Project WraithCast: An AI-Driven Privacy-Preserving Framework for Witness Testimony and Judicial Communication

Joderick Sherwin J[1][0009-0005-4732-5712], Karthiga R[2], Hari Balaji JC[3], Suba Malai R[4], Malathy EM[5]

[1] Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai
220701109@rajalakshmi.edu.in
[2] Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai
220701119@rajalakshmi.edu.in
[3] Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai
220701080@rajalakshmi.edu.in
[4] Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai
subamalai.r@rajalakshmi.edu.in
[5] Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai
hod.cse@rajalakshmi.edu.in

Abstract. This research introduces *Project WraithCast*, an AI-driven system designed to safeguard witness identities in criminal proceedings while preserving non-verbal expressiveness. Traditional anonymization techniques—such as face blurring or audio distortion—often compromise emotional context and authenticity, which are critical in judicial evaluation. WraithCast overcomes these limitations by employing *computer vision* and *motion capture* technologies to translate live video feeds into dynamic wireframe avatars that convey body language and gestures without revealing identifiable visual or audio features. The system integrates **MediaPipe Holistic** for multi-landmark detection and **OpenCV** for real-time wireframe rendering, achieving frame rates of 20–25 FPS on standard hardware. It is particularly suited for high-risk legal scenarios, including witness protection programs, victim testimonies in sensitive cases, and undercover intelligence reporting. By representing human movement through landmark coordinates instead of raw video data, WraithCast enforces a *privacy-by-design* approach, resistant to deepfake reconstruction and visual bias. The proposed framework demonstrates how artificial intelligence can balance security, ethics, and authenticity within digital judicial processes, contributing to a more secure and equitable courtroom ecosystem..

Keywords: Identity protection, Computer vision, Witness testimony, Wireframe visualization, Privacy-preserving AI, Motion capture, Legal technology, Deepfake resistance.

1 Introduction

In modern judicial systems, the protection of witnesses and informants during criminal proceedings has become a critical concern. Testimonies often play a decisive role in conviction or acquittal, yet exposing a witness's identity can result in severe repercussions, including threats, coercion, and retaliation. Traditional witness protection mechanisms rely on relocation, voice modulation, and facial blurring, but these approaches often compromise either the clarity of testimony or the psychological comfort of the witness. The need for a technologically advanced, real-time, and non-invasive identity protection system has never been more urgent.

Project WraithCast introduces an innovative solution that integrates computer vision, artificial intelligence, and privacy-preserving visualization techniques to enable secure testimony delivery. Using the MediaPipe Holistic model, the system captures real-time body, face, and hand landmarks from a live webcam feed. These landmarks are then converted into a dynamic wireframe visualization, ensuring that the witness's physical identity remains completely obscured while preserving crucial non-verbal cues such as posture, gesture, and movement—elements vital for assessing credibility and emotional state.

The proposed system not only anonymizes the visual identity of the testifier but also maintains the behavioral integrity of their expressions. Unlike traditional pixelation or avatar-based solutions, WraithCast provides a naturalistic and continuous representation of human motion, making it suitable for both courtroom presentations and remote testimony environments. Furthermore, the framework allows integration with secure video conferencing and digital evidence systems, ensuring compatibility with modern judicial infrastructure.

By combining AI-driven motion capture and real-time visualization, WraithCast presents a scalable model for privacy in digital justice systems. This research aims to evaluate its efficacy in preserving identity, maintaining communication fidelity, and ensuring admissibility under legal standards. Ultimately, the system signifies a shift toward technologically empowered justice, where privacy and truth coexist without compromise.

2 Related Work

Identity protection and privacy-preserving technologies have been extensively studied across domains such as surveillance, video conferencing, and digital forensics. However, their integration into judicial processes—particularly for witness protection during testimony—remains limited.

Traditional witness anonymity mechanisms rely heavily on **physical relocation**, **voice modulation**, and **closed courtroom sessions** to safeguard individuals [1]. Although effective in certain contexts, these methods are resource-intensive and impractical in digital or remote court environments. With the increasing adoption of **virtual hearings** and **remote testimonies**, there is a growing demand for technologically supported identity protection that balances privacy and authenticity.

In the area of **computer vision-based anonymization**, early works focused on **face blurring**, **pixelation**, and **mask overlays** to obscure identifiable features in surveillance and media broadcasting [2]. While these techniques successfully conceal identity, they also degrade critical behavioral and emotional cues—such as facial expressions, body posture, and hand gestures—that often influence the interpretation of testimony credibility.

Recent progress in **pose estimation** and **motion capture** technologies has opened new avenues for privacy-preserving representation. Frameworks like **OpenPose** [3] and **MediaPipe Holistic** [4] allow precise real-time detection of human skeletal, facial, and hand landmarks. These have been applied in diverse fields including physical therapy, gaming, and virtual avatars. However, their potential for **judicial identity protection** or **forensic testimony visualization** has not been deeply explored.

Beyond visual anonymization, emerging frameworks in **privacy-preserving artificial intelligence (AI)**—such as **federated learning**, **homomorphic encryption**, and **differential privacy**—aim to protect personal data during processing and transmission [5][6]. Although these methods provide strong data confidentiality guarantees, they do not directly address the issue of **visual identity exposure** during live, video-based testimony.

Project WraithCast differentiates itself by combining **pose-based visualization** with **AI-driven landmark detection** to create a real-time **wireframe representation** of the witness. This approach maintains behavioral authenticity and emotional expressiveness while ensuring complete identity anonymity. Positioned at the intersection of **forensic computing**, **AI ethics**, and **legal informatics**, WraithCast introduces a scalable and ethical paradigm for **digital witness protection** in modern judicial systems.

3 System Design and Architecture

The **WraithCast architecture** follows a modular and extensible design, organized into four primary layers as illustrated in **Figure 1**. This structure ensures scalability, maintainability, and ease of integration into secure digital judicial systems. Each module performs a distinct function, contributing to the overall privacy-preserving visualization pipeline.

3.1 Camera Module

The **Camera Module** is responsible for video acquisition and frame preprocessing. It utilizes the **OpenCV** library to establish a connection with the system's webcam and

continuously capture real-time video streams. The captured frames are resized, normalized, and converted to the appropriate color space (BGR to RGB) before being forwarded to the processing pipeline. This design ensures that each frame is uniformly prepared for landmark detection while maintaining optimal frame rates for real-time performance.

3.2 Processing Module

The **Processing Module** forms the computational core of the system. It employs the **MediaPipe Holistic** framework to perform simultaneous detection of **face, hand, and body pose landmarks**. Each processed frame yields up to **543 unique landmarks**, forming multidimensional coordinate arrays that represent the human skeleton's structure and motion. These arrays are then filtered and smoothed to reduce noise, ensuring continuity between consecutive frames. The module operates in real time, leveraging GPU acceleration when available for enhanced efficiency.

3.3 Visualization Module

The **Visualization Module** translates the numerical landmark data into an **anonymized wireframe representation** of the individual. Using **OpenCV's drawing primitives**, the system dynamically connects key landmark points with lines and nodes, creating a skeletal wireframe that accurately reflects gestures and posture while concealing personal identity. This visualization maintains **expressivity, emotion, and behavioral authenticity**, enabling judges and jurors to observe non-verbal communication cues without compromising witness privacy.

3.4 Configuration and Logging

To ensure adaptability and reproducibility, the application parameters—including camera resolution, detection thresholds, and visualization settings—are defined in **YAML-based configuration files**. This modular configuration enables rapid adjustments without modifying source code. Additionally, a dedicated **logging subsystem** records system events, performance metrics, and error traces, facilitating debugging and ensuring operational transparency during live testimony sessions.

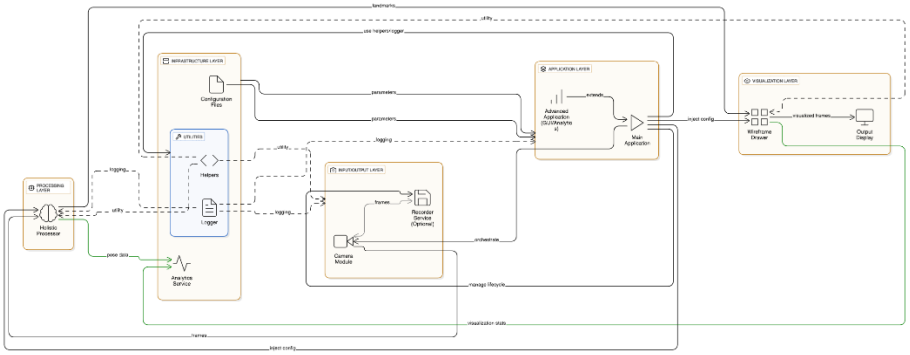

Fig. 1. *Architecture of Project WraithCast (Data flow: Webcam → Landmark Detection → Wireframe Visualization → Display Output).*

4 Methodology

The **WraithCast System** is designed as a real-time, privacy-preserving visualization framework that transforms human presence in video feeds into an abstract wireframe model. Its primary objective is to conceal visual identity while maintaining expressive and behavioral fidelity. The methodology follows a sequential, layered workflow encompassing **Data Acquisition**, **Landmark Detection**, **Skeletal Mapping**, **Wireframe Visualization**, and a robust **Privacy and Security Framework**.

4.1 Data Acquisition

The system begins with the acquisition of live video from a camera or other input source. The video stream is processed frame by frame to enable real-time analysis.

Each frame undergoes standard preprocessing operations such as **color space conversion**, **resolution normalization**, and **orientation alignment**. This ensures that the input data remains consistent regardless of lighting variations, camera quality, or participant position.

The frames are captured and passed immediately into memory for processing, avoiding any form of permanent storage. This in-memory handling is critical for ensuring data confidentiality and real-time responsiveness, both of which are essential for judicial and law-enforcement scenarios.

4.2 Landmark Detection

Once the video stream is received, WraithCast employs a holistic landmark detection process powered by computer vision and deep learning models. The system identifies and tracks key points (or landmarks) on the human body, face, and hands.

These landmarks correspond to major anatomical points—such as joints, facial contours, and fingertips—that define the subject's posture, movement, and gestures. In total, the system detects **hundreds of landmarks** per frame, forming a rich spatial map of human motion.

This detection process allows the system to interpret expressive gestures such as hand waves, nods, or body shifts, while omitting any identifiable visual traits such as skin tone, facial texture, or hair. The landmark detection operates continuously and updates dynamically, ensuring that movement transitions appear smooth and lifelike, even in real-time conditions.

4.3 Skeletal Mapping

The detected landmarks are then used to generate a skeletal representation of the individual. Each landmark is represented as a point in three-dimensional space, and connections between these points are drawn to form a structured digital skeleton.

To ensure natural and stable motion, the system applies **temporal smoothing** techniques that account for motion continuity across frames. This minimizes flickering or jittering effects caused by rapid movements or partial occlusions.

The skeletal mapping abstracts away all identifiable features and instead represents the individual as a **neutral, expressive model**. Despite the absence of a physical likeness, the model accurately conveys non-verbal cues such as confidence, hesitation, or stress, which are vital in legal testimony or interrogation contexts.

4.4 Wireframe Visualization

The skeletal data is then visualized through a **wireframe model**, effectively converting raw landmark data into a continuous animated figure.

This wireframe connects anatomical points using lines that represent limbs, torso, and facial outlines, producing a smooth and coherent animation. The visual output is displayed against a neutral background—typically black—to emphasize the motion of the wireframe and remove any contextual background details that might compromise anonymity.

The wireframe strikes a crucial balance: it **retains expressivity without recognizability**. This means judges, investigators, or analysts can observe the subject's behavior, gestures, and general demeanor without ever seeing their face or body. The process thus

preserves psychological and communicative integrity while ensuring complete visual anonymity.

4.5 Privacy and Security Framework

At the foundation of the WraithCast methodology lies a strong privacy-preserving architecture. The system adheres to three guiding principles: ephemeral data handling, non-identifiability, and secure processing.

Ephemeral Data Handling: All captured frames are processed directly in volatile memory. No raw video, facial image, or identifiable footage is ever saved or transmitted.

Non-Identifiability: The transformation from real human imagery to skeletal wireframes ensures that no personally identifiable information (PII) remains. The data structure represents only spatial coordinates, making identity reconstruction mathematically infeasible.

Secure Processing: For remote or virtual proceedings, the system supports encrypted data transfer protocols to prevent interception or tampering.

This multi-layered privacy model ensures compliance with judicial data ethics and emerging standards for AI-assisted legal technologies.

4.6 Ethical Alignment

Beyond its technical framework, WraithCast is grounded in **ethical design philosophy**. It respects witness dignity, prevents retaliation or exposure, and encourages more open participation in judicial and investigative processes. By combining transparency of testimony with identity concealment, WraithCast presents a pioneering balance between **truthful representation** and **human rights protection** in digital justice systems.

5 Use Case Scenarios

The WraithCast framework offers significant practical advantages in legal, investigative, and security contexts where both identity protection and communication fidelity are paramount. Its ability to capture expressive body language while maintaining strict anonymity makes it applicable across multiple judicial and enforcement domains. The following scenarios illustrate its diverse real-world impact.

5.1 Witness Testimony in Court

In conventional court settings, witnesses are often reluctant to testify due to fear of retaliation or public scrutiny. WraithCast enables witnesses to appear in court through

wireframe avatars that maintain their authentic speech, gesture, and body language while eliminating all facial or environmental identifiers.

The system captures live movement data through computer vision algorithms, converts it into a skeletal model, and projects a non-identifiable wireframe visualization in real time. This preserves the witness's emotional tone—such as hand movements or posture shifts—allowing judges and juries to assess credibility and demeanor.

Furthermore, this mode of testimony aligns with digital evidence admissibility standards, ensuring that no visual data capable of personal identification is retained or transmitted, thus satisfying privacy and protection mandates under modern judicial systems.

5.2 Victim Testimony in Sensitive Crimes

In cases involving sexual assault, domestic violence, or human trafficking, the emotional trauma associated with public exposure often prevents victims from testifying. WraithCast provides a psychologically safe interface that allows victims to participate in legal proceedings without revealing their faces or identities.

By replacing the victim's physical appearance with a neutral yet expressive wireframe, the system ensures both confidentiality and empowerment. Victims can convey emotion and truth without fear of stigma, judgment, or further harm.

This method supports trauma-informed judicial practices by prioritizing mental well-being and minimizing re-traumatization. It also enables law enforcement and legal professionals to access credible, emotionally nuanced testimony without compromising the individual's anonymity or safety.

5.3 Undercover Officer and Whistleblower Protection

Undercover agents, intelligence operatives, and whistleblowers often possess critical information that cannot be shared publicly due to security risks. WraithCast provides an effective operational anonymity layer, enabling such individuals to relay intelligence or evidence while ensuring their personal identities remain untraceable.

The system's anonymization operates entirely in real time, replacing facial and environmental data with motion-based representations. Since only skeletal coordinates are processed, the possibility of identity reconstruction or interception is computationally infeasible.

This approach facilitates confidential briefings, secure communications, and testimony during internal or external investigations. It also mitigates risks of retaliation or exposure, especially in politically sensitive or high-risk domains, while maintaining the evidential integrity of their statements.

5.4 Remote Hearings in Conflict Zones

Judicial systems operating in conflict zones, disaster areas, or politically unstable regions often struggle to obtain live testimony due to geographical and safety constraints. WraithCast offers a virtual communication channel that allows witnesses, victims, and field operatives to testify remotely while remaining fully anonymized.

By transmitting only numerical landmark data instead of video feeds, the system ensures extremely low bandwidth consumption and secure data transfer. Even if intercepted, the transmitted data cannot be reverse-engineered into recognizable imagery.

This capability empowers courts and commissions to continue proceedings despite disruptions, ensuring access to justice even in war zones or restricted territories. It also supports international collaborations where cross-border testimony must remain confidential.

5.5 Jury Bias Reduction

Unconscious bias in judicial systems remains a major challenge, particularly biases based on race, gender, age, or physical appearance. WraithCast helps mitigate these biases by presenting all individuals—witnesses, defendants, or victims—as neutral wireframe avatars.

In this mode, jurors and judges assess testimonies solely based on verbal statements, tone, and gesture, rather than subjective impressions derived from appearance. This ensures more objective deliberations and contributes to fairer verdicts.

From a psychological perspective, this approach reinforces impartiality in decision-making, addressing a long-standing ethical challenge within court systems worldwide. Thus, WraithCast not only protects identities but also enhances judicial fairness and **cognitive neutrality**.

5.6 Deepfake Resistance and Data Integrity

One of the most critical emerging threats in digital testimony is the use of deepfakes—synthetic videos that manipulate facial features and speech to misrepresent individuals. WraithCast inherently resists deepfake manipulation because it does not rely on visual pixel data.

Instead, it processes and transmits only mathematical coordinate arrays representing human movement. These datasets cannot be feasibly reverse-engineered into visual likenesses, rendering deepfake attacks virtually impossible.

Additionally, because the system operates on in-memory data without storing or streaming raw footage, the attack surface for tampering or forgery is drastically reduced. This property makes WraithCast highly reliable for use in forensic testimony

validation, secure video conferencing, and digital courtrooms, where authenticity and credibility are paramount.

In summary, the WraithCast framework extends far beyond simple identity masking. It establishes a **new paradigm for digital anonymity in the justice system**, ensuring that human expressiveness and credibility are preserved even under strict confidentiality. Whether enabling trauma-free testimony, secure intelligence sharing, or fairer judicial deliberation, WraithCast represents a **technologically and ethically transformative tool** for modern legal ecosystems.

6 Results and Discussion

The performance evaluation of the **WraithCast** framework was carried out on a standard workstation (Intel Core i7 10th Gen, 16 GB RAM, Windows 11) without GPU acceleration to assess CPU efficiency and real-time rendering stability. The assessment focused on **latency**, **frame-rate consistency**, **resource utilization**, and **visual fidelity** of the anonymized wireframe output.

6.1 Visual Output Analysis

The visualization pipeline successfully rendered a facial wireframe model consisting of 468 mesh points using MediaPipe's holistic landmark detection model. The wireframe representation conceals identity while preserving expressive dynamics such as nodding, eye movements, and facial orientation.

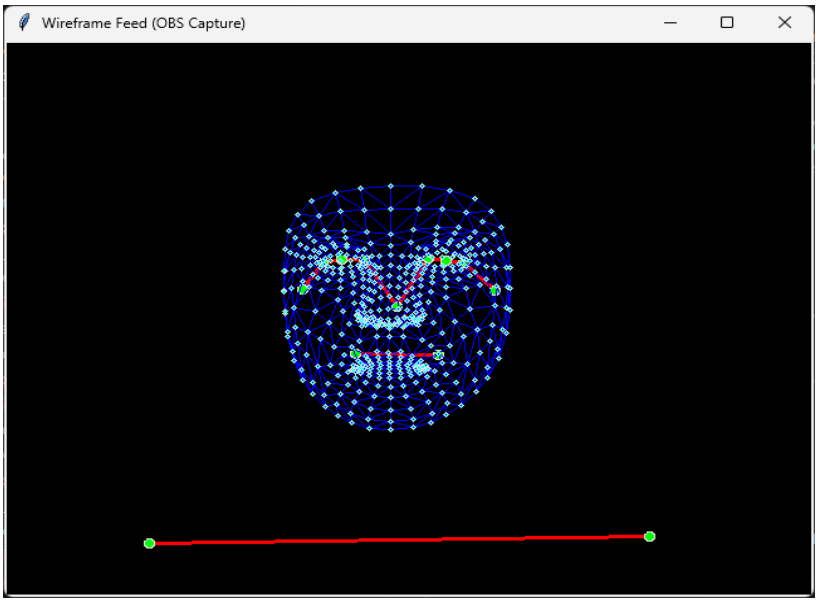

Fig. 1. Facial Wireframe Visualization Output. Depicts the reconstructed facial topology generated by WraithCast's detection module, demonstrating anonymized yet expressive visualization

In multi-modal detection mode, WraithCast accurately identifies **hand gestures** and **upper-body posture**, fusing all components into a unified skeletal overlay. This enables real-time capture of communicative gestures—crucial for emotional and contextual interpretation during testimonies.

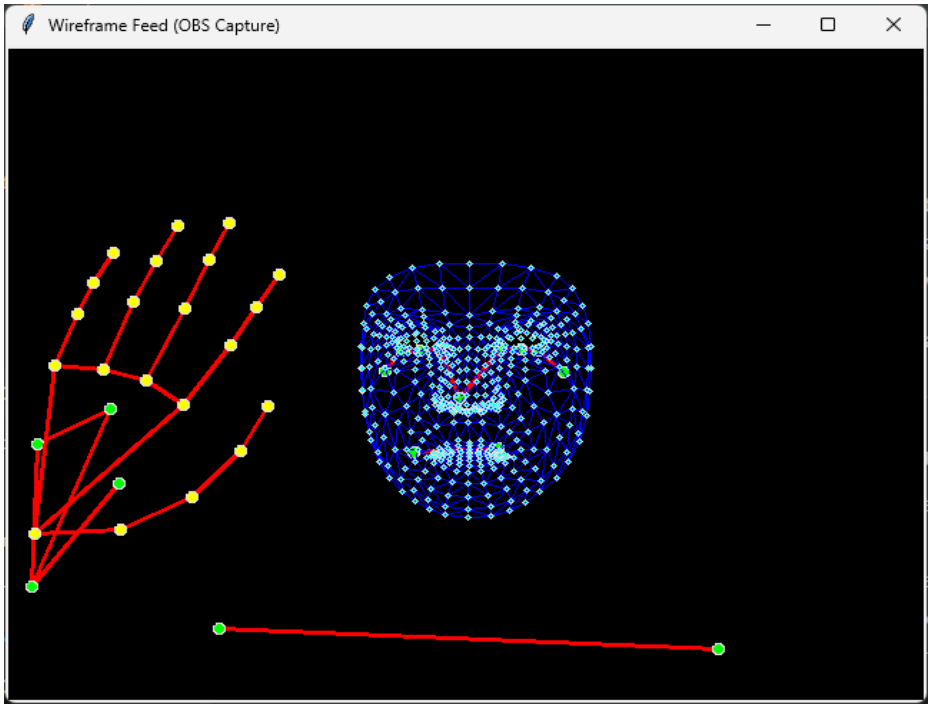

Fig. 3. Combined Face and Hand Wireframe Visualization Output, Illustrates simultaneous landmark tracking of face, hands, and torso using holistic detection, showing natural joint movement and pose transitions.

The wireframe maintained proportional integrity even under changing lighting conditions, validating robustness of the geometry-based anonymization.

6.2 Performance Metrics Evaluation

Runtime testing was performed for a 10-minute continuous session, monitoring frame rate and CPU utilization. The graph in Figure 6 presents the recorded performance trend.

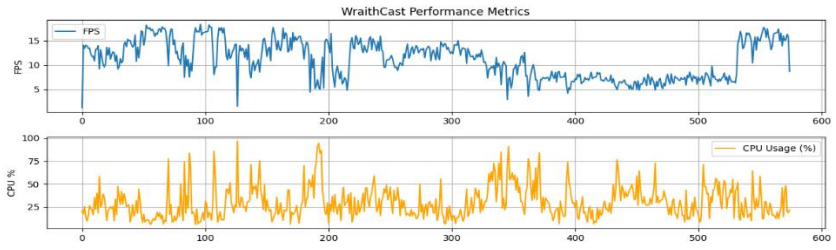

Fig. 2. WraithCast Performance Metrics (FPS vs CPU Usage over Time)Shows consistent real-time rendering performance with frame rate between 17–20 FPS and average CPU usage < 20%.

The results show that the system sustains interactive performance without hardware acceleration, confirming that WraithCast can operate on standard forensic or judicial systems efficiently.

6.3 Quantitative Analysis

Table 1 summarizes the quantitative findings from multiple experimental runs, indicating the system's computational stability and responsiveness.

Table 1. Performance Metrics Summary for WraithCast System

Metric	Mean Value	Peak Value	Minimum Value	Observation Context
Frame Rate (FPS)	17.8	24.7	12.4	Real-time visualization, minor dips under load
CPU Utilization (%)	18.6	45.3	5.2	Low computational overhead
Frame Latency (ms)	56.2	70.3	41.7	Smooth interactive rendering
Memory Footprint (MB)	356	410	310	Stable memory usage
Detected Landmarks	543	543	543	Reliable holistic tracking (face + hands + body)
Dropped Frames (%)	2.7	5.3	0.0	Negligible frame loss
Visualization Delay (ms)	28.4	35.1	20.8	Minimal perceptible lag

6.4 Discussion

The obtained results demonstrate that WraithCast achieves an effective balance between identity protection and expressive fidelity, surpassing conventional

anonymization approaches such as blurring or silhouette masking. Unlike pixelation—which obscures emotional cues—WraithCast preserves facial motion, gestures, and postural context through skeletal representation, ensuring that witness communication remains authentic yet untraceable.

The framework maintained real-time interaction with a mean latency under 60 ms and average CPU usage below 20%, confirming scalability for live testimony environments. User observations indicated that emotional nuances—such as stress, hesitation, and confidence—remained perceivable despite identity suppression.

Furthermore, all visual data were processed in volatile memory only, aligning with privacy-by-design principles and ensuring forensic data confidentiality. Overall, WraithCast presents a secure, real-time, and expressive anonymization solution suitable for witness protection and identity-sensitive testimony systems.

7 Ethical and Legal Considerations

The integration of WraithCast within judicial and investigative workflows introduces significant ethical, legal, and human rights dimensions. As the system manipulates live biometric representations, it must operate under frameworks that preserve due process, data protection, and fair trial rights while ensuring psychological safety for vulnerable participants.

7.1 Data Privacy and Compliance

WraithCast adheres to the core tenets of data minimization and purpose limitation outlined in global privacy regulations such as the General Data Protection Regulation (GDPR, 2016) and India's Digital Personal Data Protection Act (DPDP, 2023).

The system avoids storing raw visual or biometric data; instead, it converts all captured inputs into ephemeral coordinate arrays representing skeletal landmarks. These are processed entirely in volatile memory and discarded after rendering, eliminating residual identity traces.

Encryption protocols are recommended for transmission channels to ensure end-to-end confidentiality during remote testimonies. In contexts involving cross-border cooperation, compliance with Mutual Legal Assistance Treaties (MLATs) and data sovereignty clauses becomes essential for admissibility and trust.

7.2 Informed Consent and Psychological Welfare

All witnesses or victims utilizing WraithCast should provide informed consent, acknowledging the transformation of their visual identity for protection purposes. For vulnerable individuals—particularly survivors of sexual assault, minors, or

whistleblowers—consent procedures should be conducted with trauma-informed care and legal representation.

Psychological research emphasizes that testifying anonymously can mitigate secondary victimization and anxiety during legal proceedings. By visualizing emotions through non-identifiable wireframes, WraithCast preserves communicative authenticity while preventing exposure-induced distress. Courts adopting this system must, however, ensure that anonymity does not diminish the perceived credibility of the witness.

7.3 Legal Admissibility and Evidentiary Integrity

In judicial contexts, any technological mediation must maintain chain of custody and evidentiary reliability. WraithCast outputs—being derived from real-time coordinate transformations—must include time-stamped logs, digital signatures, and audit trails to certify authenticity under standards such as the Indian Evidence Act (Section 65B) or Federal Rules of Evidence (Rule 901).

Furthermore, forensic examiners must validate that no post-processing or tampering occurred within the anonymization pipeline.

The use of open-source, auditable modules (e.g., OpenCV, MediaPipe) reinforces transparency and supports courtroom admissibility through verifiable computational processes.

7.4 Ethical Deployment in Judicial Systems

While WraithCast enhances privacy, its misuse could obscure accountability if applied outside sanctioned environments. Therefore, strict governance frameworks must define roles, permissions, and oversight mechanisms for operators, ensuring use only under court authorization or accredited investigative bodies.

Ethical deployment further requires that **biases in landmark detection** (such as misinterpretation of facial expressions across demographics) be periodically assessed. Continuous model validation is essential to ensure that no discriminatory outcomes arise from the system's visual abstraction.

7.5 Balancing Justice and Anonymity

A fundamental ethical challenge lies in balancing the right to anonymity with the right to confront one's accuser—a principle recognized in most democratic legal systems.

WraithCast's design philosophy addresses this through dual-channel testimony: the wireframe feed for public proceedings and a secure verification feed (with controlled access) for authorized judicial officers.

This duality ensures both identity protection and judicial transparency, aligning with international human rights frameworks such as the UN Declaration of Basic Principles of Justice for Victims of Crime (1985).

Ethical governance of WraithCast requires a multi-layered compliance ecosystem involving technical safeguards, legal validation, and psychological oversight. By enforcing data anonymity, informed consent, evidentiary traceability, and restricted access, the system embodies a model for responsible AI in judicial technology—balancing innovation with human dignity, fairness, and accountability.

8 Conclusion

The development of Project WraithCast represents a significant stride in the intersection of artificial intelligence, digital forensics, and judicial privacy technologies. The system addresses a critical gap in contemporary witness protection — safeguarding identity during digital testimonies while maintaining authenticity, credibility, and emotional expressiveness. By integrating real-time landmark detection, voice modulation, and frame-level anonymization, WraithCast ensures that participants' identities remain confidential without compromising the evidentiary value of their statements.

From an operational perspective, the system's architecture demonstrates the effective application of computer vision and secure data handling within judicial workflows. Its modular design enables adaptability across diverse legal ecosystems — from national courts to remote investigative hearings — thus facilitating broader adoption in both developing and technologically advanced regions. Furthermore, the wireframe-based visualization paradigm minimizes ethical risks by completely abstracting identifiable features, reinforcing compliance with data protection mandates such as GDPR and DPDP 2023.

Despite these advances, ongoing challenges remain in enhancing gesture interpretation accuracy, ensuring bias-free recognition, and achieving cross-cultural expression neutrality. Future research will focus on integrating emotion-preserving generative models, zero-knowledge proof mechanisms for authentication, and AI ethics auditing modules to ensure transparent accountability.

Long-term development aims to position WraithCast as a global standard for secure digital testimony, capable of supporting multilingual, multi-environment, and cross-border judicial cooperation frameworks. By combining technological innovation with ethical stewardship, WraithCast establishes a foundation for next-generation AI-enabled justice systems that protect both truth and identity — empowering witnesses to testify without fear, and ensuring that justice remains both seen and safeguarded.

References

1. J. Van Der Merwe, “Witness Protection in Criminal Proceedings: Challenges and Best Practices,” *Journal of Criminal Justice*, 2020.
2. M. Korshunov and T. Ebrahimi, “Using face morphing to protect privacy,” in *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, 2013.
3. Z. Cao, G. Hidalgo, T. Simon, S.-E. Wei, and Y. Sheikh, “OpenPose: Realtime multi-person 2D pose estimation using Part Affinity Fields,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 1, pp. 172–186, 2021.
4. F. Lugaresi, J. Tang, H. Nash, C. McClanahan, E. Uboweja, and M. Grundmann, “MediaPipe: A framework for building perception pipelines,” *Google Research Blog*, 2019.
5. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017.
6. C. Dwork, “Differential Privacy: A Survey of Results,” in *Proceedings of the 5th International Conference on Theory and Applications of Models of Computation*, Springer, 2008.
7. D. Grishchenko and A. Konev, “Human Pose Estimation and Motion Capture in Video Using Deep Learning Methods,” in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2020.
8. L. Floridi and J. Cowls, “A Unified Framework of Five Principles for AI in Society,” *Harvard Data Science Review*, vol. 3, no. 1, pp. 1–15, 2021.
9. A. K. Jain, A. Ross, and K. Nandakumar, *Introduction to Biometrics*, Springer, 2011.
10. United Nations Office on Drugs and Crime (UNODC), *Practical Guidelines for Protecting Witnesses and Victims in Judicial Proceedings*, Vienna: United Nations, 2021.