require extensive datasets for training. These systems use AI algorithms to analyze and match complex fingerprint patterns. The reliability of AI-driven fingerprint recognition depends on the quality and comprehensiveness of the fingerprint datasets used for training.

g. **Accuracy and Error Rates:** AI systems for both facial recognition and fingerprint recognition can achieve high accuracy rates. However, the accuracy can still vary based on the quality of the input data and the algorithms used. Even with AI, facial recognition might face challenges in accuracy due to variations in facial features, whereas fingerprint recognition tends to maintain higher accuracy due to the stability and uniqueness of fingerprints.

h. **Maturity of Technology:** Fingerprint recognition has a longer history of AI integration and refinement compared to facial recognition. AI has significantly enhanced the speed and precision of fingerprint matching systems (AFIS). It's a more mature technology in forensic contexts.

i. **Interpretation and Context:** Both AI-driven facial recognition and fingerprint recognition require expert interpretation and validation of the results. Human expertise is crucial in confirming matches and interpreting the significance of the identified matches within the context of a forensic investigation.

In summary, while AI has significantly advanced both facial recognition and fingerprint recognition, fingerprint recognition remains more established and reliable in forensic evidence due to its historical use, maturity of technology, and the stability of fingerprint patterns. Facial recognition, despite advancements through AI, may still face challenges in accuracy and reliability, especially in certain conditions and contexts, making fingerprint recognition currently more scientifically reliable in forensic evidence analysis through AI. However, ongoing developments in AI may continue to enhance the capabilities and accuracy of both technologies in the future (Bacci & Davimes, Facial Comparison: Current Status, Limitations, and Future Directions., 2021).

Comparison of forensic facial recognition with Finger print Analysis through Artificial intelligence in modern Era:

Certainly! Facial recognition and fingerprint recognition are both biometric identification methods, but they differ in several aspects:

i. **Biometric Feature Used**: Facial Recognition: It relies on capturing and analyzing facial features such as the distance between eyes, nose shape, jawline, etc.

ii. Fingerprint Recognition: It captures and analyzes the unique patterns of ridges and valleys present on a person's fingertip.

iii. Capture Method: Facial Recognition: It captures images of the face using cameras or other imaging devices.

iv. Fingerprint Recognition: It uses specialized scanners to capture an individual's fingerprint impressions from crime scene during investigation.

v. Invasiveness and Convenience: Facial Recognition: Generally non-intrusive and can be implemented without direct physical contact, making it convenient for scenarios like surveillance or public spaces.

vi. Fingerprint Recognition: Requires physical contact with a scanning device, which may not be as convenient in some scenarios and can raise hygiene concerns.

Comparison of Accuracy and Reliability of facial recognition and fingerprints analysis:

- **Facial Recognition**: Susceptible to variations in lighting, angle, facial expressions, and certain facial alterations, potentially affecting accuracy.
- **Fingerprint Recognition**: Generally considered highly accurate and reliable due to the uniqueness and stability of fingerprint patterns.
- **Usage and Applications:**
- **Facial Recognition**: Widely used in security systems, access control, authentication on mobile devices, and increasingly in public spaces for identification and tracking.
- **Fingerprint Recognition**: Commonly used in various security applications such as unlocking smartphones, access to secure facilities, forensic identification, and law enforcement.
- **Security and Privacy:**
- **Facial Recognition**: There are concerns regarding privacy invasion and misuse due to the ease of capturing facial images in public spaces and the potential for unauthorized surveillance.
- **Fingerprint Recognition**: While biometric data is also sensitive, fingerprint data might be perceived as more secure as it generally requires physical contact, making it harder to capture without the person's knowledge.
- **Adoption and Cost:** Facial Recognition: Increasingly adopted due to technological advancements and integration with everyday devices. However, the cost of implementation and accuracy improvements can vary.
- **Fingerprint Recognition**: Relatively mature technology with widespread adoption, and it may have lower implementation costs in some cases compared to facial recognition systems.

Table 1
Comparison table of all biometrics

Biometrics	Accuracy	Cost	Size of template	Long term stability	Security level
Facial recognition	Low	High	Large	Low	Low
Iris scan	High	High	Small	Medium	Medium
Finger print	Medium	Low	small	Low	Low
Finger vein	High	Medium	Medium	High	High
Voice recognition	Low	Medium	Small	Low	Low
Lip Recognition	Medium	Medium	Small	Medium	High

In summary, both facial recognition and fingerprint recognition are biometric methods used for identification, but they differ in the type of biometric feature used, their capture methods, levels of invasiveness, accuracy, applications, security concerns, and adoption rates. Each has its strengths and weaknesses, making them suitable for different contexts and applications (Bacci & Davimes, Facial Comparison: Current Status, Limitations, and Future Directions., 2021).

Scientist conducted an extensive screening process to assess the challenges in matching identities using a fusion of three top-performing algorithms identified from the Face Recognition Vendor Test 2006 (FRVT 2006) competition. These algorithms were utilized to stratify images into three difficulty levels based on their performance.

To refine the selection of image pairs, we incorporated human experimental data. Initially, we measured the accuracy of undergraduate students on the two most challenging levels identified by the algorithm. The top 25% of performers were selected, and from this group, we curated 84 pairs of images depicting the same identity and 84

pairs depicting different identities that resulted in the highest error rates(Huiting Sun, 2023).

This selection formed a stimulus pool representing image pairs that were particularly demanding for both humans and previous-generation face recognition algorithms. A second stimulus pool was created with the aim of identifying image pairs on which earlier algorithms consistently failed. These pairs were sampled from a study that examined image pairs causing 100% incorrect predictions by machine algorithms in the FRVT 2006, where similarity scores between faces of the same identity were consistently lower than those of different identity pairs (Facial Image Comparison Feature List for Morphological Analysis, 2018).

Subsequently, a third level of stimulus screening was implemented for both stimulus pools. This involved evaluating performance on an identity matching task under very brief (30-second) stimulus presentation times. The stimuli were sorted based on the difficulty experienced by forensic examiners during this test.

Prior discussions with facial examiners revealed their willingness to evaluate 20 pairs of images within a span of 3 months. This time frame was chosen to replicate the duration typically allotted for a thorough forensic comparison. Employing the screening criteria mentioned earlier, we specifically selected 12 image pairs from the first stimulus pool and 8 pairs from the second. These pairs comprised both same identity (n=12) and different identity (n=8) pairs. The slight imbalance in the numbers of selected pairs precluded the application of a process of elimination strategy.

Forensic face Recognition

We simulate a real-world lineup scenario by constructing a lineup of six images, one being the suspect (probe) and the others serving as decoys with similar attributes. The probe image reflects an unconstrained real-world capture, akin to CCTV footage, while the lineup images adhere to standardized mug-shot style criteria (frontal view, no glasses or masks, and consistent lighting). This setup aims to emulate typical situations encountered in real-world identification scenarios. In our analysis of real-world datasets, we propose that the dissimilarity between synthetic and authentic data stems from ArcFace's deliberate elimination of noisy images during training, leading to a model optimized for relatively clean images. Despite this disparity, our findings demonstrate that manipulating the probe image quality used in lineup creation can realign accuracy between synthetic and real-world datasets. While the current study doesn't encounter this issue, if synthetic dataset accuracy were lower than real-world accuracy, we suggest modifying the lineup selection process. Instead of choosing the top-five most similar faces, selecting faces ranked between the nth and (n−4)th positions could simplify the forensic lineup task (Melnykov, 2012).

During a study it is observed that it is analyzed and examined a sample of one hundred individuals during a study at U.S, comprising 40 females and 60 males. Among these, 75 individuals were enrolled in the system, while 25 were not. The performance evaluation of our two modal access control systems yielded the following results:

Facial Recognition System: 70 true positive identifications, 5 false negative identifications, 8 false positive identifications, and 17 true negative identifications.

Fingerprint Recognition System: 73 true positive identifications, 2 false negative identifications, 4 false positive identifications, and 21 true negative identifications.

These results form the confusion matrix for our analysis. Upon thorough examination of the tests conducted, it is evident that the decisions made by the fingerprint

recognition system exhibit superior accuracy compared to those made by the facial recognition system (Bopatriciat Boluma Mangata, 2022).

Database availability for forensic Facial recognition and fingerprint identification

In Pakistan for this purpose NADRA (National database and registration authority) could be connected with forensic Labs. But only on NADRA could not be relied for this purpose Facebook, Instagram, twitter, and other social media websites should also be used and open access data should be utilized.

Conclusion

Biometric technology, particularly facial expression recognition, holds significant promise for identification and verification in various domains. Its potential for identifying individuals within crowds offers a pathway to enhance security by pinpointing known criminals, terrorists, or fraudulent individuals. However, facial recognition technology grapples with substantial challenges concerning accuracy, efficiency, speed, cost, and security. Addressing these complexities is imperative to maximize its effectiveness and applicability in real-world scenarios. The collective judgments of individuals working together significantly outperformed those made by individuals working independently. Combining these judgments also contributed to stabilizing performance by enhancing the accuracy of less proficient individuals and reducing variability. When a single forensic facial examiner collaborated with the most effective algorithm, their accuracy surpassed that of two individual examiners working together. Consequently, collaboration, whether among humans or between humans and machines, presents substantial advantages for improving face identification accuracy in critical applications. These findings establish a data-supported strategy for attaining the highest possible accuracy in face identification (Facial Image Comparison Feature List for Morphological Analysis, 2018).

In the realm of AI technologies, there's significant potential to mitigate human errors and function at an expert level. Unlike traditional software relying on predetermined facial recognition features or demographic patterns, AI algorithms for video and image processing can learn intricate tasks and independently establish complex facial recognition parameters beyond human consideration.

These AI algorithms have multifaceted applications, from matching faces and detecting objects like weapons to identifying complex events such as accidents or ongoing crimes. Responding to criminal justice needs, the National Institute of Justice (NIJ) has directed efforts to enhance data collection, imaging, and contextual analysis in law enforcement.

For example, research funded by NIJ(national institute of justice U.S) at the University of Texas, Dallas, in collaboration with the FBI and National Institute of Standards and Technology, explores the comparison between human facial identification and AI algorithms. Initial findings suggest that AI-based facial recognition algorithms, when restricted to 30 seconds, perform on par with human examiners. This implies that AI could act as a complementary tool, enhancing the accuracy of expert human examiners and boosting productivity.

Carnegie Mellon University, also supported by NIJ funding, is developing AI algorithms to address challenges posed by images captured at different angles or with partial obstructions. Their work encompasses scenarios where faces are obscured by masks, helmets, lighting, or low-quality resolutions, aiming to enhance detection and recognition in such conditions.

Furthermore, research at Dartmouth College involves AI algorithms that systematically degrade high-quality images to match with low-quality ones, aiding in deciphering license plates or identifying individuals in low-quality media (Facial Image Comparison Feature List for Morphological Analysis, 2018).

Additionally, efforts in "scene understanding" involve generating descriptive text that contextualizes relationships between objects in images, aiming to identify ongoing crimes or support post-event investigations. University of Central Florida researchers, partnered with the Orlando Police Department, are developing algorithms for object and action identification in videos without human intervention.

Predictive behavior analysis is another AI application. The University of Houston, through NIJ funding, is working on algorithms for continuous monitoring to predict suspicious behavior across camera networks, utilizing factors like clothing, skeletal structure, and movement for identifying individuals and predicting their actions across various cameras.

Recommendations

Researcher suggest following recommendations for future betterment:

1. To increase reliability and validity in facial recognition system Artificial intelligence tools should be design to draw results not only by systematically but also human judgment also should be included.

2. AI tools should be installed in forensic labs as AI algorithm can analyze facial features such as the distance between eyes, nose shape, and jawline etc. to match faces captured in image or videos to identify individuals. This technology will help not only to identify suspect but also remain helpful in finding missing persons.

3. That such type of software designed with works by using hybrid technology and identification tools. AI tools which are designed to match fingerprints should also be installed in forensic labs.

4. That image drafting software should be used to draw image on directions of eyewitness to improve accuracy.

5. All investigation agencies should train their investigators in this regard. AI algorithms can be used to store and analyze crime pattern as AI algorithms can analyze crime data minutely including time, location and modus operandi (mode of crime).

6. This is the high time to use AI tools in betterment of demolishing image of Justice system in Pakistan.

7. New legislation is required to deal all different kinds of forensic evidence only Article 164 of QSO is not sufficient to deal with new emerging challenges.

Utilizing AI and predictive policing analytics within integrated systems, including computer-aided response and live public safety video networks, law enforcement stands to significantly enhance incident response, threat prevention, intervention planning, resource allocation, and the investigation and analysis of criminal activities. AI represents a promising and enduring facet of our criminal justice framework, offering investigative support and empowering criminal justice experts to more effectively uphold public safety.

Bibliography:

Arabina, R. J. (june 2009). A Survey of Face Recognition Techniques. *Journal of Information Processing Systems,*5(2), 10-21

Ashby, M.P.J., & Bowers, K.J. (2012). A comparison of methods for temporal analysis of aoristic crime. *Crime Science, 2*(1). https://doi.org/10.1186/2193-7680-2-1

Bacci N, Davimes JG, Steyn M, Briers N. Forensic Facial Comparison: Current Status, Limitations, and Future Directions. Biology (Basel). 2021 Dec 3;10(12):1269. doi: 10.3390/biology10121269. PMID: 34943183; PMCID: PMC8698381.

Bopatriciat Boluma Mangata, Contribution of an Embedded and Biometric Systemin a Replicated Database for Access Control in a Multi-Entry Institution. InternationalJournal of Science and Research (IJSR), 10 (Issue 3), 2021

Bopatriciat Boluma Mangata, D. I. (2022). COMPARATIVE STUDIES BETWEEN A FACIAL RECOGNITION SYSTEM AND A FINGERPRINT RECOGNITION SYSTEM FOR ACCESS CONTROL. *International Journal of Information System and Computer Science*. 6(2) 69-71

Duncan, J. (2018, 1 3). *How CCTV surveillance poses a threat to privacy in South Africa. Conversation*. Retrieved from How CCTV surveillance poses a threat to privacy in South Africa. Conversation: https://theconversation.com/how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa-97418

Facial Image Comparison Feature List for Morphological Analysis. (2018). published by fiswg.org Retrieved from Facial Identification ScientificWorking Group: https://fiswg.org/FISWG_Morph_Analysis_Feature_List_v2.0_20180911.pdf

Group., F. I. (2019). *Facial Comparison Overview and Methodology Guidelines published by fiswg.org.com* Retrieved from Facial Identification Scientific Working Group.: https://fiswg.org/fiswg_facial_comparison_overview_and_methodology_guidelines_V1.0_20191025.pdf

Huiting Sun, J. P. (2023). *A survey on face recognition methods with federated leaning", Institution of Engineering and Technology (IET).* IET.

Jain, A. K. (2004). Fingerprint recognition: Recent advances and future directions. *Journal of the ACM Computing Surveys (CSUR), 36(2)*, 381-422.

Kaipeng Zhang, Z. Z. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. *IEEE Signal Processing Letters*, 1499-1503. https://doi.org/10.48550/arXiv.1604.02878

Kong, A., & Zhang, D. (2009). A survey of palmprint recognition. Pattern Recognition, 42(7), 1408-1418.

Melnykov, V. C. (2012). MixSim: An R package for simulating data to study performance of clustering algorithms. *Journal of Statistical Software, 51*, 1-25.

Nicholas Bacci, Maryna Steyn, Nanette Briers, Performance of forensic facial comparison by morphological analysis across optimal and suboptimal CCTV settings, Journal Science & Justice, Volume 61, Issue 6, 2021, Pages 743-754, ISSN 1355-0306, https://doi.org/10.1016/j.scijus.2021.09.003.

Noyes E, P. P. (2017). *What is a super-recogniser? Face Processing:Systems, Disorders, and Cultural Differences, eds,.* New Yark: Nova New yark.

Phillips, P. J. (2005). Overview of the face recognition grand challenge. In the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. *IEEE COMPUTER SOCIETY.*

Phillips, P. J., Wechsler, H., Huang, J., & Rauss, P. J. (1998). The FERET database and evaluation procedure for face-recognition algorithms. Image and Vision Computing, 16(5), 295-306.

Rabia Jarfi & Hamid R. Arabina, (2009). "A Survey of Face Recognition Techniques", Journal of InformationProcessing Systems, 5, (2),

Rattani, A., & Nandakumar, K. (2016). Comparative analysis of fingerprint recognition algorithms. In 2016 IEEE International Conference on Image Processing (ICIP) (pp. 2471-2475).

Ross, A., Jain, A. K., & Nandakumar, K. (2006). Introduction to multimodal biometrics. In Advances in Biometrics (pp. 1-22). Springer

Rupinder saini, n. R. (2014). COMPARISON OF VARIOUS BIOMETRIC METHODS. *International journal of advance science and technology volume 1 issue 2*. p.24-30

S.K Jatoi, P. D. (2021). Forensic DNA Profiling and Criminal Justice System in Pakistan:. *Pakistan Social Sciences Review*, 5(2).677-697.

Stephan, C., Caple, J., Guyomarc'h, P., & Claes, P. (2019). An overview of the latest developments in facial imaging. *Forensic Science*, 4(1),10-28.

Steyn, M., Pretorius, M., Briers, N., Bacci, N., Johnson, A., & Houlton. (2018). T.M.R. Forensic facial comparison in South Africa: State of the science. *Forensic Sci. Int.*, volume 287,190-194.

Urbanová, P. (2016). Performance of distance-based matching algorithms in 3D facial identification. Egypt. *Forensic science Journal*, 6. 135-151.

Wayman, J. L. (2022). *Biometric systems: Technology, design, and performance evaluation.* U.K: SPRINGER.