J Inf Process Syst, Vol.19, No.6, pp.767~777, December 2023
https://doi.org/10.3745/JIPS.03.0190

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Machine Learning-Based Reversible Chaotic Masking Method for User Privacy Protection in CCTV Environment

Jimin Ha[1], Jungho Kang[2], and Jong Hyuk Park[1,*]

Abstract

In modern society, user privacy is emerging as an important issue as closed-circuit television (CCTV) systems increase rapidly in various public and private spaces. If CCTV cameras monitor sensitive areas or personal spaces, they can infringe on personal privacy. Someone's behavior patterns, sensitive information, residence, etc. can be exposed, and if the image data collected from CCTV is not properly protected, there can be a risk of data leakage by hackers or illegal accessors. This paper presents an innovative approach to "machine learning based reversible chaotic masking method for user privacy protection in CCTV environment." The proposed method was developed to protect an individual's identity within CCTV images while maintaining the usefulness of the data for surveillance and analysis purposes. This method utilizes a two-step process for user privacy. First, machine learning models are trained to accurately detect and locate human subjects within the CCTV frame. This model is designed to identify individuals accurately and robustly by leveraging state-of-the-art object detection techniques. When an individual is detected, reversible chaos masking technology is applied. This masking technique uses chaos maps to create complex patterns to hide individual facial features and identifiable characteristics. Above all, the generated mask can be reversibly applied and removed, allowing authorized users to access the original unmasking image.

Keywords

CCTV, Chaotic Masking, Privacy Protection, Security

1. Introduction

In recent years, large deployments of closed-circuit television (CCTV) systems have led to an unprecedented surge in the amount of video data generated every day. These systems are used for a variety of purposes, including security monitoring, traffic monitoring, and enhanced public safety [1,2]. However, the rapid development of digital technology and growing concerns about personal information protection have raised the issue of protecting personal information captured in these videos as an important concern [3,4].

The fundamental challenge arises from the conflict between the benefits of video surveillance and potential breaches of privacy. Video surveillance has proven effective in crime prevention and law

Manuscript received September 20, 2023; first revision November 6, 2023; accepted November 8, 2023.
* **Corresponding Author:** Jong Hyuk Park (jhpark1@seoultech.ac.kr)
[1] Dept. of Computer Science and Engineering, Seoul National University of Science & Technology (SeoulTech), Seoul, Korea (jimin.ha@seoultech.ac.kr, jhpark1@seoultech.ac.kr)
[2] Dept. of Information Security, Baewha Women's University, Seoul, Korea (kjh7548@naver.com)

enforcement support, but it can expose sensitive information about individuals' behavior, routines, and identities, raising concerns about unauthorized monitoring and privacy abuse [5-7].

Moreover, the expansion of smart cities and the integration of artificial intelligence (AI)-based analytics make automatic processing and analysis of video data unprecedented, further amplifying these privacy concerns.

The fundamental challenge arises from the inherent conflict between the benefits of video surveillance and potential breaches of privacy. Video surveillance has proven effective in crime prevention and law enforcement support, but it can expose sensitive information about individuals' behavior, routines, and identities, raising concerns about unauthorized monitoring and privacy abuse. Moreover, the expansion of smart cities and the integration of AI-based analytics make automatic processing and analysis of video data unprecedented, further amplifying these privacy concerns [8].

CCTV can cause various problems related to personal information protection. Below are some of the major privacy issues related to the CCTV system:

- De-identification absence: If the faces or identities of individuals are clearly exposed in CCTV footage, this may result in the leakage of de-identified personal information. Someone can use this information for personal use, which can lead to personal privacy violations [9].
- Data security issues: Personal information may be exposed by hackers or unauthorized access if CCTV image data is stored or transmitted without appropriate security measures. This may infringe on the privacy of the person being monitored.
- Unnecessary data collection: CCTV systems may collect unnecessary personal information. This collection of information can cause privacy issues if it is not legally allowed.
- Information sharing and access: When CCTV image data is shared with other organizations or individuals, unauthorized disclosure of personal information may occur if there are no or unclear restrictions on information sharing and access.
- Use of hidden cameras: Personal privacy and human rights may be violated if CCTV cameras are secretly installed or used for illegal purposes.
- Leakage and sale: Unauthorized leakage or sale of collected CCTV data may result in abnormal use of personal information.
- Privacy infringement: CCTV video data can easily identify individuals' daily lives, behavior patterns, and location information, which can lead to privacy infringement.

To solve these problems, it is necessary to comply with appropriate laws and regulations, and to operate the CCTV system by preparing technical, organizational, and legal measures. It is important to manage and improve the CCTV system in a way that balances personal information protection and public interest purposes.

This paper introduces the “machine learning based reversible chaotic masking method” to balance the personal information problem and public use of CCTV. This work proposes a reversible masking method that combines machine learning and chaos theory to protect users' faces and other personal identification in a CCTV environment. Unlike conventional fixed masking methods, the proposed method leverages chaos theory to transform user information into an arbitrary order and performs masking based on it. This allows you to fully protect the original information while restoring it back to the original information if necessary. The objectives of this paper are as follows. First, it highlights the problem of personal information exposure in CCTV environments and presents the importance of this. Second, we examine

the limitations and shortcomings of existing privacy protection methods and introduce the advantages of the proposed "machine learning-based reversible chaotic masking method" as an alternative to this. Third, it provides a brief overview of the key concepts and operations of the proposed method and helps you understand how it can protect and restore user information.

2. Related Work

Various studies have been continuously conducted to solve personal information problems, such as face de-identification in the CCTV environment. This section examines the existing CCTV video face de-identification technology to protect human personal information. It also examines additional technologies such as AI for face de-identification of CCTV images.

2.1 Existing Studies

Pixelization reduces the likelihood of identification by dividing the face area into pixels to remove sharp features. This is a simple method, but it has the disadvantage of visually distorting the original image. However, pixelation has the following problems. Pixelization causes images to be unclear and less readable. As the image quality decreases, information in the image may be distorted. Facial shapes or features can also be inferred from pixelated images of sufficient size. This means that personal identification of the face may not be protected. Pixelization may have difficulty interpreting the pixelated image by removing the details of the image. This can lead to unintentional inference or interpretation of incorrect information. Pixelization may reduce the usefulness of the image, making it difficult to obtain information suitable for actual monitoring purposes [10-12].

Blurring has the following problems. Blurred makes the face look blurry, but fine details of the face can still be preserved. This may not completely remove the information required to recognize the face. Determining how much to blur and how much to blur the face area is subjective, which can make it difficult to achieve consistent results. Blurring faces in large-scale image data can be computationally resource intensive. In addition, blurring can generally degrade the image quality due to technical problems. Blurring may be more effective as a way to protect your face relatively than pixelation, but it does not provide complete privacy. Blurring has the following problems. Blurred makes the face look blurry, but fine details of the face can still be preserved. This may not completely remove the information required to recognize the face. Determining how much to blur and how much to blur the face area is subjective, which can make it difficult to achieve consistent results. Blurring faces in large-scale image data can be computationally resource intensive. In addition, blurring can generally degrade the image quality due to technical problems. Blurring may be more effective to protect your face relatively than pixelation, but it does not provide complete privacy [13-15].

Face landmark marking is a technique that identifies landmark points that represent the main characteristics of the face and uses them to cover the face. This is used as one of the methods for face de-identification and can be applied for privacy purposes. However, the original facial features can still be inferred if the landmark is not correctly identified or if it is obscured. Facial landmarks are points that represent the main characteristics of the face and can have the only uniqueness between the faces. When this landmark information is leaked or combined with other data, the likelihood of personal identification

increases. Facial landmark marking for large video data can be computationally expensive. This can make it difficult to process large amounts of data in real time. The shape, size, and facial expression of the face can vary. Face landmark marking can be difficult to consider all of this diversity, which can result in a complete inability to cover your face. If the facial landmark marking or masking process is accurately described, malicious users can use the information to attempt a reverse engineering attack to restore the original face shape. Face landmark marking only considers certain parts of the face, so you may not be able to consider your surroundings or context. This can lead to identifying individuals from the information around them [16-18].

To de-identify CCTV for personal information protection, it is necessary to check the face that needs de-identification in the video. To this end, the real-time face recognition AI algorithm of the CCTV environment exists as follows.

BlazeFace is a lightweight facial detection algorithm developed by Google that focuses on real-time facial detection in mobile and embedded systems. BlazeFace consists of a single network with fast throughput and relatively low memory requirements thanks to a small network. It also shows strong performance for various face sizes and angles [19].

Haar Cascades is one of the traditional computer vision technologies that uses relatively simple feature extraction and classification to perform facial detection. This algorithm is used to detect specific patterns in images, which identify face and non-face areas. Haar Cascades can detect faces at high speed with simple operations but can be limited in terms of accuracy and diversity compared to deep learning-based algorithms [20].

2.2 Key Considerations

The primary considerations of the proposed solutions are depicted as follows:

1) Privacy protection: CCTV footage is very vulnerable because it contains personal information of people such as the user's face, body characteristics, behavior, and voice. These CCTV images are easy to expose personal information when attacked by malicious users, so they temporarily cover the personal information of the person shown in the CCTV video to protect people's personal information.
2) Confidentiality: The main challenge of CCTV footage is the confidentiality of the user's personal information data taken. Critical data is likely to lead to data manipulation, loss, or exposure of unauthorized individuals due to leakage and attacks by third parties. Therefore, we solve the problem by protecting this form of data by allowing access only to pre-authenticated users.
3) Integrity: Users who have been granted access will receive CCTV image data. Data manipulation and loss can make it difficult for an attacker to identify a particular user in CCTV footage and change it to be recognized as another user. This can be related to crime, and integrity is very important in the CCTV environment to solve this problem.
4) Efficiency: The efficiency of calculation is another important requirement in CCTV environment. CCTV video is important to protect people information of AI is captured and protect the individual information of many people exposed to these CCTV environments exposed to protect people who are exposed to this CCTV environment. Therefore, the performance of AI that identifies people can ensure better personal information protection performance.

3. Proposed Framework

3.1 Proposal Architecture Overview

The proposed architecture is designed to ensure personal information protection in a CCTV environment. It introduces a machine learning-based reversible chaos masking method for protecting user privacy in a CCTV environment (Fig. 1):

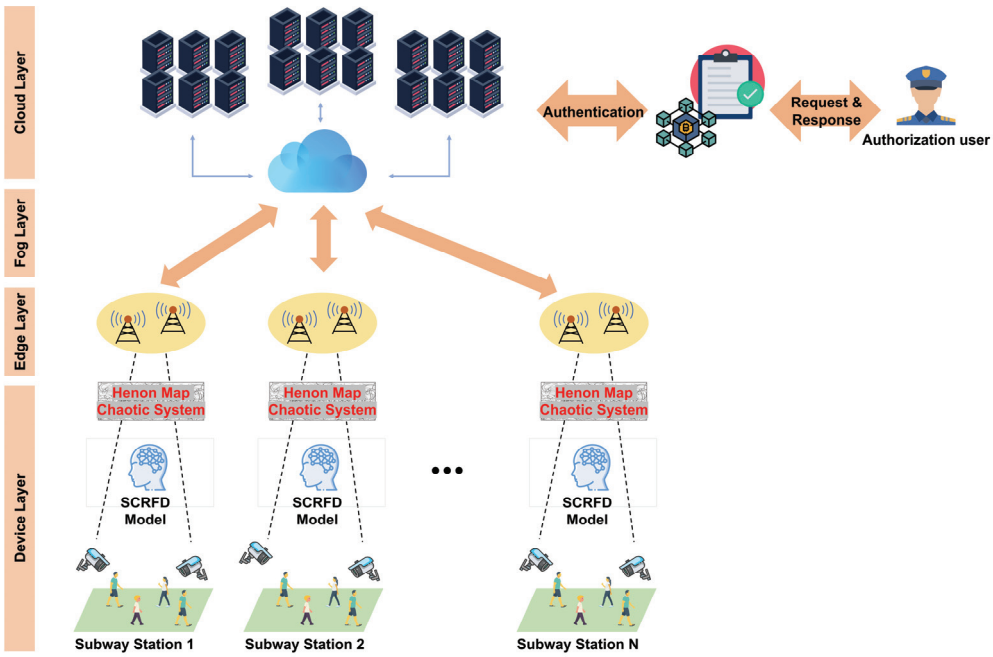

Fig. 1. Machine learning-based reversible chaotic masking for user privacy protection in CCTV environment.

1) Device layer: The first layer of the proposed architecture is the device layer. Numerous CCTVs in subway stations shoot throughout the station and collect video data. These data include personal information of customers, such as the face, body, appearance, and movement of people using subway stations. The AI algorithm, sample and computation redistribution for efficient face detection (SCRFD), is used to identify a person's face in real time from the collected image data. SCRFD has the characteristic of efficiently identifying faces of various sizes in real time.
2) Edge layer: The second layer of the proposed architecture is edge layer. In this layer, we receive face-identified image data obtained from the device layer. To protect the personal information of people using subway stations, the class uses the chaos system to cover the face from the identified video data so that it cannot be assumed as a specific person. The chaos system generates a chaos signal, an unpredictable and random sequence, and then uses this signal to generate a mask. Data is masked by combining it with identified image data through a mask generated by the chaos system.
3) Fog layer: The third layer of the proposed architecture is fog layer. This layer receives de-identified image data obtained from the edge layer. Along with the data, feature data of de-identified people

are also transmitted. The de-identification data received in this way is transmitted to management organizations such as the Subway Transportation Corporation.

4) Cloud layer: The last layer of the proposed architecture is the cloud layer, which is considered a management organization such as the Subway Corporation. Cloud layer stores and manages de-identified data transmitted from lower layers.

There are times when de-identified CCTV images, such as tracking missing persons and criminals, need to be restored to original images. In this case, a reversible chaotic masking method is used to restore the original. The technology matches the characteristics of the de-identified people in the de-identified image and releases masking when it matches. Only authorized users have access to de-identified data in the cloud layer. At this stage, the user's authentication is conducted through a blockchain-based smart contract, and the original video is checked through the reversible chaotic masking method after authentication is completed.

As such, the proposed architecture can efficiently guarantee personal information protection in a CCTV environment.

3.2 Facial Recognition Model

To de-identify CCTV for personal information protection, it is necessary to check the face that needs de-identification in the video. To this end, real-time face recognition AI algorithms in CCTV environments exist as follows, but in this paper, the SCRFD algorithm is used. SCRFD is a facial detection algorithm using the latest deep learning technology. As the name suggests, the algorithm works in a “single shot” manner to detect faces in real time in each frame of the image or video. SCRFD is based on the cascade residual network structure and includes several hierarchical cascade classifiers. These classifiers are used to detect faces of different sizes. SCRFD has the advantage of providing fast processing speed while effectively detecting faces of various sizes [20].

3.3 Chaotic Masking Method

Chaotic masking method is one of the technologies used in data security and cryptography, which leverages chaotic systems or chaotic systems to protect and hide data. This method is primarily used to secure sensitive information and prevent unauthorized access. This includes a variety of ways to confuse and hide data using chaotic systems or chaotic maps. Henon maps are suitable for considering the geographical characteristics of images when used to encrypt images and generate random numbers. In this study, it is used to hide personal and identity information of people in CCTV images previously identified through SCRFD. The key is to hide personal information partially rather than entirely hiding physical characteristics such as human faces and tattoos, which is a feature for Reversible Chaotic Masking, which will be described in the next section.

In this study, the chaotic masking system, Henon map, is used to proceed with chaotic masking Henon map is a two-dimensional chaos system from Chaos theory to a nonlinear dynamics system, based on the following simple mathematical equations:

The Henon map repeatedly uses the above formula to calculate the following positions given the initial conditions. By repeating this process, the Henon map exhibits a chaotic behavior, which allows it to generate a random sequence. This random sequence is unpredictable, sensitive to initial conditions, and

has the properties described in chaos theory [21].

Henon maps are used in various applications such as image encryption, random number generation, and data protection. In image encryption, it is useful to use the spatial characteristics of the image to confuse pixel values, which can improve image security.

3.4 Reversible Chaotic Masking Method

In some cases, it is necessary to restore masked CCTV images, such as in the event of a crime, and for this purpose, the reversible chaotic masking method is used. The reversible chaotic masking method is one of the chaos-based technologies used for data security and privacy. This method is designed to hide and protect data, while also accurately recovering the original data. In other words, the term “reversible” means that there is a two-way or reverse path between masking data and recovering the original data.

The main problems that can be solved using the reversible chaotic masking method are:

1) Personal information disclosure issues: People's faces and other personal information can be exposed in CCTV environments. This acts as a problem that can infringe on privacy and threaten personal safety. The reversible chaotic masking method provides a way to completely hide the original information while recovering it if necessary, by transforming personal information based on chaos theory.
2) Limitations of fixed masking: Traditional fixed masking methods are often difficult to restore once masked information. This can be a problem if security and legal action are required. The reversible chaotic masking method leverages chaos to enable conversion and restoration, providing flexible privacy management.
3) Risk of information leakage: Some privacy protection methods protect by removing or distorting some of the information, but this can lead to loss of important information. The reversible chaotic masking method reversibly transforms information to reduce the risk of identifiable information leakage while maintaining useful information.
4) Useful information retention: Some privacy protection methods completely mask the information, so useful information cannot be utilized for analysis and research. The reversible chaotic masking method provides privacy protection while maintaining the nature of the information, so you can balance security with useful information.
5) Processing different data types: In CCTV environments, there are different types of personal information, as well as faces. The reversible chaotic masking method combines machine learning with chaos theory, giving you the flexibility to process and protect different data types.

Since CCTV contains personal information, the problem of personal information leakage can occur, so anyone who can demask must be allowed only to authorized users. For example, there are police investigating crimes. However, police who are legally authorized to investigate the case, not all police, can access it. If an unauthorized user approaches by impersonating an authorized user, legal responsibility and personal information leakage are necessary.

In this paper, only users who are certified through blockchain and smart contracts are supported with recovered images. The reversible chaotic masking method compares the features of stored characters, such as chaotic masked CCTV images, and recovers the image when matched. We improve the efficiency of the masking process through the reversible chaotic masking method and balance between user privacy and the usefulness of CCTV images.

4. Case Study

The proposed method can be implemented based on the data collected in the existing CCTV environment, and the proposed method is easy to apply to the existing CCTV environment. The case scenario is set in a subway station with a large floating population. Under the assumption that one CCTV per 10 m^2 area is installed on the subway. The flow in which the proposed framework operates in the subway station is explained based on Fig. 2.

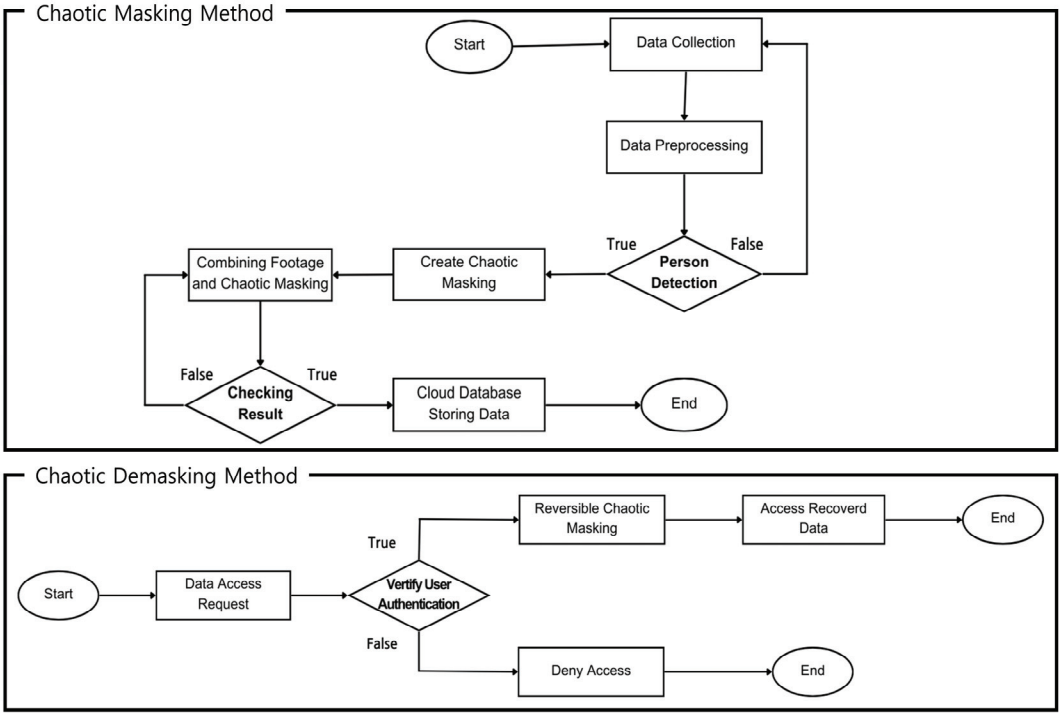

Fig. 2. Detail chaotic masking and demasking method flowchart.

- Data collection: collects video that includes people moving inside the subway station through CCTV installed in the subway station. At this stage, personal characteristics such as the walking, tattoo location, and body shape of people moving around the subway station are also collected in the video.
- Data preprocessing: Data preprocessing works to organize collected data. Data is cleaned so that deep learning algorithms such as human body angle and face angle can easily recognize it.
- Person detection: The SCRFD algorithm is used to recognize and detect people in images collected through CCTV. Through this algorithm, each person's features, such as faces, are detected in real time. If anyone is detected at this stage, we move on to the next step, otherwise the framework flow for the image scene is terminated.
- Create chaotic masking: Randomly generates chaotic masking to mask the person in CCTV footage. Henon map is used as a chaotic system to create chaotic masking.
- Combining footage and chaotic masking: Combines chaotic masking made by Henon map with subway CCTV footage. At this stage, for reversible chaotic masking, only a part of the person is covered, not the whole person.

- Checking results & storing data: Check that people in CCTV footage are well covered and store them on a cloud server. At this stage, it covers the people in the video, and stores the face, tattoo location, and gait together for each person.
- Data access request: A theft occurred at a subway station. To investigate the incident, the police must check the CCTV footage and request access to the video data from the cloud server.
- Certify user authentication: CCTV footage should only allow access to authorized users because it contains the personal information of everyone using the subway. Therefore, it checks whether the person who requested access through the blockchain is the police in charge of the case. At this stage, if an unrelated person, not the police, requests for access, the request is rejected. If an unauthorized user approaches by impersonating an authorized user, legal responsibility is required accordingly.
- Reversible chaotic masking & access recovered data: When the police's identity authentication is completed, access to CCTV footage is successful. However, it is necessary to remove chaotic masking and restore it to its original state because it is necessary to identify customers using the subway for investigation of the case. At this stage, the video and the stored gait are compared with the behavior in the video and restored to a matching face. Through the restored video, the police can find out who was in the subway station at the time of the incident and what actions were taken.

5. Conclusion

CCTV is a means to threaten personal information prevention and evidence collect personal information. The analysis of sensitive personal information protection and digital video monitoring in CCTV environment and digital video monitoring. CCTV video was used in real-time, many people who have been filmed and efficiently identifying people exposed to these CCTV environments exposed to these CCTV environments exposed to protect people who are exposed to this CCTV environment. Therefore, the performance of AI to identify people, efficiently created a better personal information protection environment. Using the Chaotic Masking system was conducted by using the Chic Masking system. The technology provides high level security features and integrity of the image identified through AI, and integrity information that can prevent personal information that can prevent personal information infringement of personal information. In addition, it was also provided by storing personal information and identified personal information and identified personal information and identified personal information and identified personal information. Through this, improvement efficiency of the mask was improved and maintain balance between user personal information protection and the usefulness of CCTV images.

In conclusion, this study presents innovative ways to maintain tension between user personal information protection and video monitoring technology and video surveillance technology. Our research results are applied in real CCTV environment, and expectations that recognize personal information protection and video monitoring of personal information protection. In future research, we will improve this way to improve this method and expand this method.

Acknowledgement

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

References

[1] M. Sheeraz, M. A. Paracha, M. U. Haque, M. H. Durad, S. M. Mohsin, S. S. Band, and A. Mosavi, "Effective security monitoring using efficient SIEM architecture," *Human-centric Computing and Information Sciences*, vol. 13, article no. 17, 2023. https://doi.org/10.22967/HCIS.2023.13.017

[2] W. Ding, "Role of sensors based on machine learning health monitoring in athletes' wearable heart rate monitoring," *Human-centric Computing and Information Sciences*, vol. 13, article no. 16, 2023. https://doi.org/10.22967/HCIS.2023.13.016

[3] T. Jaichuen, N. Ren, P. Wongapinya, and S. Fugkeaw, "BLUR & TRACK: real-time face detection with immediate blurring and efficient tracking," in *Proceedings of 2023 20th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, Phitsanulok, Thailand, 2023, pp. 167-172. https://doi.org/10.1109/JCSSE58229.2023.10202064

[4] B. W. Kwon, P. K. Sharma, and J. H. Park, "CCTV-based multi-factor authentication system," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 904-919, 2019. https://doi.org/10.3745/JIPS.03.0127

[5] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools and Applications*, vol. 80, pp. 34517-34534, 2021. https://doi.org/10.1007/s11042-020-08776-y

[6] S. Prange, A. Shams, R. Piening, Y. Abdelrahman, and F. Alt, "Priview: exploring visualisations to support users' privacy awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama, Japan, 2021, pp. 1-18. https://doi.org/10.1145/3411764.3445067

[7] Y. Beugin, Q. Burke, B. Hoak, R. Sheatsley, E. Pauley, G. Tan, S. R. Hussain, P. McDaniel, "Building a privacy-preserving smart camera system," 2022 [Online]. Available: https://arxiv.org/abs/2201.09338.

[8] E. Kristiani, Y. T. Tsan, P. Y. Liu, N. Y. Yen, and C. T. Yang, "Binary and multi-class assessment of face mask classification on edge AI using CNN and transfer learning," *Human-centric Computing and Information Sciences*, vol. 12, article no. 53, 2022. https://doi.org/10.22967/HCIS.2022.12.053

[9] E. Jasinskaite, "Combining deep privacy with an attribute-driven generative adversarial network to preserve gender and age in de-identified CCTV footage," M.S. thesis, University of Agder, Grimstad, Norway, 2021.

[10] Z. Zhong, Y. Du, Y. Zhou, J. Cao, and S. He, "Delving deep into pixelized face recovery and defense," *Neurocomputing*, vol. 513, pp. 233-246, 2022. https://doi.org/10.1016/j.neucom.2022.09.141

[11] J. Zhou and C. M. Pun, "Personal privacy protection via irrelevant faces tracking and pixelation in video live streaming," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1088-1103, 2020. https://doi.org/10.1109/TIFS.2020.3029913

[12] J. Zhou, C. M. Pun, and Y. Tong, "Privacy-sensitive objects pixelation for live video streaming," in *Proceedings of the 28th ACM International Conference on Multimedia*, Seattle, WA, USA, 2020, pp. 3025-3033. https://doi.org/10.1145/3394171.3413972

[13] L. Li, Z. Xia, A. Hadid, X. Jiang, H. Zhang, and X. Feng, "Replayed video attack detection based on motion blur analysis," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2246-2261, 2019. https://doi.org/10.1109/TIFS.2019.2895212

[14] X. Hu, S. Peng, L. Wang, Z. Yang, and Z. Li, "Surveillance video face recognition with single sample per person based on 3D modeling and blurring," *Neurocomputing*, vol. 235, pp. 46-58, 2017. https://doi.org/10.1016/j.neucom.2016.12.059

[15] T. Rakhimzhanova, "Face and facial landmark detection for event-based imaging," M.S. thesis, School of Engineering and Digital Sciences, Nazarbayev University, Astana, Kazakhstan, 2023.

[16] S. S. Jang, C. J. Kim, S. Y. Hwang, M. J. Lee, and Y. G. Ha, "L-GAN: landmark-based generative adversarial network for efficient face de-identification," *The Journal of Supercomputing*, vol. 79, pp. 7132-7159, 2023. https://doi.org/10.1007/s11227-022-04954-x

[17] J. Lin, "Accurate and Fast mask recognition based on multiple color areas detection and face landmarks locating," in *Proceedings of 2022 IEEE 22nd International Conference on Communication Technology (ICCT)*, Nanjing, China, 2022, pp. 1463-1467. https://doi.org/10.1109/ICCT56141.2022.10072864

[18] V. Bazarevsky, Y. Kartynnik, A. Vakunov, K. Raveendran, and M. Grundmann, "BlazeFace: sub-millisecond neural face detection on mobile GPUs," 2019 [Online]. Available: https://arxiv.org/abs/1907.05047.

[19] T. Mantoro and M. A. Ayu, "Multi-faces recognition process using Haar cascades and eigenface methods," in *Proceedings of 2018 6th International Conference on Multimedia Computing and Systems (ICMCS)*, Rabat, Morocco, 2018, pp. 1-5. https://doi.org/10.1109/ICMCS.2018.8525935

[20] J. Guo, J. Deng, A. Lattas, and S. Zafeiriou, "Sample and computation redistribution for efficient face detection," 2021 [Online]. Available: https://arxiv.org/abs/2105.04714.

[21] N. Guisande, M. P. di Nunzio, N. Martinez, O. A. Rosso, and F. Montani, "Chaotic dynamics of the Hénon map and neuronal input-output: a comparison with neurophysiological data," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 33, no. 4, article no. 043111, 2023. https://doi.org/10.1063/5.0142773

Jimin Ha **https://orcid.org/0009-0006-0248-6704**

She received B.S. in Department of Information Security, Baewha Women's University in 2023. She is currently pursuing her Master degree in computer science and engineering, Seoul National University of Science and Technology with the Ubiquitous Computing Security (UCS) Laboratory, under the supervision of Prof. Jong Hyuk Park. Her current research interests include AI-based Security, AI Security and Internet-of-Things (IoT) security.

Jungho Kang **https://orcid.org/0000-0002-5038-698X**

He received Ph.D. degrees in Department of Computer Science and Engineering from Soongsil University, Republic of Korea. From July 2010 to July 2014, Dr. Kang had been a director at the Plumsoft, Korea. He is now a professor at the Department of Information Security, Baewha Women's University, Republic of Korea. His research field is Information Security, IoT, cloud, fuzzy theory, etc.

Jong Hyuk (James J.) Park **https://orcid.org/0000-0003-1831-0309**

He received Ph.D. degrees in the Graduate School of Information Security from Korea University, Korea. He is a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. He has published about 200 research papers in international journals and conferences. His research interests include the IoT, human-centric ubiquitous computing, information security, digital forensics, vehicular cloud computing, and multimedia computing. He is a member of the IEEE Computer Society, KIPS, and KMMS. He got the best paper awards from ISA-2008 and ITCS-2011 conferences and the outstanding leadership awards from IEEE HPCC-2009, ICA3PP-2010, IEE ISPA-2011, PDCAT-2011, and IEEE AINA-2015. Furthermore, he got the outstanding research awards from the SeoulTech, in 2014. He has been serving as the Chair, the Program Committee, or the Organizing Committee Chair for many international conferences and workshops. He is also the Steering Chair of international conferences–MUE, FutureTech, CSA, CUTE, UCAWSN, and World IT Congress-Jeju. He is editor-in-chief of *Human-centric Computing and Information Sciences* (HCIS) by KIPS, *The Journal of Information Processing Systems* (JIPS) by KIPS, and *Journal of Convergence* (JoC) by KIPS CSWRG. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford University Press, Emerald, Inderscience, and MDPI.