Advances in Dynamical Systems and Applications.
ISSN 0973-5321, Volume 16, Number 1, (2021) pp. 171-179

https://dx.doi.org/10.37622/ADSA/16.1.2021.171-179

De-identification Mechanism of Block Network Image Privacy Information based on Risk Level

Jinsu Kim*, Sungwook Jung*, Sangik Oh*, Won-chi Jung*, Doik Hyun, Yujin Jung*, Eunsun Choi**, and Namje Park*,****

**Convergence Information Security, Graduate School, Jeju National University, Jeju Special Self-Governing Province, 63294, Korea.*

***Major in Computer Education, Faculty of Science Education, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, 63294, Korea.*

Corresponding Author: Namje Park

Abstract

As society develops, the protection of individual safety is becoming increasingly important. In particular, the leakage of personal information, which means information that can be inferred from individuals, is a big topic that has caused a huge impact on society. In order to strengthen the protection of personal information, the video system pays a lot of attention to recorded video information or personal information, and a lot of research is being conducted to prevent it from being leaked or to identify the target from the leaked data. However, the recorded information may include criminals as well as ordinary people. There are also cases where personal information is not required to be disclosed for all criminals, but some disclosure is required depending on the risk of the subject. In this paper, we study the mechanism of applying risk-dependent non-identification in a blockchain-based data recording environment to enhance the reliability of data in the process of de-identification based on target risk information and whether it is criminal or not.

Keywords: block network, de-identification, risk based de-identification, privacy data

Introduction

As society develops, more attention is being paid to individual security. This can be seen especially with closed circuit television (CCTV), which is increasing every year. In particular, such video surveillance systems are operated on a large scale for the purpose of crime prevention or traffic control in vulnerable times, such as dawn or night in the public sector, and are applied not only for simple family crime but also for corporate security. Such video surveillance systems are especially frequently used in densely populated areas.

However, the problem that video surveillance systems cannot protect personal information by infringing on the portrait rights of objects being filmed at the same time has been continuously suggested. In general, if the importance of personal information protection precedes the importance of public purposes, the video can be checked, but it is important to minimize the leakage of personal information except in inevitable circumstances. In particular, as the number of systems for using face-area information as part of biometric information increases, protecting the information of subjects connected by visual information is also important, unlike the previously evolving imaging system. A typical example of linking information about facial areas with identity information of a particular individual is China's Skynet. China's Skynet is an anti-corruption and anti-crime video surveillance system that has been established since 2015 to track and determine dynamic objects and to link databases containing information on criminal suspects to track criminals.

As it provides different services through convergence with more and more diverse systems, the scope of personal information covered in the process is expanding and the importance is being emphasized. Research is also underway on de-identification, which replaces information with information that cannot be identified to protect personal information. Biometric information and personal information are applied to enhance the convenience of users by incorporating them into services, but preventing the leakage of information used should be more thoroughly.

In this paper, we propose a mechanism to ensure the integrity and confidentiality of the subject's information by non-identifying the subject's information and recording it to the blockchain network for the identification information captured by the video surveillance system.

Video personal information de-identification mechanism based on risk block network

The risk block network-based video privacy mechanism proposed in this paper is not identified even if it is leaked externally through de-identification of the collected video information or the individual's identification, and the image information is phased out according to the individual's risk. The step-by-step processing of individual risk can help investigation cooperation and crime prevention by disclosing information about high-risk individuals, and protect personal information by preventing them from identifying information when they are not willing to commit crimes and low-risk individuals.

The proposed mechanism prevents the recorded information from being identified by proceeding with the de-identification process for the collected individual's personal information. However, non-identifying information is carried out by a certain rule, in which case there is a possibility of inferring information by interpreting the rule. In particular, it can weaken the integrity of the characteristic data of block networks that share all data, especially over public networks. To solve this problem, unidentified data is written to the block network through encryption, and clients or servers in the block network share the data. Such a configured server can track targets through data rather than target identification, through the same de-identification process if specific individual information is required. Block networks are subsequently utilized as risk databases for de-identification of video information.

Afterwards, it will proceed with the process of de-identification of video information. Facial areas are used as identification information in the process of non-identification of video information. The collected facial area proceeds based on the risk of the target recorded in the block network to evaluate the risk of the target, and the higher the risk of the target, the more circular the image is provided. We provide video information that is difficult to identify when the risk of the subject is low. [Figure 1] shows the overall flow of the proposed mechanism.

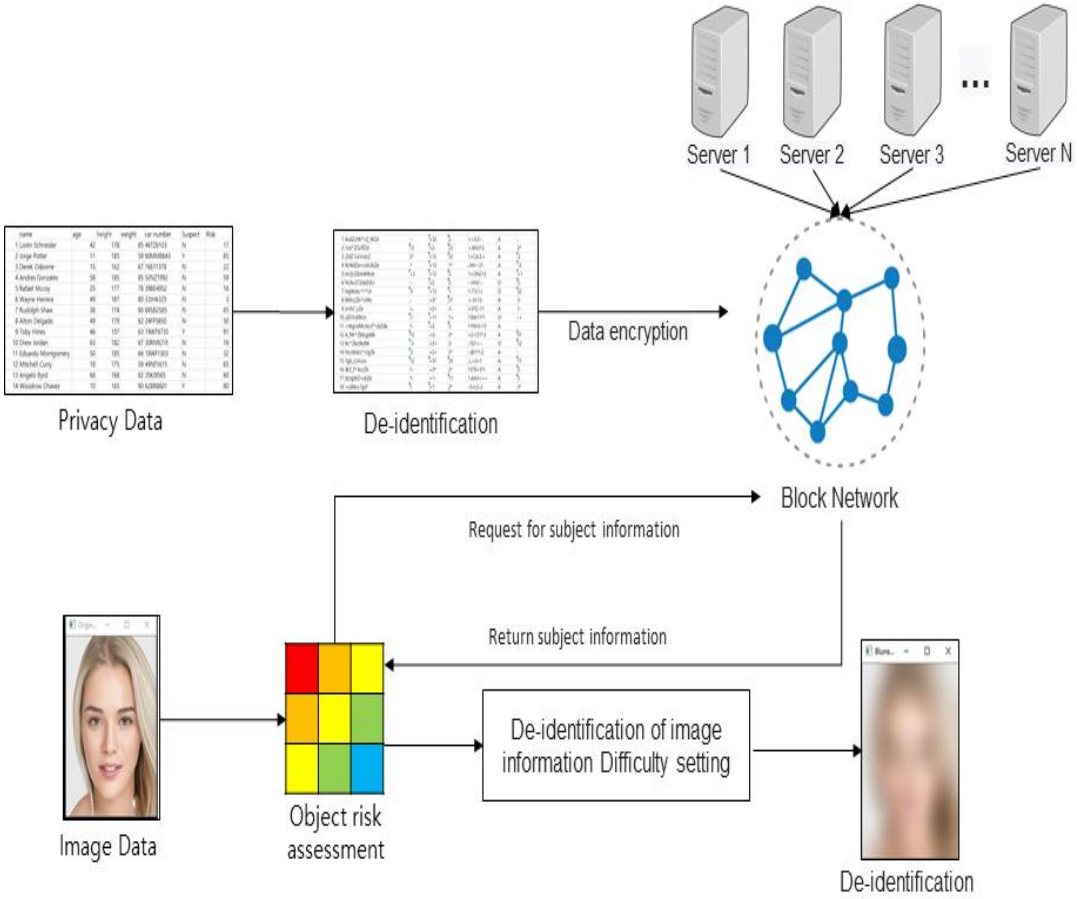

Figure 1 Block Network-Based Image Privacy Non-Identification Mechanism Flow Chart

Video personal information de-identification mechanism based on risk block network : Privacy Information De-Identification Module

A privacy non-identification module refers to a module that proceeds with a non-identification process for documentary information that does not contain video information as the personal information of the target being collected. If a manager who manages personal information requires the registration of personal information, the data to be registered is first sent to the non-identification module. Non-identification modules will be non-identified and then registered in block network after encryption.

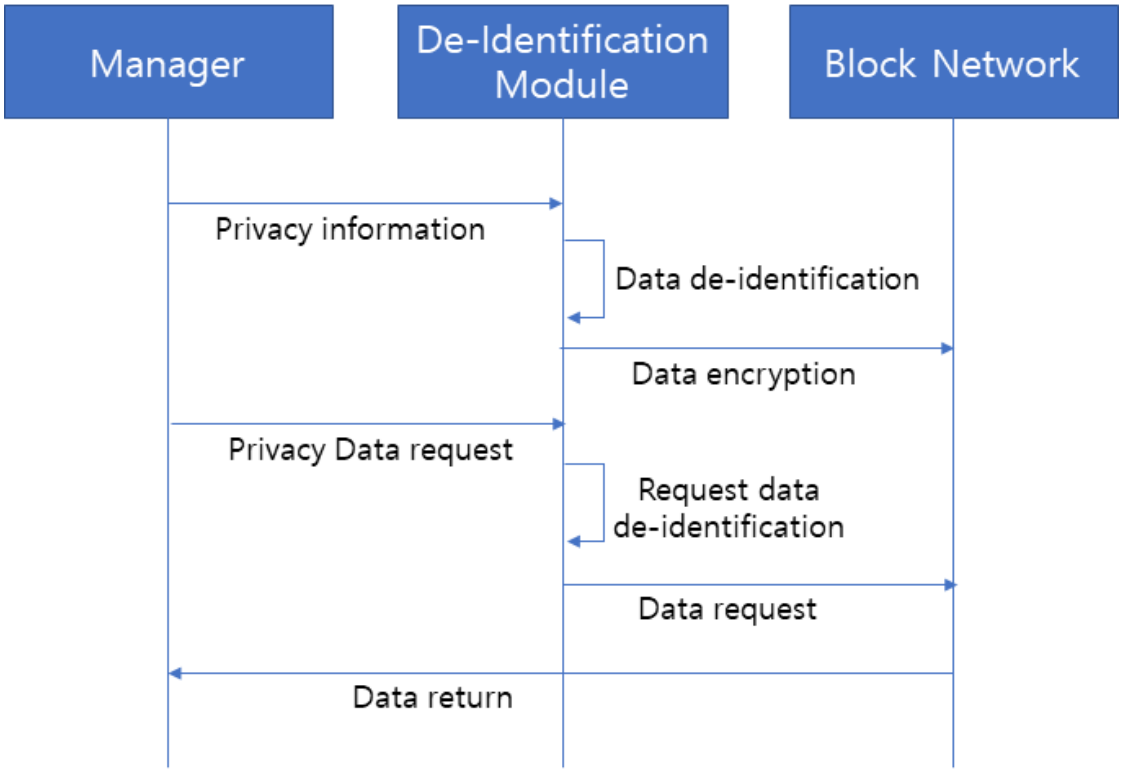

Figure 2 Process for processing privacy de-identification modules

The information request process by the manager then requests a search as raw, unprocessed information, and the de-identification module proceeds with the de-identification processing of the data requiring the search through the same process. Subsequently, the same data is retrieved from the block network using unidentified data, and the search results can be provided to the manager, thereby enhancing the integrity of the data by preventing the restoration of unidentified data written to the block network during the search. [Figure 2] shows the processing of privacy de-identification modules.

Video personal information de-identification mechanism based on risk block network : Image Information De-Identification Module

The image information de-identification module aims to de-identify image information in stages based on the risk information de-identified by the privacy de-identification module. The variables that have a major influence on de-identification are the subject's

risk assessment and criminal intention, and the risk assessment consists of three stages, assuming a maximum of 100.

First, as for the risk variable, the non-identification difficulty level can be set differently as shown in [Equation 1] according to the subject's risk assessment. In the text, the risk level is arbitrarily specified, and the value can be adjusted according to the application subject or can be carried out by dividing the steps in more detail.

$$Risk\ Group = \begin{cases} Group\ 1 = 30\ if)\ Risk \leq 50 \\ Group\ 2 = 3\ \ if)\ Risk \leq 70 \\ Group\ 3 = 0\ \ if)\ Risk \leq 90 \end{cases} \quad (1)$$

The de-identification difficulty obtained by [Equation 1] is higher in the current stage in order to set a high de-identification difficulty for subjects with a low risk, and a low de-identification difficulty for subjects with a high risk. The de-identification difficulty level is summed to proceed. [Equation 2] shows the process of setting the non-identification difficulty. x means a variable for a risk group. [Equation 3] shows the process of calculating the de-identification difficulty in the case of group 1 with a low risk.

$$Risk\ De-identification\ difficulty = \sum_{x+2}^{x=x} Group\ x \quad (2)$$

$if)\ Group\ 1\ them$

$$Risk\ De-identification\ difficulty = 30 + 3 + 0 = 33 \quad (3)$$

Finally, the difficulty of de-identification can be set by changing the size of the mask according to the criminal will of the subject. [Equation 4] is a value arbitrarily set for the de-identification setting. Subjects who are suspected of crime apply a small mask to make it easier to identify, and subjects who are not willing to commit crime are more likely to identify by expanding the mask range. Made it difficult.

$$Suspect\ difficulty = \begin{cases} 0.3\ if)\ Suspect = Yes \\ 0.7\ if)\ Suspect = No \end{cases} \quad (4)$$

[Equation 5] shows the process of de-identification based on Gaussian distribution based on the risk and criminal will of the subject determined by [Equation 2] and [Equation 4].

$$De - identification = Suspect\ difficulty * ((Risk\ De - identification - 1 \quad * 0.5 - 1) + 0.8 \quad (5)$$

Image information that has been de-identified provides different levels of de-identification according to the subject's risk and criminal will, as shown in [Figure 3]. [Figure 3] shows the original image information, de-identified image information that is not intended to be criminal, and de-identified image information that is intended to be criminal.

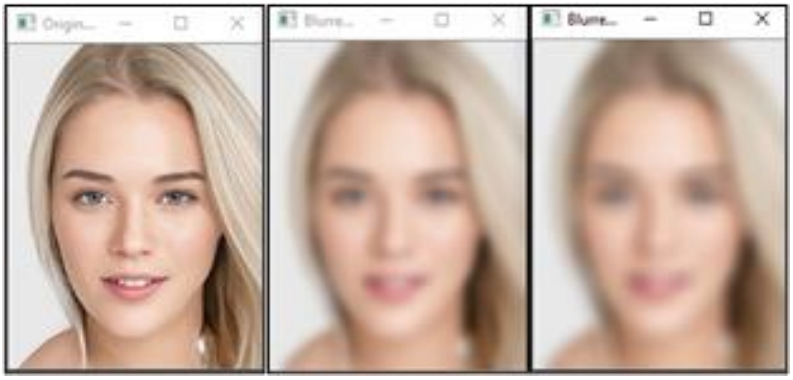

Figure 3 Examples of image information de-identification

Conclusion

As various industries converge and develop, the video surveillance system is also undergoing a lot of development. Clear images resulting from an increase in resolution of a physical imaging device are also applied to CCTV, so that an image capable of identifying an object is taken even in a more difficult environment than before. Shooting a clearer image can be of great help in recognizing the subject, but at the same time, it may have a problem of invading the privacy of the subject. Of course, there are examples in which the movement of the target must be provided depending on the target person, but the privacy of the target person must be protected unless there is a special case.

In this paper, the subject's image information is provided step by step to prevent

indiscriminate leakage of image information by varying the degree of non-identification difficulty based on the subject's risk and criminal will to protect the subject's privacy. Information related to the subject's risk assessment was de-identified and recorded using a block network to reinforce the integrity of the data.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2019R1I1A3A01062789). And, this work was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government(MOE).

References

[1] Abhishek Joshi & Mohammad Wazid & R.H. Goudar (2015). An Efficient Cryptographic Scheme for Text Message Protection Against Brute Force and Cryptanalytic Attacks, Procedia Computer Science, 48, 360-366.

[2] Jinsu Kim & Namje Park (2019). Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing. Personal and Ubiquitous Computing, 1-9.

[3] Namje Park & Younghoon Sung & Youngsik Jeong & Soo-Bum Shin & Chul Kim (2018). The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea, International Conference on Computer and Information Science, Springer, 1-15.

[4] S.S. Nalegaev & N.V. Petrov (2015). Simple Criteria to Determine the Set of Key Parameters of the DRPE Method by a Brute-force Attack, Physics Procedia, 73, 281-286.

[5] José Tomás Martínez Garre & Manuel Gil Pérez & Antonio Ruiz-Martínez (2020). A novel Machine Learning-based approach for the detection of SSH botnet infection, Future Generation Computer Systems.

[6] Jinsu Kim & Namje Park (2020) Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments, Applied Sciences.

[7] Laurens Hellemons & Luuk Hendriks & Rick Hofstede & Anna Sperotto & Ramin Sadre & Aiko Pras (2012). SSHCure: A Flow-Based SSH Intrusion Detection System, IFIP International Conference on Autonomous Infrastructure, Management and Security, 86-97.

[8] Namje Park (2018). The Core Competencies of SEL-based Innovative Creativity Education, International Journal of Pure and Applied Mathematics, 118(19), 837-849.

[9] Md Delwar Hossain & Hideya Ochiai & Fall Doudou & Youki Kadobayashi (2020). SSH and FTP brute-force Attacks Detection in Computer Networks: LSTM and Machine Learning Approaches, 2020 5th International Conference on Computer and Communication Systems (ICCCS).

[10] Donghyeok Lee & Namje Park (2017). A Secure Almanac Synchronization Method for Open IoT Maritime Cloud Environment, Journal of Korean Institute of Information Technology, 15(2), 79-90.