CCTV Footage De-identification for Privacy Protection: A Comprehensive Survey

Sekione Reward Jeremiah[1], Oscar Enrique Llerena Castro[1], Pradip Kumar Sharma[2], Jong Hyuk Park[1]*

[1] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Korea
[2] Department of Computer Science, University of Aberdeen, UK
{reward, researcher1}@seoultech.ac.kr, pradip.sharma@abdn.ac.uk, jhpark1@seoultech.ac.kr

Abstract

Privacy preservation is a significant concern in our data-driven society, both in the social and political spheres. These concerns are amplified by the continuous emergence of technologies and services, expanding the boundaries of what is possible in our modern era. Technologies, such as audio-video surveillance, play an essential role in security and law enforcement but can potentially lead to privacy breaches. One of the approaches for privacy preservation in still images and video is de-identification which involves replacing or concealing personal identifiers to prevent unauthorized, unintended use or disclosure of personal information. This paper comprehensively reviews privacy and security issues in closed-circuit television (CCTV) data streams, representative state-of-the-art de-identification techniques for privacy protection. We also present a service scenario in which a MEC-enabled distributed system is used for CCTV footage de-identification and re-identification for individuals' privacy protection. Finally, we highlight open research challenges and future directions for privacy protection in CCTV footage.

Keywords: CCTV footage, Personal identifiers, Privacy protection, De-identification, Security

1 Introduction

Modern technologies have significantly enhanced the capabilities and reach of video surveillance systems, also known as closed-circuit television (CCTV). These advancements have improved the quality of surveillance and expanded its applications. Furthermore, advances in smart multi-camera networks, multispectral image sensors, wireless networks, distributed computing, and audio-sensor arrays have contributed to surveillance systems advancements. However, this progress has also raised serious privacy concerns, as these systems capture, store, and analyze a vast amount of personal data [1].

The implementation of CCTV recording and surveillance systems is justified by their essential role in maintaining security, aiding law enforcement, and predicting disasters. Modern surveillance systems are equipped with image tracking capabilities, which monitor and analyze the movement of objects or individuals within images or video footage captured by CCTV cameras. Tracking an individual or object of interest is done in real-time or later for reference. Cities like London, Los Angeles, Beijing, and Seoul have installed millions of surveillance cameras to monitor public spaces for crime prevention [2]. However, increased surveillance systems usage can potentially infringe on individuals' privacy.

Moreover, services such as Google Street View, Yandex, and Naver maps, which provide panoramic views of streets worldwide, can also contribute to privacy issues [3]. While these technologies offer a wealth of visual information about urban environments, they also raise privacy concerns. They capture detailed images of streets, communities, and sometimes private spaces, potentially revealing personal information without individuals' consent [4]. Furthermore, these technologies' object detection and blurring precision are not 100% efficient. For instance, Google reported that its automatic system could blur 94-96% of license plates and 89% of faces meaning at least 4% of license plates and 11% of faces go undetected and unblurred [5].

Given these issues, significant research efforts have been directed toward developing methods and tools to protect individuals' privacy by removing or modifying personal identifiers in CCTV recordings and other multimedia content. Personal identifiable information or personal identifiers allows one's identification, and de-identification is the process of removing or concealing personal identifiable information. There are several biometric personal identifiers; however, the face is the primary identifier, and most studies focus on face blurring.

Nevertheless, there remains a lack of sufficient review studies focusing on state-of-the-art technologies, tools, and their limitations. Existing surveys are either technology-specific, scenario-specific, or problem-driven, thus making it challenging to summarize existing solutions in a macroscopic way. Moreover, there are specific challenges to de-identifying still images, text, audio, and videos, thus necessitating an organized review to pinpoint them and the way forward.

This paper focuses on privacy preservation in CCTV footage to bridge the gap. It systematically and comprehensively surveys de-identification techniques applicable to CCTV footage for visual privacy protection. The survey covers biometric, non-biometric, and soft-biometric identifiers. It provides insights into the current state-of-the-art de-identification techniques, identifies

*Corresponding Author: Jong Hyuk Park; E-mail: jhpark1@seoultech.ac.kr
DOI: 10.53106/160792642024052503004

remaining challenges, and discusses the way forward for visual privacy protection in CCTV footage. A case study scenario is provided as a possible solution to the existing challenges. Finally, we highlight future research areas and provide recommendations for researchers and practitioners.

The remaining paper sections are organized as follows: Section 2 discusses the research background, focusing on personal identifiers, and summarizes related works. AI and blockchain-based deidentification solutions for visual privacy protection are discussed in Section 3. Section 4 presents the deidentification service scenario, open challenges, and future directions. Section 5 concludes the work and provides recommendations for future work.

2 Research Background

This section explains the key considerations of this study and then explores categories of personal identifiers in multimedia content. Furthermore, visual privacy, image tracking system characteristics, and recent related works are examined in this section.

2.1 Key Considerations

The key considerations of our work are as follows:

- *Privacy*: a personal right to control the extent of personal information usage and exposure and prevent disseminating sensitive information into the public sphere. This protection extends to visual data such as images, generally termed visual privacy protection.
- *CCTV Footage*: the multiple forms of media, such as audio, images, and video, integrated into a single experience.
- *Human and Computer Vision (CV)*: CV technologies can identify and comprehend visual data for information extraction, offering numerous advantages and presenting significant privacy risks. Human vision (HV) allows individuals to derive meaning from what they see; therefore, it is paramount to develop privacy protection mechanisms against HV.

2.2 Image Tracking Systems

An image tracking system is a mechanism employed to trace the movement trajectory of an object captured by a CCTV within an integrated video network [6]. The fundamental objective of image tracking systems is to follow the movement trajectory of a particular person or an object. These systems are employed in scenarios necessitating continuous tracking or identification of a specific person's activities, either in real-time or for reference later. Nonetheless, the analysis of people and objects, which has significantly advanced owing to imaging systems, is debatable due to concerns over privacy violations. As such, it necessitates implementing measures to safeguard the privacy of innocent individuals who are inevitably "captured" in these recordings.

2.3 Privacy Issues in CCTV Visual Contents

Privacy interpretation varies depending on a society's legal, social, cultural, and technological contexts. For example, while some cultures may prioritize the right to privacy, others may prioritize the need for surveillance and security. Privacy concerns arise when personal information is collected and shared without the permission of the individual in question. Privacy violations can occur in various ways, but in both cases, it involves sensitive personal information being accessed or used without the individual's consent or knowledge. Here are the security and privacy concerns in CCTV footage:

1. The data may be gathered and disseminated without a person's awareness or consent.
2. Data initially gathered for specific purposes may be utilized for unlawful or unanticipated purposes.
3. Users' biometric information is susceptible to unauthorized access and misuse. It can be duplicated or deleted and exploited for purposes other than the intended raising security concerns.
4. Biometric data can disclose sensitive personal information such as mental and physical health status, ethnicity, race, gender, etc.

2.4 Multimedia Contents Identifiers Taxonomy

We consider the taxonomy shown in Figure 1, drawing from the principles of the Safe Harbour approach [7] for our study, which includes biometric, non-biometric, and soft-biometric identifiers, as explained below.

- *Biometric Identifiers*: Biometric identifiers involve physiological or behavioral characteristics that can be used to identify individuals, such as fingerprints, facial features, ears, and iris scans. These features are highly personal and unique to an individual, making them particularly sensitive to privacy concerns. Biometric data de-identification involves modifying data; thus, the original biometric features are no longer recognizable while preserving data statistical properties [8]. One approach for biometric de-identification is replacing the original biometric data with a synthetic template or hash value that preserves some of the identifying features of the original data but does not allow for the reconstruction of the original biometric data.
- *Non-biometric Identifiers:* information that can potentially identify individuals without relying on physiological or behavioral characteristics (e.g., facial hair styles and vehicle plate numbers). Techniques used for non-biometric de-identification involve masking, hashing, or substituting identifiers with additional data to render them less recognizable. To maintain data utility, de-identified data must retain its original structure and context [9].
- *Soft-biometric Identifiers:* Physical or behavioral characteristics that can provide information about an individual but are not unique enough to differentiate them from others make up soft biometric identifiers. Ethnicity, gender, age, race, tattoos, scars, and body marks comprise soft biometric identifiers. These identifiers can be used with primary biometric identifiers to improve recognition accuracy in less clear scenarios such as long-distance recognition.

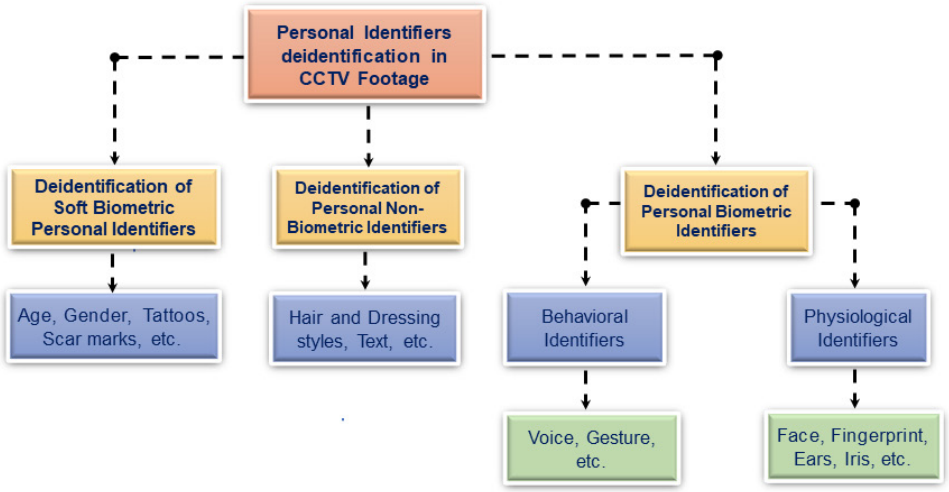


Figure 1. CCTV footage personal identifiers taxonomy

Table 1. Comparison of existing surveys and this survey

Ref.	CV	Video	Images	Biometric Identifiers	Non-biometric Identifiers	Soft-biometric identifiers	Focus
[10] (2022)	√√	√√	√√	N/A	N/A	N/A	Privacy based on machine learning
[11] (2022)	N/A	√√	√√	N/A	N/A	N/A	Differential privacy for unstructured data
[12] (2023)	√√	✗	√√	✗	√√	✗	Online social networks images
[13] (2015)	√√	✗	√√	✗	✓	✗	Surveillance systems images
[14] (2023)	√√	√√	√√	✗	✗	✓	Facial recognition systems
[15] (2021)	√√	✗	√√	✗	✗	✗	Facial biometrics
This study	√√	√√	√√	√√	√√	√√	CCTV footage de-identification (biometric, non-biometric, soft-biometric identifiers)

Note: √√ = Explicitly mentioned, ✓ = Partially covered, ✗= survey did not explicitly mention/include the item.

2.5 Existing Surveys Analysis

Studies addressing this subject can be classified into surveys on specific scenarios, specific privacy concerns, and technologies, as elaborated hereafter.

- *Specific Technologies*: These studies review technologies aimed at addressing certain privacy issues. Liu et al. [10] provide an overview of privacy attacks and protective measures based on machine learning, specifically targeting the security of visual content. Meanwhile, Zhao et al. [11] reviewed protection strategies for differential privacy applications for unstructured data content, including (but not limited to) image and video data.
- *Specific Scenarios*: These reviews examine privacy issues within specific contexts and scenarios. Given the privacy threats associated with image sharing on social networks, Liu et al. [12] propose a privacy protection framework, categorizing and reviewing existing strategies. CV advancements have significantly enhanced the capacity to automate surveillance data processing, posing a substantial privacy risk. Padilla-López et al. [13] reviewed image privacy in surveillance systems, offering a classification and summary of various strategies. Hasan et al. [14] reviewed automated face detection studies and recognition systems privacy concerns, discussing their limitations and potential future development.
- *Specific Privacy Concerns:* these studies review specific privacy issues without considering the technologies and scenarios involved. For instance, [15] concerns the privacy of facial images, introducing the primary concepts, characteristics, and challenges of protection technologies.

The main distinction between this study and earlier review studies lies in its coverage of privacy issues and countermeasures associated with visual content, as opposed to a restricted selection of a few problems and technology. Moreover, earlier studies have adopted a problem-centric approach, focusing on a particular subject or context. The key difference of this work for the previous one is summarized in Table 1.

3 Technology-enabled Solutions for Deidentification

This section covers Deep Learning (DL) and blockchain-based solutions for de-identifying personal information in CCTV footage. The section also discusses the advantages and limitations of these solutions in achieving effective de-identification while maintaining data privacy.

3.1 Deep Learning-based Solutions

Liu et al. in [16] present a model for protecting the privacy of face images using facial feature analysis and Generative Adversarial Network (GAN). The aim is to safeguard the user's privacy without compromising the image's usability for the online media domain. The model presented in this work is evaluated on two widely used face datasets in facial research, and the results show that it outperforms other face privacy protection methods. The experimental results demonstrate that the generated protected image retains essential features other than facial features and significantly reduces the recognition rate in the face recognition model.

Wen et al. [17] present a modular architecture for reversible face video de-identification named IdentityMask, incorporating deep motion flow to avoid needing per-frame evaluation for more efficiency. The proposed model comprises two distinct stages: concealing personally identifiable information by generating an IdentityMask, and the recovery stage allowing removing the protective mask if the correct key is provided. The IdentityMask model performs better than other state-of-the-art methods in protecting privacy.

Another recent work by Kim et al. [18] proposed a real-time face de-identification system to prevent personal information leakage in video surveillance systems by modifying face pixels to make them unrecognizable. The proposed design was optimized for inference using TVM-based DL inference optimization and task-level pipeline parallelism. The authors showed through experimental results that the proposed approach effectively de-identifies images in real-time.

The study by Lee et al. [19] addresses data privacy in deep-learning-based computer vision technologies using a wireless channel as differential privacy noise. The system uses deep neural networks (DNN) to construct its three main parts: the transmitter, wireless channel, and receiver. The authors report extensive evaluations of the proposed system, demonstrating its effectiveness in de-identifying transmitted face images while maintaining usefulness and showing potential for wireless privacy protection.

Authors in [20] propose a solution to biometric data leakage in the CCTV IoT environment and present a method to de-identify metadata and face information at different levels based on the user's authority and the subject's risk level. They suggest classifying access rights to anonymous data according to four roles and providing only differentially de-identified data according to the authority of the accessor. The required execution time for the de-identification of one image was found to be shortened with an increase in dataset.

3.2 Blockchain-based Solutions

Lee et al. [21] introduced a novel approach for a cloud-based CCTV blockchain system that addresses the security and privacy concerns arising from malicious attackers and untrusted third parties in the CCTV cloud system for both original and de-identified videos. The proposed technique employs a Merkle-Tree facilitating transmission efficiency transmission of video data, thereby reducing transmission bandwidth. This approach assures security privacy preservation by encrypting transmitted data, making it challenging to launch sniffing attacks.

Kim et al. [22] propose a privacy-preserving mechanism for video surveillance systems (VSSs). The proposed mechanism reduces the likelihood of face forgery by recording the original image of the virtualized face on a blockchain. The proposed tool converts the original images into a non-identifiable format to prevent disclosure and stores the face area separately in a secure blockchain-based database. The approach presented in this study protects the privacy of recorded individuals utilizing intelligent video surveillance systems (IVSSs).

Khan et al. [23] proposed a blockchain-based system to ensure the authenticity and integrity of video recordings captured by surveillance cameras in smart cities. Dharani et al. [24] offer a secure information-sharing mechanism to address security and privacy issues faced by city applications, focusing on surveillance applications, and present a system that integrates blockchain technology with intelligent IoT devices.

4 Deidentification Service Scenario and Open Challenges

This section discusses technical aspects and service scenarios for deidentification, crucial for protecting sensitive personal information and maintaining privacy in CCTV footage, and the open research challenges.

4.1 MEC Distributed System for Video De-ID and Re-ID for Privacy Preservation in CCTV Footage

The proposed system architecture is structured into four layers, illustrated in Figure 2.

- *The data acquisition layer:* Consists of CCTV cameras connected to edge servers through high-speed data connections (fiber, 5G), mitigating communication speed as a constraint. The edge server must address factors like resolution, color-depth scale, and occlusion from the diverse array of CCTV cameras during footage processing.
- *Edge layer*: Comprised of four primary processes, the initial stage involves a frame pre-processing module standardizing video frame resolution and color depth. Subsequently, face detection is carried out using the MobileNet-SSD algorithm. MobileNet, a collection of convolutional neural networks (CNN), is designed for mobile and embedded devices, emphasizing low latency and resource consumption. The Single Shot MultiBox Detector (SSD) is an object detection framework that forgoes the need for a separate region

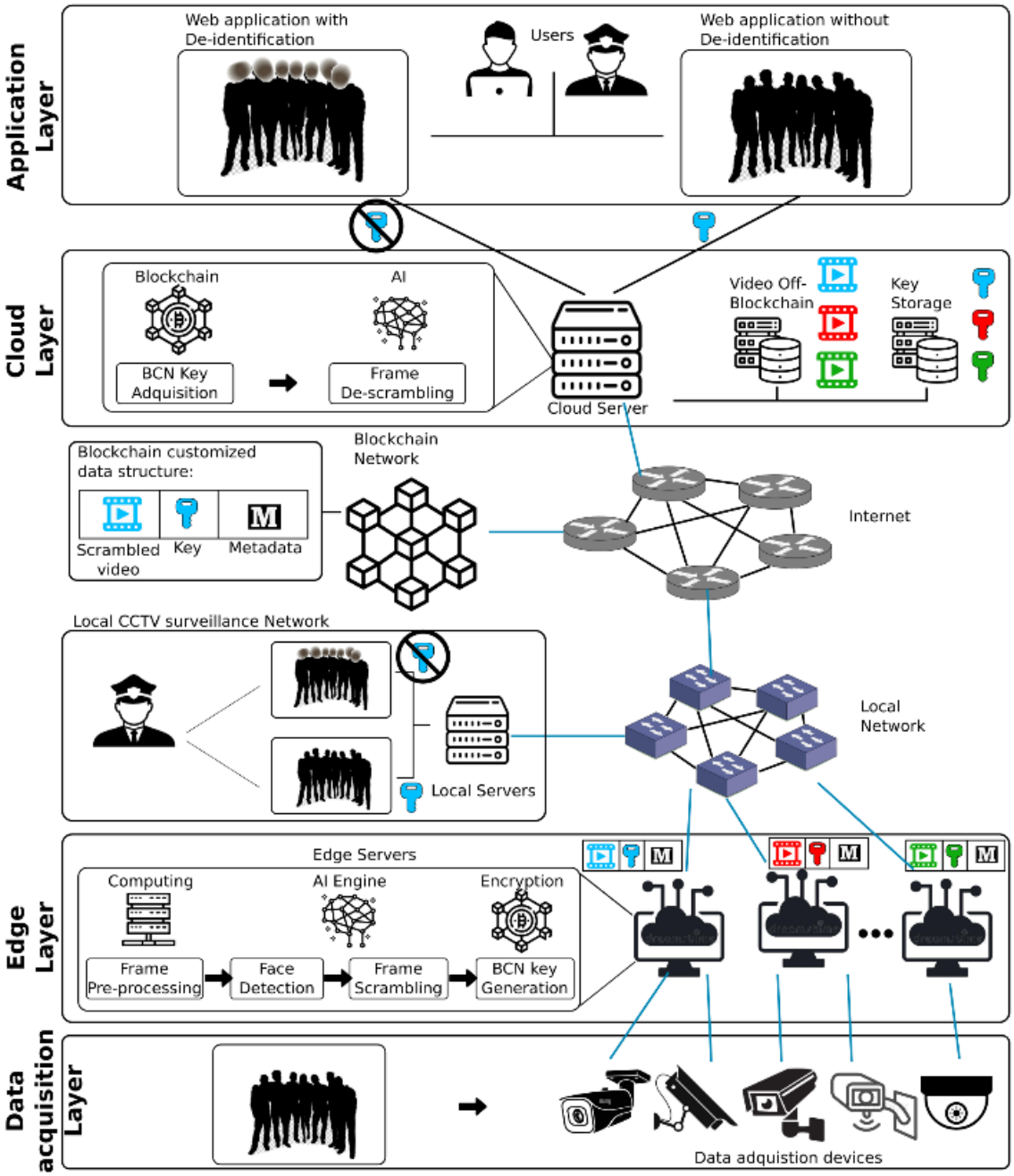


Figure 2. CCTV surveillance system with de-identification and re-identification features

proposal network, as observed in algorithms like Faster R-CNN. SSD directly predicts bounding boxes and class probabilities in a single forward pass, enhancing speed.

SSD employs multiple layers with varying scales and aspect ratios to predict bounding boxes, improving detection accuracy for objects of diverse sizes and shapes. MobileNet-SSD merges the MobileNet architecture with the SSD framework by substituting the base architecture of the original SSD with MobileNet. This combination yields an object detection model that preserves MobileNet's lightweight nature while leveraging the speed and accuracy of SSD. Table 2 compares state-of-the-art algorithms suitable for face detection and frame scrambling, considering edge resource limitation.

Upon extracting face subframes, the Reversible Chaotic Masking (ReCAM) algorithm is applied to scramble pixel positions within the subframes containing human faces. The original subframes in the video frame are replaced with the scrambled versions and sent to the cloud server. If an attacker intercepts the scrambled video and key (i.e., the parameters used in the chaotic scrambling process), they can reverse the ReCAM process to unscramble the video. To address prior challenges, a private blockchain network is proposed for distributed encryption of all subframes produced at each edge server. A private blockchain network comprises authorized nodes such as local servers, cloud servers, and necessary edge servers [25].

Table 2. Comparison of object detection candidate algorithms for the face detection module

Task	Algorithm	Speed	Model size	Accuracy	Suitable for edge-computing
Face detection	MTCNN	Moderate	Moderate	High	Possibly
	Haar Cascade	Fast	Small	Moderate	Yes
	HOG + SVM	Fast	Small	Moderate	Yes
	MobileNet-SSD	Fast	Small	High	Yes
	SqueezeNet-SSD	Fast	Very Small	Moderate	Yes
Frame encryption	Reversible Chaotic Masking	Moderate	Small	Moderate	Possibly
	DL-based anonymization	Moderate to slow	Large	High	Possible with optimization
	Gaussian blurring	Fast	N/A	Low	Yes
	Pixelation	Fast	N/A	Low	Yes
	K-anonymization	Moderate	Varies	Moderate to high	Implementation dependent

The scrambled video footage and unscrambling key are encrypted using the AES algorithm with a shared secret key known only to authorized nodes in the private blockchain network [26]. Encrypted data and relevant metadata are packaged into a transaction, signed by the sending node's private keys and broadcast to other network nodes. Receiving nodes validate the transaction by verifying the sender's signature and ensuring transaction compliance with predefined rules or constraints. Once validated, the transaction is added to a new block using the selected consensus algorithm.

- *Cloud Layer and Application Layer*: cloud server receives the new block containing encrypted data, extracts the scrambled video footage and unscrambling key from the transaction, and decrypts the scrambled video footage and unscrambling key using the shared secret key. The ReCAM inverse process unscrambling key recovers the de-identified video footage. Video footage storage utilizes a distributed file system or a video-specific database, such as a NoSQL database, enabling efficient data storage, indexing, and retrieval.

In the application layer, specific web applications cater to users authorized to view the re-identified footage. Secure access control and authorization are ensured through combination of multi-factor authentication (MFA), role-based access control (RBAC), and attribute-based access control (ABAC), restricting user access based on assigned roles to preserve footage security and privacy [27].

4.2 Open Challenges and Future Directions

While efforts have been made to address security and privacy issues in CCTV footage, significant challenges remain. This section identifies remaining research challenges that still need to be addressed.

- *Loss of important detail in de-identified footage*: De-identification of images presents a significant challenge that requires balancing privacy protection and preserving necessary information. While using de-identification techniques helps to prevent the disclosure of sensitive information, it may also lead to the loss of valuable details crucial for accurate video analysis or forensic investigation. This underscores the need for effective techniques to de-identify images while adequately retaining essential information.
- *The anonymity of de-identified images*: Another significant challenge in de-identifying CCTV footage is ensuring that the de-identified data is anonymous. Even after applying de-identification techniques, there is still a risk that individuals can be re-identified through cross-referencing with other data sources. This applies when footage is combined with other data sources such as mobile phone data or public records, underscoring the need for techniques to prevent cross-referencing of stored de-identified information.
- *Conceal hairstyles and color*: There remains a significant gap in de-identifying non-biometric identifiers such as hairstyles and color. Further research is required to mitigate the risk of personal identification based on these features, specifically dressing and hairstyles. This may involve more complex techniques than simple concealment. Initial efforts have been made, such as concealing hairstyles and hair color [28]. More studies are needed for effective and scalable methods for non-biometric de-identification beyond hair and dressing styles.
- *Pixelation and blurring limitations*: De-identifying faces from CCTV recordings using pixelation and blurring may obscure an individual's identity from HV. These techniques make it difficult for a human observer to identify an individual in the footage. Still, they may not be enough to protect privacy against CV technologies like facial recognition software or advanced DL algorithms. More de-identification methods, such as facial feature modification, may be necessary alongside blurring and pixelation; sophisticated techniques must be developed to enhance de-identification.
- *Face localization and detection algorithms*: Lighting variations, variable head postures, and structural components such as mustaches, sunglasses, beards, glasses, and occlusions are some of the difficulties that make face detection problematic. Real-time face detection and de-identification in crowded scenarios remain challenging. Developing trustworthy and effective algorithms is of utmost importance for such studies, as a single flaw in the face detection algorithm can risk the privacy of video sequences. Researchers need to focus on developing efficient algorithms to handle face detection/identification complexities.

- *Drone-based surveillance systems instability*: Ensuring privacy and security in drone-based surveillance systems is complex and challenging for various reasons. Drones capture images from various heights, angles, and distances, affecting the quality of the captured images. This poses a unique challenge to detecting and concealing identifiable features such as faces to protect individuals' privacy. Drones' movement, changes in weather conditions, and obstacles such as buildings affect image stabilization, making object tracking challenging. Specialized de-identification techniques are needed to cater to these challenges.
- *Deidentification of voices on CCTV footage*: Voice de-identification is a complex area that presents various challenges, including environmental noise and crosstalk. The de-identification process must distinguish between relevant speech and noise in scenarios with significant background noise. Moreover, voice de-identification becomes more complicated when multiple speakers are present, and their voices overlap, causing crosstalk. Therefore, developing robust and effective algorithms to address these challenges is crucial to ensuring privacy and security in voice de-identification.

5 Conclusion

Re-identification and privacy breach threats in multimedia content are important political and social issues in our information society. In the CCTV context, arguably, the most effective strategy would be de-identifying data immediately upon its acquisition. This paper emphasizes de-identification's significance in protecting virtual privacy in CCTV footage and comprehensively surveys the state-of-the-art de-identification technologies and techniques for personal identifiers in CCTV footage. De-identification involves removing or concealing personal identifiers from still images, text, audio, and video streams. We considered different personal identifiers, including biometric, non-biometric, physiological, behavioral, and soft-biometric identifiers. However, it is worth noting that de-identification alone cannot ensure maximum privacy protection, and therefore, other security measures must be devised. Thus, we propose a service scenario in which a blockchain-based MEC-enabled distributed system is used for CCTV data de-identification and re-identification for privacy protection. We also identified open research challenges and future research directions. Our work focuses on technical aspects of privacy protection. However, given the topic's legal and social importance, an effective solution must result from the collective efforts of experts from both fields.

Acknowledgments

This work was supported by Korea Internet & Security Agency (KISA) grant funded by the Korea government (Real-time face de-identification technology that enables same-subject connection analysis in facial recognition CCTV, No: 1781000008).

References

[1] K. Abas, C. Porto, K. Obraczka, Wireless smart camera networks for the surveillance of public spaces, *Computer*, Vol. 47, No. 5, pp. 37–44, May, 2014.

[2] H. Sheng, K. Yao, S. Goel, Surveilling Surveillance: Estimating the Prevalence of Surveillance Cameras with Street View Data, *AIES'21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, Virtual Event, USA, 2021, pp. 221–230.

[3] R. Uittenbogaard, C. Sebastian, J. Vijverberg, B. Boom, D. M. Gavrila, P. H. N. de With, Privacy Protection in Street-View Panoramas using Depth and Multi-View Imagery, *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Long Beach, California, USA, 2019, pp. 10573-10582.

[4] X. Han, L. Wang, S. H. Seo, J. He, T. Jung, Measuring Perceived Psychological Stress in Urban Built Environments Using Google Street View and Deep Learning, *Frontiers in Public Health*, Vol. 10, Article No. 891736, May, 2022.

[5] S. L. Garfinkel, *De-identification of personal information*, National Institute of Standards and Technology, NISTIR 8053, October, 2015.

[6] Y. Lin, J. Shen, S. Cheng, M. Pantic, FT-RCNN: Real-time Visual Face Tracking with Region-based Convolutional Neural Networks, *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020)*, Buenos Aires, Argentina, 2020, pp. 61-68.

[7] V. Bhagwan, T. Grandison, C. Maltzahn, Recommendation-based de-identification: A practical systems approach towards de-identification of unstructured text in healthcare, *2012 IEEE 8th World Congress on Services, SERVICES 2012*, Honolulu, HI, USA, 2012, pp. 155–162.

[8] Q. N. Tran, B. P. Turnbull, J. Hu, Biometrics and Privacy-Preservation: How Do They Evolve?, *IEEE Open Journal of the Computer Society*, Vol. 2, pp. 179–191, April, 2021.

[9] M. H. Joo, H. Y. Kwon, Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea, *Government Information Quarterly*, Vol. 40, No. 2, Article No. 101805, April, 2023.

[10] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, Z. Lin, When Machine Learning Meets Privacy, *ACM Computing Surveys*, Vol. 54, No. 2, p. 1-36, March, 2022.

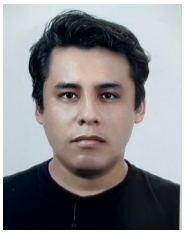
[11] Y. Zhao, J. Chen, A Survey on Differential Privacy for Unstructured Data Content, *ACM Computing Surveys*, Vol. 54, No. 10s, p. 1-28, January, 2022.

[12] C. Liu, T. Zhu, J. Zhang, W. Zhou, Privacy Intelligence: A Survey on Image Privacy in Online Social Networks, *ACM Computing Surveys*, Vol. 55, No. 8, p. 1-35,

August, 2023.
[13] J. R. Padilla-López, A. A. Chaaraoui, F. Flórez-Revuelta, Visual privacy protection methods: A survey, *Expert Systems with Applications*, Vol. 42, No. 9, p. 4177–4195, June, 2015.
[14] M. R. Hasan, R. Guest, F. Deravi, Presentation-Level Privacy Protection Techniques for Automated Face Recognition - A Survey, *ACM Computing Surveys*, Vol. 55, No. 13s, p. 1-27, December, 2023.
[15] B. Meden, P. Rot, P. Terhörst, N. Damer, A. Kuijper, W. J. Scheirer, A. Ross, P. Peer, V. Štruc, Privacy–Enhancing Face Biometrics: A Comprehensive Survey, *IEEE Transactions on Information Forensics and Security*, Vol. 16, pp. 4147–4183, July, 2021.
[16] J. Liu, N. Yu, Online New Media Oriented Privacy Data Recognition Mechanism Based on Deep Learning, *Journal of Multimedia Information System*, Vol. 10, No. 1, pp. 35–44, March, 2023.
[17] Y. Wen, B. Liu, J. Cao, R. Xie, L. Song, Z. Li, IdentityMask: Deep Motion Flow Guided Reversible Face Video De-Identification, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 32, No. 12, pp. 8353–8367, December, 2022.
[18] R. Kim, H. Yoo, J. Ryu, S. C. Kim, Accelerating Face De-Identification System for Real-time Video Surveillance Services, *International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, 2022, pp. 1477–1479.
[19] H. Lee, H. Ahn, Y. D. Park, De-identifying transmission system using wireless channel as differential privacy noise and deep neural networks, in press, *ICT Express*, 2022. https://doi.org/10.1016/j.icte.2022.09.002
[20] J. Kim, N. Park, De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information, *Sensors*, Vol. 22, No. 7, Article No. 2589, April, 2022.
[21] D. Lee, N. Park, Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree, *Multimedia Tools and Applications*, Vol. 80, No. 26-27, pp. 34517–34534, November, 2021.
[22] J. Kim, N. Park, A Face Image Virtualization Mechanism for Privacy Intrusion Prevention in Healthcare Video Surveillance Systems, *Symmetry*, Vol. 12, No. 6, Article No. 891, June, 2020.
[23] P. W. Khan, Y. C. Byun, N. Park, A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities, *Electronics*, Vol. 9, No. 3, Article No. 484, March, 2020.
[24] D. Dharani, K. A. Kumari, R. Vasanthan, Blockchain for CCTV Surveillance, in: J. D. Peter, S. L. Fernandes, A. H. Alavi (Eds.), *Disruptive Technologies for Big Data and Cloud Applications. Lecture Notes in Electrical Engineering*, Vol. 905, Springer, Singapore, 2022, pp. 107–118.
[25] H. Chen, A. El Azzaoui, S. R. Jeremiah, J. H. Park, A Novel Smart Contract based Optimized Cloud Selection Framework for Efficient Multi-Party Computation, *Journal of Information Processing Systems*, Vol. 19, No. 2, pp. 240–257, April, 2023.
[26] H. Chen, S. R. Jeremiah, C. Lee, J. H. Park, A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment, *Applied Sciences*, Vol. 13, No. 3, Article No. 1440, February, 2023.
[27] M. Choi, A. El Azzoui, S. K. Singh, M. M. Salim, S. R. Jeremiah, J. H. Park, The Future of Metaverse: Security Issues, Requirements, and Solutions, *Human-centric Computing and Information Sciences*, Vol. 12, Article No. 60, December, 2022.
[28] C. Xiao, D. Yu, X. Han, Y. Zheng, H. Fu, SketchHairSalon: Deep Sketch-based Hair Image Synthesis, *ACM Transactions on Graphics*, Vol. 40, No. 6, Article No. 216, December, 2021.

Biographies

Sekione Reward Jeremiah is a Ph.D. scholar at Seoul National University of Science and Technology, Seoul, South Korea.



Oscar Enrique Llerena Castro is a Ph.D. scholar at Seoul National University of Science and Technology, Seoul, South Korea.

Pradip Kumar Sharma is an Assistant Professor in Cybersecurity in the Department of Computing Science at the University of Aberdeen, UK.

Jong Hyuk Park is a Professor at Seoul National University of Science and Technology, Seoul, South Korea. Contact him at jhpark1@seoultech.ac.kr.