Journal of
Information Hiding
and Privacy Protection

Tech Science Press

Doi:10.32604/jihpp.2025.066524

ARTICLE

Identity-Hiding Visual Perception: Progress, Challenges, and Future Directions

Ling Huang[1,2], **Hao Zhang**[1,2], **Jiwei Mo**[1,2], **Yuehong Liu**[1,2], **Qiu Lu**[1,2,*] **and Shuiwang Li**[1,2,*]

[1]College of Computer Science and Engineering, Guilin University of Technology, Guilin, 541006, China

[2]Guangxi Key Laboratory of Embedded Technology and Intelligent System, Guilin University of Technology, Guilin, 541004, China

*Corresponding Authors: Qiu Lu. Email: 2002021@glut.edu.cn; Shuiwang Li. Email: lishuiwang0721@163.com

Received: 10 April 2025; Accepted: 10 July 2025; Published: 31 July 2025

ABSTRACT: Rapid advances in computer vision have enabled powerful visual perception systems in areas such as surveillance, autonomous driving, healthcare, and augmented reality. However, these systems often raise serious privacy concerns due to their ability to identify and track individuals without consent. This paper explores the emerging field of identity-hiding visual perception, which aims to protect personal identity within visual data through techniques such as anonymization, obfuscation, and privacy-aware modeling. We provide a system-level overview of current technologies, categorize application scenarios, and analyze major challenges—particularly the trade-off between privacy and utility, technical complexity, and ethical risks. Furthermore, we examine regulatory trends and propose future research directions, including model-level privacy mechanisms such as federated learning and machine unlearning. By synthesizing insights across technical, ethical, and policy dimensions, this work offers a conceptual roadmap for developing responsible, privacy-preserving visual perception systems.

KEYWORDS: Identity-hiding; visual perception; privacy protection

1 Introduction

Visual perception technologies [1–3] have made significant strides in recent years, enabling a variety of applications that rely on capturing and analyzing visual information from the environment. These systems have become integral in industries ranging from security and surveillance to healthcare, autonomous vehicles, and smart cities [4–7]. For instance, surveillance systems are increasingly equipped with cameras capable of real-time facial recognition [8], tracking individuals through crowds, and detecting suspicious behavior. Similarly, autonomous vehicles [9] use visual perception to detect pedestrians, vehicles, and obstacles, ensuring safe navigation through complex environments. The growing reliance on these technologies is driven by the need for accurate, real-time data to support decision-making and operational efficiency in various sectors.

However, the widespread use of visual perception systems raises significant ethical and privacy concerns [10,11], particularly with regard to the identification and tracking of individuals. Many of these systems rely on the ability to recognize faces [12], analyze behaviors [13], or track movements [14], all of which can capture personally identifiable information (PII) without explicit consent. As these technologies become more pervasive, the potential for misuse grows [15], whether through unauthorized surveillance, profiling, or even the violation of civil liberties. For instance, facial recognition technology [16], while highly effective in public safety and law enforcement, has been criticized for its potential to infringe upon personal privacy, leading to concerns about state surveillance, discriminatory practices, and data misuse.

In response to these challenges, the concept of identity-hiding visual perception has emerged as a solution that aims to mitigate privacy risks while maintaining the functionality of visual perception systems. This approach seeks to prevent the capture, processing, or storage of identity-related information—such as facial features or other unique identifiers—by anonymizing or obfuscating such data during the imaging process. By ensuring that visual systems do not store or process personally identifiable information (PII), identity-hiding technologies can protect individuals' privacy without sacrificing the accuracy or effectiveness of the system itself. As shown in Fig. 1: The framework integrates real-time anonymization techniques within the imaging pipeline to systematically mask identity-specific details while retaining essential visual information.

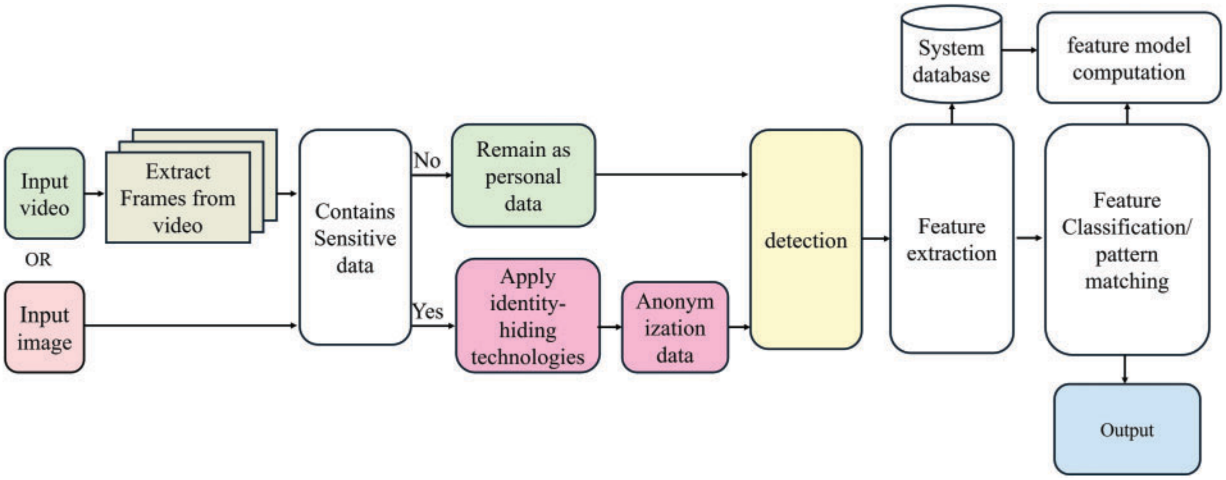

Figure 1: Description of identity concealment concept

The core goal of identity-hiding visual perception is to strike a balance between privacy protection and the operational needs of various applications. For example, in a surveillance context, identity-hiding systems can detect unusual activities or movements in public spaces without revealing the identities of individuals involved. Similarly, in healthcare, these technologies can allow for the monitoring and analysis of patient data without exposing sensitive personal information. By anonymizing the visual data while still capturing useful information for decision-making or analysis, identity-hiding visual perception systems present an innovative way to address privacy concerns while enabling the continued use of visual perception technologies.

However, the development and deployment of identity-hiding visual perception systems face a number of technical and ethical challenges. From a technical perspective, ensuring that these systems can effectively obfuscate identity-related data without compromising the utility or accuracy of the information being collected is a complex task. The need for real-time processing, high-resolution imaging, and minimal latency in many applications—such as autonomous driving and security surveillance—adds additional layers of difficulty. Furthermore, there are significant ethical considerations, including the potential for misuse of anonymization techniques, the trustworthiness of the systems, and the challenge of balancing privacy with the legitimate need for security and public safety.

While several surveys have reviewed individual anonymization techniques or discussed visual privacy more generally, there remains a gap in system-level analyses that integrate technical, ethical, and regulatory perspectives under the umbrella of identity-hiding visual perception. Most existing work focuses on either algorithmic detail or legal theory, leaving a need for interdisciplinary frameworks that bridge both.

To address this gap, this paper offers a comprehensive overview of identity-hiding visual perception from a multi-dimensional perspective. The main contributions are as follows:

- We define the concept and scope of identity-hiding visual perception as a distinct research direction, and analyze its practical relevance across key domains such as public safety, healthcare, and autonomous systems.
- We review representative identity-hiding techniques—including image blurring, pixelation, thermal imaging, depth-based abstraction, and generative obfuscation—and examine their respective trade-offs between privacy protection and visual utility.
- We explore the ethical risks and social implications of deploying identity-hiding systems, such as the potential misuse of anonymization, challenges in public trust, and the tension between privacy rights and public safety, while highlighting the importance of transparent governance mechanisms.
- We outline future research opportunities related to improving anonymization quality, ensuring real-time performance, and advancing privacy-aware visual perception through adaptive modeling and system-level integration.

The remainder of the paper is organized as follows: Section 2 presents related work, reviewing the current state of research in the field; Section 3 introduces the technical foundations and key methods; Section 4 discusses technical, ethical, and legal challenges; Section 5 outlines future research directions; Section 6 concludes with a summary and reflections on responsible development.

2 Related Work

With the growing societal concerns around visual privacy [10,17], researchers have increasingly turned their attention to identity-hiding techniques in computer vision. Several prior reviews and survey efforts have attempted to map this emerging field, but they often lack depth in categorizing technical strategies and fail to critically assess how well existing methods meet real-world demands. Many existing surveys narrowly focus on general privacy-preserving vision or specific use cases, offering fragmented overviews without addressing the systemic limitations and cross-domain applicability of identity-hiding methods. A more integrated and critical analysis is needed to connect algorithmic design with broader technical, ethical, and regulatory considerations.

Existing works can be broadly grouped into three methodological paradigms. The first is image-level anonymization [18], which uses techniques such as blurring, pixelation, and occlusion to obscure identifiable content. These methods are straightforward and computationally efficient but often result in significant loss of visual fidelity and task-relevant detail. The second is representation-level obfuscation [19,20], which aims to suppress identity information in latent features using strategies like adversarial training or disentangled representation learning. These approaches offer a better balance between privacy and utility but often suffer from instability and poor robustness in unconstrained environments. The third category is identity-neutral generation [21,22], which leverages generative models to create synthetic yet unidentifiable replacements for original visual content. While promising in visual realism, these methods face challenges in maintaining semantic consistency and model controllability.

Despite the technical progress, current research remains limited in scope and integration. Most methods are designed for isolated tasks and lack generalization across domains such as autonomous driving, healthcare, and smart city systems. Moreover, existing reviews often overlook essential system-level factors, including deployment efficiency, human interpretability, and compliance with emerging data protection norms. This paper addresses these gaps by providing a structured synthesis of identity-hiding visual perception research, critically evaluating the assumptions and boundaries of current methods, and offering a unified perspective that integrates privacy, functionality, and ethical responsibility across application contexts.

3 Opportunities of Identity-Hiding Visual Perception

The growing ubiquity of visual perception technologies—especially those relying on cameras, sensors, and advanced analytics—has resulted in increased concerns about privacy, particularly in public and sensitive spaces [23]. As these technologies evolve, the need to safeguard personal data while maintaining their functionality has become critical. Identity-hiding visual perception offers innovative opportunities to achieve this delicate balance. By protecting individual identities through anonymization techniques [24], these systems can retain the core benefits of visual perception—security, efficiency, and accuracy—while minimizing the risks to personal privacy. Below are some key opportunities where identity-hiding visual perception can be particularly transformative:

3.1 Enhancing Privacy in Surveillance Systems

Surveillance systems [25] have become ubiquitous components of urban and public safety infrastructure, designed to monitor public spaces, detect criminal activity, and enhance security. However, traditional surveillance methods that rely on facial recognition and other biometric identifiers pose significant privacy risks [26]. These systems can track and identify individuals in real time, raising concerns about unauthorized surveillance, profiling, and misuse of data.

Identity-hiding visual perception systems effectively address these concerns by anonymizing or obfuscating identity-related information such as faces, clothing, or distinguishing features while still enabling detection of suspicious activities or events. Instead of focusing on individuals' faces or personal identifiers, these systems emphasize broader patterns such as behavior analysis, movement trajectories [27–29], or detecting unusual objects in specific areas. By removing personally identifiable information (PII) from the data, these systems enable monitoring of public spaces without the invasive privacy risks associated with traditional surveillance.

Technically, common identity-hiding methods include thermal imaging, pixelation, and depth map processing. Thermal imaging uses infrared sensors to capture the heat emitted by the human body, producing thermal images that do not reveal facial details but still accurately indicate a person's location and movement. Pixelation reduces the resolution or blurs key regions such as faces to obscure identity features; this approach is simple and computationally efficient but may sacrifice image detail. Depth map processing leverages 3D spatial information from depth cameras to reconstruct the geometric structure of the scene rather than surface textures, thereby preserving privacy while supporting spatial behavior analysis. As shown in Fig. 2, these identity-hiding techniques effectively mask personal identity details while preserving essential scene information for analysis. The figure illustrates the application and differences among these methods, providing a clear visualization of the trade-offs between privacy protection and information retention.

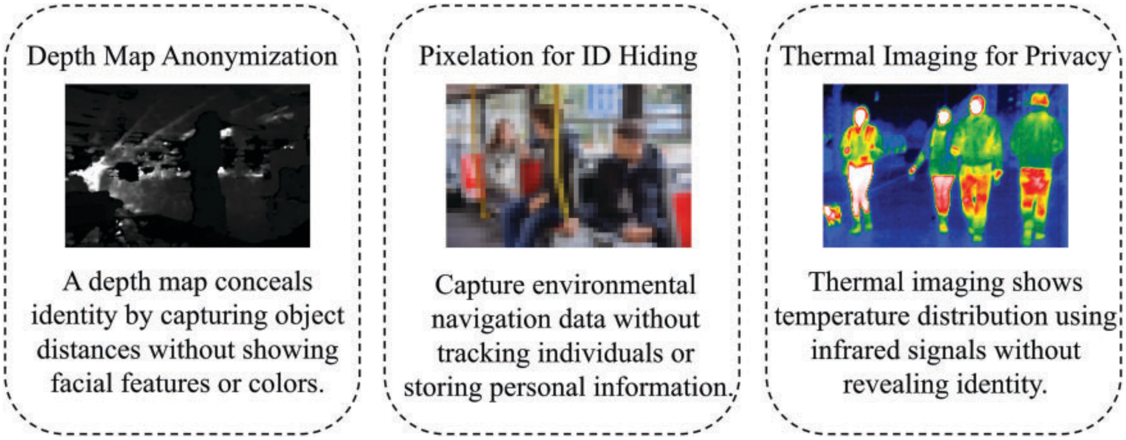
Depth Map Anonymization
A depth map conceals identity by capturing object distances without showing facial features or colors.
Pixelation for ID Hiding
Capture environmental navigation data without tracking individuals or storing personal information.
Thermal Imaging for Privacy
Thermal imaging shows temperature distribution using infrared signals without revealing identity.

Figure 2: Examples of image processing methods for identity hiding

These identity-hiding techniques offer clear advantages in privacy protection but come with trade-offs in performance. Thermal imaging is sensitive to environmental temperature variations and generally provides lower resolution, which can limit fine detail capture. Pixelation has low computational cost but may reduce accuracy in detecting subtle abnormal behaviors. Depth map processing requires specialized hardware and higher computational resources, increasing system complexity and deployment cost. Moreover, lacking direct identity information, these systems may face challenges in precisely identifying individuals or detecting anomalies in complex environments, potentially increasing false positives or negatives.

Overall, identity-hiding visual perception systems strike a balance between surveillance effectiveness and privacy protection, making them suitable for public safety applications where privacy concerns are paramount. Different techniques vary significantly in their level of privacy protection, identification accuracy, and computational demands. Practical deployment should carefully select or combine these methods based on specific requirements to achieve the best compromise between security and privacy.

3.2 Enabling Ethical Autonomous Systems

Autonomous systems, including vehicles, robots, and drones [30–32], rely heavily on visual perception for tasks such as navigation, object detection, and decision-making. These systems typically capture vast amounts of visual data in real-time to understand their environment and interact with the world around them. However, their deployment in public spaces raises privacy concerns, particularly when it comes to identifying or tracking individuals in ways that are not fully transparent or consented to.

By integrating identity-hiding technologies into the visual perception systems of autonomous vehicles [33] and robots, these systems can process visual data effectively while maintaining privacy. For example, an autonomous car might rely on visual perception to detect pedestrians and other vehicles, but using identity-hiding algorithms could prevent the system from recording identifiable features, such as a person's face or other private identifiers. Instead of relying on face recognition to track pedestrians, the system could focus on broader patterns of movement, ensuring that personal privacy is protected. As illustrated in Fig. 3: Identity Hiding Technology enables various autonomous platforms, including vehicles, drones, and service robots, to operate in public spaces without compromising individual privacy.

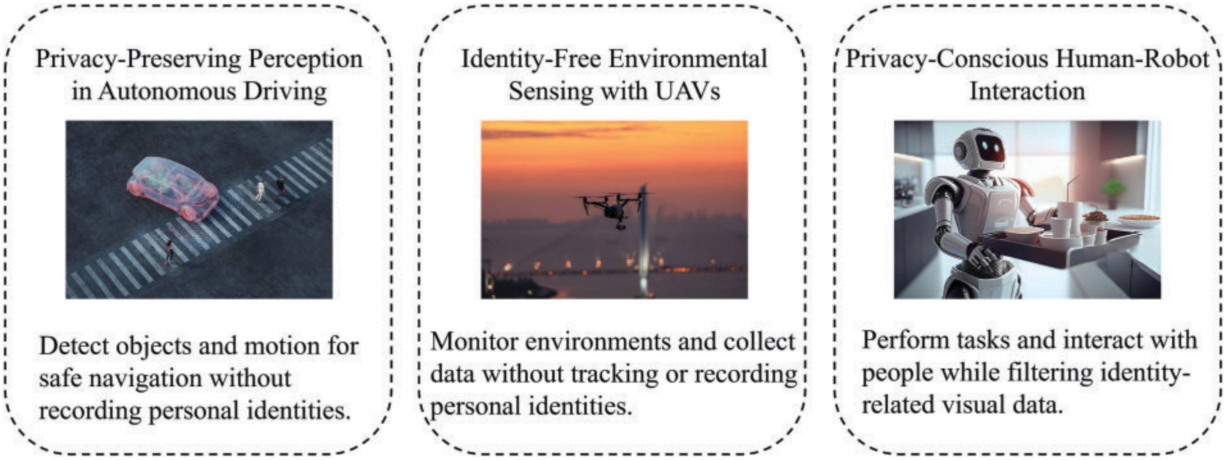
Privacy-Preserving Perception in Autonomous Driving
Detect objects and motion for safe navigation without recording personal identities.
Identity-Free Environmental Sensing with UAVs
Monitor environments and collect data without tracking or recording personal identities.
Privacy-Conscious Human-Robot Interaction
Perform tasks and interact with people while filtering identity-related visual data.

Figure 3: Application of identity hiding technology in autonomous systems

This technology could also extend to autonomous drones used for delivery or public monitoring. These drones could capture images of individuals in public spaces, but by anonymizing the data, their visual perception systems would only record environmental information necessary for navigation, without identifying or tracking individuals. This helps to make autonomous systems more ethical, addressing public concerns about unauthorized surveillance and privacy invasion while still allowing for safe and effective operation.

3.3 Safeguarding Healthcare Data

In healthcare, visual perception technologies are increasingly used for a range of applications [34–36], from non-invasive diagnostic tools to remote patient monitoring. These technologies offer a number of benefits, such as providing detailed imaging for diagnosis [37], improving the accuracy of medical assessments, and enabling real-time monitoring of patients' conditions. However, these systems often capture sensitive patient data, including identifiable visual features like faces, body shapes, or specific marks, which raises concerns about the privacy and security of healthcare information.

Identity-hiding visual perception can play a crucial role in addressing these concerns by anonymizing identifiable data during the imaging process. For instance, in telemedicine or remote health monitoring applications, where patients are video-monitored for health conditions, anonymization techniques could ensure that patients' identities are never exposed to healthcare providers or third parties. This would allow for the continued use of advanced imaging technologies—such as MRI scans, ultrasound, or CT scans—without violating privacy laws or breaching patient confidentiality. As illustrated in Fig. 4: The process begins with data acquisition, followed by systematic anonymization and validation steps, ensuring that all sensitive information is securely masked before further analysis is conducted.

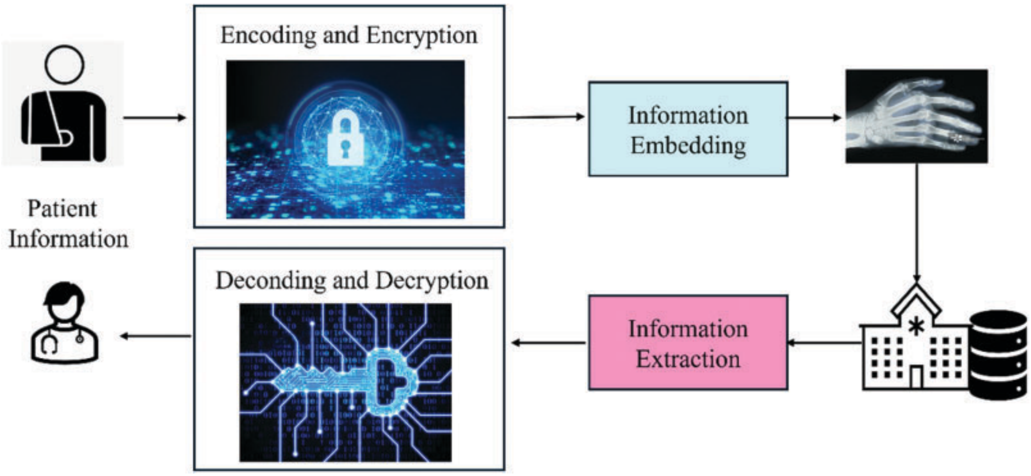

Figure 4: Flow chart of proposed methodology

Furthermore, in situations where large-scale health data is aggregated for research or diagnostic purposes, identity-hiding techniques can ensure that no personally identifiable information is included in datasets, thus enabling the use of real-world health data while protecting patients' privacy. Such applications would foster trust in digital healthcare systems, ensuring that patient information remains secure while still enabling the healthcare system to leverage visual perception technologies for improved patient care.

3.4 Privacy in Smart Cities and Public Spaces

Smart citie are transforming the way urban environments are managed, making use of sensors, cameras, and data analytics to optimize everything from traffic flow and energy use to public safety [38] and environmental monitoring. As the technology underlying smart cities becomes more advanced [39,40], vast amounts of visual and sensor data are collected in real-time, often from public spaces. While this data helps improve urban efficiency, it also introduces significant privacy risks, as personal identity data may be inadvertently captured in public areas.

Identity-hiding visual perception technologies offer a solution by ensuring that the data collected from public spaces is anonymized or obfuscated, thus protecting citizens' privacy while still allowing for the analysis of valuable information. For example, a smart city surveillance system [41] might analyze crowd density in real-time, detect traffic patterns, or identify potential hazards like abandoned vehicles [42], all without recording individuals' identities. By anonymizing data related to people's faces or other identifiable features, cities can still maintain a high level of security, operational efficiency, and public safety without compromising the privacy of their residents.

Additionally, these identity-hiding systems could help mitigate concerns around government surveillance and the growing presence of monitoring technologies in public spaces. By anonymizing data, cities can balance the need for data-driven innovation with the protection of civil liberties, ensuring that personal privacy is respected in an increasingly connected urban environment.

4 Challenges of Identity-Hiding Visual Perception

While identity-hiding visual perception offers significant opportunities for safeguarding privacy in visual data collection systems, it also introduces several challenges. These challenges stem from the complexity of implementing such technologies in real-world applications while ensuring that the systems remain functional, efficient, and ethically sound. As shown in Table 1, these challenges include technical complexity and performance trade-offs, ethical dilemmas and trust issues, as well as balancing privacy with utility.

Table 1: Challenges and responses to privacy protection technologies

Challenge	Cause	Solution
Technical complexity and performance trade-offs	Anonymizing identity data can reduce visual quality, affecting recognition, detection, and behavior analysis, while high computational demands can hinder real-time performance.	Use advanced anonymization algorithms, such as deep learning models with adjustable privacy levels; optimize resource management to improve real-time processing.
Ethical dilemmas and trust issues	Could be misused to evade responsibility, affecting public safety; privacy measures may reduce transparency and accountability; public doubts about system accuracy.	Establish clear ethical guidelines and usage restrictions; enhance system transparency to improve user understanding and trust.
Balancing privacy and utility	Anonymization may strip essential details, impacting fields like healthcare and surveillance that need precise data.	Develop anonymization techniques that retain essential features, such as encryption or partial obfuscation; optimize anonymization strategies based on context.

4.1 Technical Complexity and Performance Trade-offs

One of the primary challenges in developing identity-hiding visual perception systems lies in the technical complexity involved in anonymizing identity-related data without sacrificing the utility and accuracy of the visual information. Identity-hiding techniques, such as blurring, pixelation, or face obfuscation [43], are commonly used to mask identifiable features, but these techniques often compromise the quality of the captured data. For instance, blurring faces in surveillance videos or pixelating identifying details may prevent facial recognition, but it could also make it harder to track important events or accurately assess the behavior of individuals, ultimately reducing the system's effectiveness in detecting threats or understanding context.

In practical systems, identity-hiding methods generally fall into two categories: traditional visual transformations and learning-based approaches. Traditional methods such as blurring and pixelation are easy to implement and computationally lightweight, making them suitable for scenarios like public video release or child image protection, where privacy requirements are high and visual detail can be sacrificed. However, these methods often result in significant information loss and are insufficient for behavior analysis or high-precision tasks. In contrast, learning-based approaches such as GAN-based face replacement aim to preserve the visual realism of the scene while anonymizing identity-related regions. These are better suited for privacy-sensitive scenarios like remote conferencing or social media avatars but pose challenges such as high computational cost and the risk of generating synthetic faces that may be mistaken for real individuals, raising ethical concerns.

In more complex systems, such as autonomous vehicles or healthcare imaging [44,45], the challenge is even greater. Autonomous systems require precise detection and real-time processing of environmental information, including the identification of obstacles, pedestrians, and other vehicles. Anonymizing individuals' appearances without losing the ability to recognize objects or interpret complex visual data is a delicate balancing act. Similarly, in healthcare applications where visual data is critical for diagnosis and treatment planning, anonymizing certain features could inadvertently obscure key medical details or interfere with the accurate identification of conditions. For instance, anonymizing faces or other identifiable features might reduce the ability of doctors to track patient histories or accurately diagnose diseases.

Moreover, the computational demands of implementing identity-hiding techniques can significantly affect the performance of visual perception systems, especially in real-time applications. Identity-hiding technologies that involve advanced algorithms—such as differential privacy [46], adversarial machine learning [47], or deep neural networks designed to mask identities—can be computationally intensive. These systems may require significant processing power, leading to increased latency and slower response times. In resource-constrained environments, such as autonomous drones or mobile devices, these computational challenges can hinder the scalability and practical implementation of identity-hiding technologies.

4.2 Ethical Dilemmas and Trust Issues

While the potential for privacy protection through identity-hiding visual perception is significant, the technology also introduces ethical concerns that must be carefully navigated. One of the most pressing ethical dilemmas is the potential for abuse of anonymization techniques [48,49]. In certain contexts, the ability to anonymize identity-related data could be exploited to evade accountability or responsibility, undermining the overall effectiveness of the system. For example, in surveillance systems, the anonymization of faces could be used to conceal the identities of individuals engaged in criminal activities or to obstruct law enforcement efforts. This could lead to a loss of trust in the system and raise concerns about the integrity of the data being collected. A potential mitigation strategy is the implementation of role-based de-anonymization protocols, where authorized personnel under strict oversight can access original data for legitimate investigative purposes, balancing privacy with accountability.

Additionally, while the anonymization of personal data protects privacy, it may also hinder efforts to ensure transparency and accountability, especially in critical sectors such as law enforcement or healthcare [50]. For instance, in healthcare, the ability to trace patients' health progress over time is crucial for accurate diagnosis and treatment. The use of identity-hiding techniques may complicate this task by obscuring important medical information or hindering longitudinal tracking. This introduces a legal challenge in balancing patient privacy with the need for effective healthcare delivery. One possible approach is to design reversible anonymization mechanisms secured by encryption and strict access controls, enabling authorized clinicians to access identifiable information when necessary while maintaining privacy protections.

Another significant concern is public trust, which is essential for the adoption and success of identity-hiding technologies. Many users may be hesitant to trust such systems, particularly in high-stakes areas such as healthcare, finance, or public safety [51]. The ability to anonymize visual data raises questions about system accuracy and the potential for misinterpretation or false conclusions. For example, patients may worry that anonymization could lead to medical errors or reduced quality of care. Similarly, in surveillance, people may question whether obscured identities compromise the system's ability to detect and respond to threats. To address this, transparency is key. Clear communication about how the identity-hiding process works, what data is anonymized, and what safeguards are in place to protect privacy is vital for maintaining public confidence [52]. Furthermore, independent audits and certifications of identity-hiding technologies can reinforce trust by validating their reliability and ethical compliance.

4.3 Balancing Privacy and Utility

A significant challenge in developing identity-hiding visual perception systems is finding the optimal balance between privacy protection and system utility. While identity-hiding technologies are designed to anonymize personal data, they can sometimes restrict the functionality and effectiveness of the system. The process of anonymization, by its nature, can remove or obscure valuable data that could be critical for the task at hand, especially when high accuracy and detailed information are required.

For example, in healthcare, medical imaging technologies that rely on visual data—such as MRI scans, X-rays, or even telemedicine video consultations [53]—often require the use of patient-specific information to provide an accurate diagnosis or track health changes over time. Anonymizing patient faces or unique features may inadvertently hinder the doctor's ability to monitor specific conditions or provide personalized treatment. The challenge here is ensuring that anonymization does not interfere with the system's capacity to detect critical medical information.

In security and surveillance applications, the need to track and identify individuals over time can conflict with the goal of privacy protection [54]. For instance, in a public safety context, it may be necessary to track certain individuals or groups across various locations to detect potential threats or patterns of criminal activity. Anonymizing faces or identities could limit the system's ability to recognize individuals consistently, making it more difficult to monitor behavior or detect long-term threats. This trade-off between privacy and utility is particularly pronounced when the systems are tasked with identifying specific patterns—such as recognizing criminals or preventing terrorist activities [55]—where detailed visual data is essential.

The key challenge here lies in the system design. How can identity-hiding technologies be structured to retain useful features—such as activity recognition, object detection, or context analysis—while removing identifiable personal information [56] This requires careful consideration of both the specific application and the context in which the technology is deployed. It also necessitates the development of more sophisticated anonymization techniques that preserve the relevant details for tasks like behavior analysis or pattern detection, while ensuring that no personally identifiable information is captured or processed.

5 Future Directions and Conclusion

The field of identity-hiding visual perception is poised to play a pivotal role in advancing privacy protection while enabling the continued utility of visual technologies across a wide range of applications. As concerns about privacy and data security continue to escalate in our increasingly digital and connected world [57], the development of privacy-preserving technologies has never been more urgent. Identity-hiding systems, which anonymize personal information in visual data without sacrificing its usefulness, represent a promising solution. However, further research and development are necessary to overcome the existing challenges and unlock the full potential of these systems. As illustrated in Fig. 5: Several Key Future Directions for Identity-Hiding, future research focuses on enhancing anonymization algorithms, balancing privacy and utility in machine learning, establishing ethical standards, and expanding industry applications.

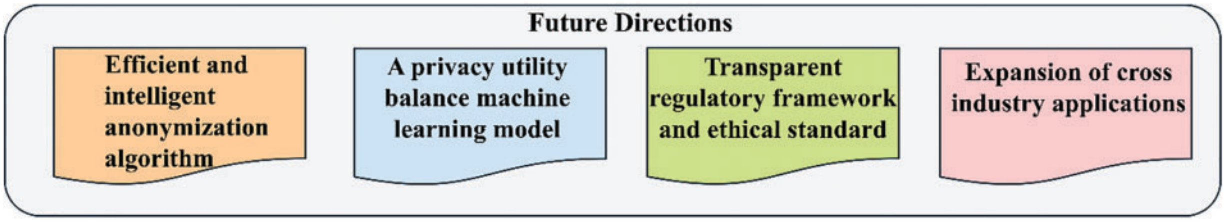
Future Directions
Efficient and intelligent anonymization algorithm
A privacy utility balance machine learning model
Transparent regulatory framework and ethical standard
Expansion of cross industry applications

Figure 5: The future development direction of identity hiding technology

5.1 Severval Key Future Directions for Identity-Hiding

To advance the development and comparability of identity-hiding methods, it is essential to establish a systematic evaluation framework. Existing studies commonly employ quantitative metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) to assess visual fidelity, as well as cosine similarity between face embeddings (e.g., using FaceNet or ArcFace) to measure residual identifiability. In practical applications, a two-dimensional evaluation is often necessary: (1) the degree of privacy achieved (i.e., how effectively identity has been removed), and (2) the preservation of downstream task performance (e.g., object detection, action recognition). The development of standardized privacy-utility benchmarks will be a crucial direction for future research to ensure both rigorous comparison and real-world deployment viability.

One of the most critical areas of future research in identity-hiding visual perception lies in improving the efficiency and effectiveness of anonymization algorithms. Current techniques [58] such as facial blurring or pixelation can distort or degrade the quality of visual data, which in turn impacts system performance. Future efforts should focus on developing more sophisticated anonymization methods that minimize the loss of useful visual information while ensuring strong privacy protection. Techniques like generative adversarial networks (GANs) [59] or deep learning-based models for data obfuscation could be explored to create more robust, dynamic systems that can anonymize identities without significant quality degradation.

Moreover, algorithms need to be designed with the capability to adapt to various real-world conditions, such as different lighting environments, occlusions, and motion dynamics. These developments could allow identity-hiding technologies to maintain high levels of accuracy, even in complex and fast-paced settings like urban environments or crowded public spaces. Research into more efficient methods of real-time processing, including edge computing or hardware acceleration, will be crucial for making these systems scalable and practical for deployment in resource-constrained scenarios, such as on mobile devices or autonomous vehicles.

5.2 Integration of Machine Learning Models for Privacy-Utility Balance

A promising future direction for identity-hiding visual perception is the integration of advanced machine learning models [60] that can intelligently balance privacy protection with system utility. Deep learning models, particularly those focused on unsupervised learning or reinforcement learning, could enable systems to automatically adjust the level of anonymization based on the context and requirements of the specific application. For example, a surveillance system could dynamically adjust the level of facial obfuscation depending on the security risk or the need for long-term tracking.

Despite the rapid development of identity-hiding algorithms, several practical challenges remain unresolved. For instance, deep learning-based anonymization models—such as GANs or privacy-aware transformers—often require high computational resources and large-scale training data, making them unsuitable for real-time applications on edge devices or embedded systems. Moreover, these methods may lack generalizability across different environmental conditions (e.g., lighting, occlusion, motion blur), which limits their robustness. Future work should therefore explore lightweight architectures, model pruning, and hardware-aware optimization strategies to reduce inference latency while preserving privacy guarantees. In addition, an important direction is the development of context-aware anonymization systems, capable of adjusting the level of identity masking dynamically based on application needs, such as prioritizing facial detail in healthcare versus stronger obfuscation in public surveillance.

Emerging privacy-preserving technologies are reshaping identity-hiding visual perception systems, offering new ways to balance utility and confidentiality. Federated Learning (FL) enables decentralized training across distributed edge devices without transmitting raw visual data, making it ideal for privacy-sensitive applications like cross-camera surveillance and multi-institutional healthcare diagnostics. By keeping data local, FL supports data sovereignty and regulatory compliance. In parallel, Machine Unlearning (MU) addresses ethical and legal concerns by allowing trained models to selectively forget specific user data, supporting consent withdrawal and data revocation. Furthermore, homomorphic encryption facilitates secure visual analytics by allowing computations on encrypted data, reducing exposure risks in remote diagnosis or telehealth scenarios. While these techniques are promising, they remain in early stages and face challenges such as computational overhead, scalability, and integration into real-time systems. Nonetheless, they are poised to play a pivotal role in building adaptive, accountable, and privacy-compliant visual perception frameworks.

5.3 Transparent Regulatory Frameworks and Ethical Considerations

As identity-hiding visual perception systems continue to evolve, there will be an increasing need for transparent regulatory frameworks that govern their ethical use. The introduction of these technologies into sensitive areas such as surveillance, healthcare, and public spaces requires clear guidelines to prevent misuse and ensure accountability. Governments, regulatory bodies, and industry leaders must collaborate to develop policies [61] that outline the appropriate use of these technologies while also safeguarding individuals' rights to privacy.

Ethical considerations will also play a central role in the future development of identity-hiding systems. It will be crucial to ensure that anonymization techniques do not undermine the accountability or transparency required in critical sectors, such as law enforcement or healthcare. Striking a balance between privacy protection and the ability to track, audit, or monitor activities in these sectors will require ongoing discussion and careful policy-making. Ensuring that individuals are informed about how their data is being used and protected will be essential for building public trust in these technologies.

At present, there is no unified international standard governing identity-hiding technologies in visual perception systems. However, several influential regulatory frameworks offer important guidance. For example, the General Data Protection Regulation (GDPR) in the European Union mandates that personally identifiable information (PII), including biometric data such as facial features, must be either explicitly consented to or effectively anonymized. Similarly, the California Consumer Privacy Act (CCPA) and China's Personal Information Protection Law (PIPL) impose strict controls on the collection, processing, and sharing of biometric visual data. In this context, identity-hiding techniques must adhere to principles such as data minimization, transparency, and accountability. Future systems should therefore implement auditable anonymization processes, support user opt-out mechanisms, and prioritize on-device or edge processing to reduce centralized data risks and improve compliance.

5.4 Expansion of Use Cases across Industries

As the underlying technologies advance, the use cases for identity-hiding visual perception will continue to expand. In the realm of smart cities [62], where surveillance and data collection are integral to managing urban infrastructure, privacy concerns are paramount. Identity-hiding visual perception could enable cities to monitor traffic flow, detect accidents, or improve public safety without exposing the personal identities of citizens. Cities could leverage anonymized data to improve urban planning, enhance security protocols, and create more livable environments, all while protecting citizens' privacy rights.

In healthcare, where the use of visual data for diagnostics, remote consultations, and patient monitoring [63] is on the rise, the need for privacy-preserving techniques is essential. Identity-hiding visual perception could allow healthcare professionals to work with sensitive data—such as medical images or video feeds from patient interactions—without risking the exposure of personal information. This would facilitate the use of telemedicine, automated diagnostics, and AI-driven health monitoring systems, while ensuring patient confidentiality.

Autonomous vehicles are another area where identity-hiding technologies could play a transformative role [64]. These vehicles rely on visual perception for navigation and interaction with the environment. By incorporating identity-hiding systems, autonomous vehicles could avoid capturing or processing personal data, ensuring that privacy is maintained even in scenarios where sensitive visual data is being collected, such as pedestrians, passengers, or individuals in nearby vehicles.

6 Conclusion

The development of identity-hiding visual perception technologies presents an exciting opportunity to address privacy concerns while enabling the continued use of powerful visual data systems. However, the challenges—ranging from technical limitations and ethical concerns to balancing privacy with system utility—must be carefully navigated. Ensuring that identity-hiding technologies can effectively anonymize personal data without compromising the functionality or accuracy of the system is a complex and ongoing task. Additionally, building trust in these technologies and addressing public concerns about their potential misuse will be critical for their successful adoption. Through continuous research and thoughtful implementation, it is possible to create identity-hiding systems that provide both privacy protection and functional utility, allowing for responsible and ethical use of visual perception technologies in a wide range of applications.

Acknowledgement: The authors would like to express their gratitude to the editors and anonymous reviewers for their insightful suggestions.

Funding Statement: This research was funded by the Guangxi Natural Science Foundation (Grant No. 2024GXNSFAA010484) and the National Natural Science Foundation of China (No. 62466013).

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: Ling Huang, Shuiwang Li; Data collection: Hao Zhang, Jiwei Mo, Yuehong Liu; Analysis and interpretation of results: Ling Huang, Hao Zhang, Qiu Lu; Draft manuscript preparation: Ling Huang, Shuiwang Li, Qiu Lu. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This article does not involve data availability, and this section is not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Dosovitskiy A, Beyer L, Kolesnikov A, Weissenborn D, Zhai X, Unterthiner T, et al. An image is worth 16x16 words: transformers for image recognition at scale. arXiv:2010.11929. 2020.
2. Jocher G, Qiu J, Chaurasia A. Ultralytics YOLO; 2023 [Internet]. [cited 2025 Jul 9]. Available from: https://github.com/ultralytics/ultralytics.
3. Wang L, Liu Y, Du P, Ding Z, Liao Y, Qi Q, et al. Object-aware distillation pyramid for open-vocabulary object detection. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition; 2023 Jun 17–24; Vancouver, BC, Canada. p. 11186–96.
4. Liu F, Lu Z, Lin X. Vision-based environmental perception for autonomous driving. Proc Inst Mech Eng Pt D J Automobile Eng. 2025;239(1):39–69. doi:10.1177/09544070231203059.
5. Yiong YT, Khairudin ARM, Redzuwan RM. Real-time substation detection and monitoring security alarm system. In: 2023 IEEE 11th Conference on Systems, Process & Control (ICSPC); 2023 Dec 16; Malacca, Malaysia. p. 1–6.
6. Nahar N, Hossain MS, Andersson K. A machine learning based fall detection for elderly people with neurodegenerative disorders. In: International Conference on Brain Informatics. Cham, Switzerland: Springer; 2020. p. 194–203.
7. Ali MA, Balamurugan B, Sharma V. IoT and blockchain based intelligence security system for human detection using an improved ACO and heap algorithm. In: 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE); 2022 Apr 28–29; Greater Noida, India. p. 1792–5.
8. Dong Z, Wei J, Chen X, Zheng P. Face detection in security monitoring based on artificial intelligence video retrieval technology. IEEE Access. 2020;8:63421–33. doi:10.1109/access.2020.2982779.
9. Wang L, Hua S, Zhang C, Yang G, Ren J, Li J. YOLOdrive: a lightweight autonomous driving single-stage target detection approach. IEEE Internet Things J. 2024;11(22):36099–113. doi:10.1109/jiot.2024.3439863.
10. Zhao R, Zhang Y, Wang T, Wen W, Xiang Y, Cao X. Visual content privacy protection: a survey. ACM Comput Surv. 2025;57(5):1–36. doi:10.1145/3708501.
11. Ardabili BR, Pazho AD, Noghre GA, Neff C, Ravindran A, Tabkhi H. Understanding ethics, privacy, and regulations in smart video surveillance for public safety. arXiv:2212.12936. 2022.
12. Chen W, Huang H, Peng S, Zhou C, Zhang C. YOLO-face: a real-time face detector. Vis Comput. 2021;37(4):805–13. doi:10.1007/s00371-020-01831-7.
13. Wu C, Cheng Z. A novel detection framework for detecting abnormal human behavior. Math Probl Eng. 2020;2020(1):6625695–9. doi:10.1155/2020/6625695.
14. Booranawong A, Jindapetch N, Saito H. A system for detection and tracking of human movements using RSSI signals. IEEE Sens J. 2018;18(6):2531–44. doi:10.1109/jsen.2018.2795747.
15. Handelman TA. Comparing the legal implications of AI-powered facial recognition technology in the USA, the EU, and China: safeguarding privacy, bias, and civil liberties. J Int'l L & Comp Stud. 2023;1:63.
16. Wang X, Wu YC, Zhou M, Fu H. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. Front Big Data. 2024;7:1337465. doi:10.3389/fdata.2024.1337465.
17. Padilla-López JR, Chaaraoui AA, Flórez-Revuelta F. Visual privacy protection methods: a survey. Expert Syst Appl. 2015;42(9):4177–95. doi:10.1016/j.eswa.2015.01.041.
18. Piano L, Basci P, Lamberti F, Morra L. Harnessing foundation models for image anonymization. In: 2024 IEEE Gaming, Entertainment, and Media Conference (GEM); 2024 Jun 5–7; Turin, Italy: IEEE. p. 1–5.
19. Bonchi F, Gionis A, Tassa T. Identity obfuscation in graphs through the information theoretic lens. Inf Sci. 2014;275(11):232–56. doi:10.1016/j.ins.2014.02.035.
20. Sun Q, Tewari A, Xu W, Fritz M, Theobalt C, Schiele B. A hybrid model for identity obfuscation by face replacement. In: Proceedings of the European Conference on Computer Vision (ECCV); 2018 Sep 8–14; Munich, Germany. p. 553–69.
21. He F, Fu S, Wang B, Tao D. Robustness, privacy, and generalization of adversarial training. arXiv:2012.13573. 2020.
22. Lecuyer M, Atlidakis V, Geambasu R, Hsu D, Jana S. Certified robustness to adversarial examples with differential privacy. In: 2019 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA: IEEE; 2019. p. 656–72.

23. Nissenbaum H. Protecting privacy in an information age: the problem of privacy in public. In: The ethics of information technologies. London, UK: Routledge; 2020. p. 141–78.
24. Majeed A, Lee S. Anonymization techniques for privacy preserving data publishing: a comprehensive survey. IEEE Access. 2020;9(1):8512–45. doi:10.1109/access.2020.3045700.
25. Mahdi FP, Habib MM, Ahad MAR, Mckeever S, Moslehuddin A, Vasant P. Face recognition-based real-time system for surveillance. Intell Decis Technol. 2017;11(1):79–92. doi:10.3233/idt-160279.
26. Iwaya LH, Fischer-Hübner S, Åhlfeldt RM, Martucci LA. mHealth: a privacy threat analysis for public health surveillance systems. In: 2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS); 2018 Jun 18–21; Karlstad, Sweden. p. 42–7.
27. Guo Y, Chen Y, Deng J, Li S, Zhou H. Identity-preserved human posture detection in infrared thermal images: a benchmark. Sens. 2022;23(1):92. doi:10.3390/s23010092.
28. Li Y, Wu Y, Chen X, Chen H, Kong D, Tang H, et al. Beyond human detection: a benchmark for detecting common human posture. Sens. 2023;23(19):8061. doi:10.3390/s23198061.
29. Huang L, Luo H, Mo J, Guo X, Lu Q, Li S. Human detection in low-resolution depth images. In: 2024 IEEE 2nd International Conference on Electrical, Automation and Computer Engineering (ICEACE); 2024 Dec 29–31; Changchun, China. p. 36–41.
30. Tang Y, Zhang C, Gu R, Li P, Yang B. Vehicle detection and recognition for intelligent traffic surveillance system. Multimed Tools Appl. 2017;76(4):5817–32. doi:10.1007/s11042-015-2520-x.
31. Robin C, Lacroix S. Multi-robot target detection and tracking: taxonomy and survey. Auton Robots. 2016;40(4):729–60. doi:10.1007/s10514-015-9491-7.
32. Du D, Qi Y, Yu H, Yang Y, Duan K, Li G, et al. The unmanned aerial vehicle benchmark: object detection and tracking. In: Proceedings of the European Conference on Computer Vision (ECCV); 2018 Sep 8–14; Munich, Germany. p. 370–86.
33. Xiong Z, Li W, Han Q, Cai Z. Privacy-preserving auto-driving: a GAN-based approach to protect vehicular camera data. In: 2019 IEEE International Conference on Data Mining (ICDM); 2019 Nov 8–11; Beijing, China. p. 668–77.
34. Boopathi S. Internet of things-integrated remote patient monitoring system: healthcare application. In: Dynamics of swarm intelligence health analysis for the next generation. Hershey, PA, USA: IGI Global; 2023. p. 137–61.
35. Esteva A, Chou K, Yeung S, Naik N, Madani A, Mottaghi A, et al. Deep learning-enabled medical computer vision. npj Digit Med. 2021;4(1):5. doi:10.1038/s41746-020-00376-2.
36. Ghoneim A, Muhammad G, Amin SU, Gupta B. Medical image forgery detection for smart healthcare. IEEE Commun Mag. 2018;56(4):33–7. doi:10.1109/mcom.2018.1700817.
37. Chen X. AI in healthcare: revolutionizing diagnosis and treatment through machine learning. MZ546 J Artif Intell. 2024;1(2):1–18.
38. Sha Y, Li M, Xu H, Zhang S, Feng T. Smart city public safety intelligent early warning and detection. Sci Program. 2022;2022(1):7552601 doi:10.1155/2022/7552601.
39. Lea R. Smart cities: an overview of the technology trends driving smart cities. IEEE Adv Technol Humanit. 2017;3:1–16.
40. Du R, Santi P, Xiao M, Vasilakos AV, Fischione C. The sensable city: a survey on the deployment and management for smart city monitoring. IEEE Commun Surv Tut. 2018;21(2):1533–60.
41. Santana JR, Sánchez L, Sotres P, Lanza J, Llorente T, Munoz L. A privacy-aware crowd management system for smart cities and smart buildings. IEEE Access. 2020;8:135394–405 doi:10.1109/access.2020.3010609.
42. Ahindu A. Detecting abandoned vehicles in public vehicle parking environment-based on time [master's thesis]. Nairobi, Kenya: University of Nairobi; 2017.
43. Lander K, Bruce V, Hill H. Evaluating the effectiveness of pixelation and blurring on masking the identity of familiar faces. Appl Cogn Psychol. 2001;15(1):101–16. doi:10.1002/1099-0720(200101/02)15:1<101::aid-acp697>3.0.co;2-7.
44. Bera S, Khandeparkar K. AI based real-time privacy-aware camera data processing in autonomous vehicles. In: 2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS); 2023 May 18–20; West Lafayette, IN, USA. p. 1–5.

45. Kim J, Park N. A face image virtualization mechanism for privacy intrusion prevention in healthcare video surveillance systems. Symmetry. 2020;12(6):891. doi:10.3390/sym12060891.
46. Wen Y, Liu B, Ding M, Xie R, Song L. IdentityDP: differential private identification protection for face images. Neurocomputing. 2022;501(2):197–211. doi:10.1016/j.neucom.2022.06.039.
47. Yang X, Dong Y, Pang T, Su H, Zhu J, Chen Y, et al. Towards face encryption by generating adversarial identity masks. In: Proceedings of the IEEE/CVF International Conference on Computer Vision; 2021 Oct 11–17; Montreal, QC, Canada. p. 3897–907.
48. Weicher M. [Name withheld]: anonymity and its implications. Proc Am Assoc Inf Sci Technol. 2006;43(1):1–11.
49. Davis S, Arrigo B. The Dark Web and anonymizing technologies: legal pitfalls, ethical prospects, and policy directions from radical criminology. Crime Law Soc Change. 2021;76(4):367–86. doi:10.1007/s10611-021-09972-z.
50. Dove ES, Phillips M. Privacy law, data sharing policies, and medical data: a comparative perspective. Medical data privacy handbook. Cham, Switzerland: Springer; 2015. p. 639–78.
51. Ioannou A, Tussyadiah I. Privacy and surveillance attitudes during health crises: acceptance of surveillance and privacy protection behaviours. Technol Soc. 2021;67(1):101774. doi:10.1016/j.techsoc.2021.101774.
52. Gritzalis A, Tsohou A, Lambrinoudakis C. Transparency-enabling information systems: trust relations and privacy concerns in open governance. Int J Electron Gov. 2019;11(3–4):310–32. doi:10.1504/ijeg.2019.103717.
53. Sharma SK. Use of AI in medical image processing. In: Future of AI in medical imaging. Hershey, PA, USA: IGI Global; 2024. p. 1–18.
54. Dobos S, Bagrin V. The balance between privacy and safety: the ethics of public video surveillance. 2024 [Internet]. [cited 2025 Jul 9]. Available from: http://repository.utm.md/handle/5014/28084.
55. Rubinstein IS, Hartzog W. Anonymization and risk. Wash L Rev. 2016;91:703.
56. Moon J, Bukhari M, Kim C, Nam Y, Maqsood M, Rho S. Object detection under the lens of privacy: a critical survey of methods, challenges, and future directions. ICT Express. 2024;10(5):1124–44. doi:10.1016/j.icte.2024.07.005.
57. Hagen J, Lysne O. Protecting the digitized society—the challenge of balancing surveillance and privacy. The Cyber Defense Review. 2016;1(1):75–90.
58. Maity A, More R, Kambli G, Ambadekar S. Preserving privacy in video analytics: a comprehensive review of face de-identification and background blurring techniques. TechRxiv. 2023. doi:10.36227/techrxiv.24587100.v1.
59. Al-Khasawneh MA, Mahmoud M. Safeguarding identities with GAN-based face anonymization. Eng Technol Appl Sci Res. 2024;14(4):15581–9.
60. Liu B, Ding M, Shaham S, Rahayu W, Farokhi F, Lin Z. When machine learning meets privacy: a survey and outlook. ACM Comput Surv (CSUR). 2021;54(2):1–36. doi:10.1145/3436755.
61. Hirsch DD. The law and policy of online privacy: regulation, self-regulation, or co-regulation. Seattle UL Rev. 2010;34:439.
62. Cui L, Xie G, Qu Y, Gao L, Yang Y. Security and privacy in smart cities: challenges and opportunities. IEEE Access. 2018;6:46134–45. doi:10.1109/access.2018.2853985.
63. Selvaraj P, Doraikannan S. Privacy and security issues on wireless body area and IoT for remote healthcare monitoring. Intelligent pervasive computing systems for smarter healthcare. Hoboken, NJ, USA: Wiley; 2019. p. 227–53.
64. Kim S, Shrestha R, Kim S, Shrestha R. Security and privacy in intelligent autonomous vehicles. Automotive cyber security: introduction, challenges, and standardization. 1st ed. Singapore: Springer; 2020. p. 35–66.