Protecting Personal Information using Homomorphic Encryption for Person Re-identification

Kazunari Morita[1], Hiroki Yoshimura[1,2], Masashi Nishiyama[1,2] and Yoshio Iwai[1,2]
[1] Graduate School of Engineering, Tottori University, Japan
[2] Cross-informatics Research Center, Tottori University, Japan
Email: nishiyama@tottori-u.ac.jp

***Abstract*—We investigate how to protect features corresponding to personal information using homomorphic encryption when matching people in several camera views. Homomorphic encryption can compute a distance between features without decryption. Thus, our method is able to use a computing server on a public network while protecting personal information. To apply homomorphic encryption, our method uses linear quantization to represent each element of the feature as integers. Experimental results show that there is no significant difference in the accuracy of person re-identification with or without homomorphic encryption and linear quantization.**

***Index Terms*—Person Re-identification, Personal Information, Linear Quantization, Homomorphic Encryption**

I. Introduction

There is a high demand for an authentication system that widely covers many areas using several cameras. An authentication system operates using a person re-identification technique that extracts and matches features representing identities from video sequences. In particular, an authentication system needs to carefully protect the features because they correspond to personal information. Personal information is often protected using a private network that cannot be accessed from the outside. However, a private network is an expensive solution.

We discuss how to design an authentication system at a large scale. We need to consider the scalability of person re-identification because the amount of computation for person re-identification exponentially increases when many pedestrian images are acquired. For instance, we frequently encounter a case in which the number of people increases when there is a crowd. Alternatively, the number of cameras increases when monitoring areas are expanded. To deal with such scalability issues, a common solution is to use a computing server on a public network using public hardware. However, there is a danger that the features for person re-identification could be leaked if a computing server is the victim of malicious attacks. An authentication system must keep the information on a computing server inaccessible from third persons by encrypting the features.

In this paper, we propose a novel method for protecting features extracted from video sequences using homomorphic encryption [1]. The aim is to use this method in the design of an authentication system on a publicly available computing server. Using homomorphic encryption, we can compute the distance between features for matching persons without decrypting the features on a computing server. Even though the scale of an authentication system has been expanded this way, we can safely protect personal information. With respect to pattern recognition techniques using homomorphic encryption, deep learning [2] and principal component analysis [3] are reported. We focus on the distance calculation for matching features of person re-identification. Generally, features are often represented using floating-point numbers. However, when applying homomorphic encryption, the features should be represented as integers to increase calculation efficiency. We thus investigate whether our method can quantize and encrypt features while maintaining the accuracy of person re-identification. Experimental results show that our method maintains this accuracy when using linear quantization and homomorphic encryption.

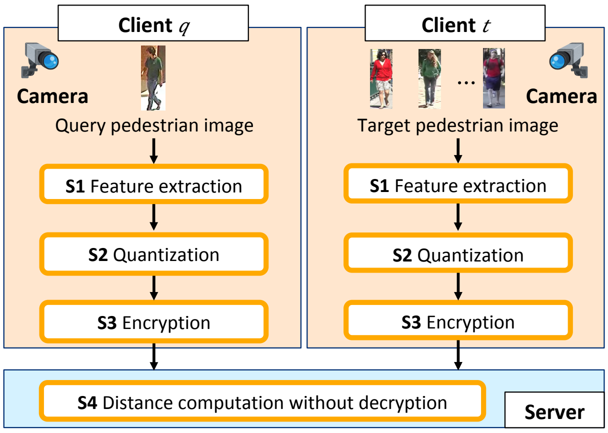

Fig. 1. Overview of our method.

II. Our method

A. Overview

Figure 1 shows an overview of our method. In S1, we extract query and target features $\boldsymbol{f}_q$ and $\boldsymbol{f}_t$, respectively, from video sequences I_q and I_t. We use the confidence of co-occurrence attributes described in [4] for designing the features. Note that each element of $\boldsymbol{f}_q$ and $\boldsymbol{f}_t$ is within the range $-1 \leq f_q \leq 1, -1 \leq f_t \leq 1$. We explain S2 and S3 in Section II-B, Section II-C. In S4, we use a large-margin nearest-neighbor (LMNN) [5] technique to improve the accuracy of person re-identification. We represent a metric matrix as $\mathbf{M} = \mathbf{L}^{\mathrm{T}}\mathbf{L}$ ($||\mathbf{M}||_f \leq 1$) and compute a square of distance d^2 as

$$\begin{aligned} d^2 &= (\boldsymbol{f}_q - \boldsymbol{f}_t)^{\mathrm{T}}\mathbf{M}(\boldsymbol{f}_q - \boldsymbol{f}_t) \quad (1)\\ &= (\boldsymbol{f}'_q - \boldsymbol{f}'_t)^{\mathrm{T}}(\boldsymbol{f}'_q - \boldsymbol{f}'_t), \quad (2)\end{aligned}$$

where $\boldsymbol{f}'_q = \mathbf{L}\boldsymbol{f}_q$ and $\boldsymbol{f}'_t = \mathbf{L}\boldsymbol{f}_t$. We use $\boldsymbol{f}'_q$ and $\boldsymbol{f}'_t$ because the computational cost of matrix operations using homomorphic encryption is very large.

B. Homomorphic encryption

Homomorphic encryption is able to perform addition and multiplication operations on a finite field without decryption. Our method computes a square of distance d^2 between encrypted features for person re-identification using fully homomorphic encryption (FHE) library.[1] To encrypt a N-dimensional feature, we control the following parameters of the library: prime p determines an integer ring $\mathbb{Z}_p$ representing a plain text space and parameter m determines the number of slots n $(n \geq N)$. The parameter n is defined as

$$n = \frac{\phi\,(m)}{\mathrm{order}\,(m, p)}, \quad (3)$$

where ϕ is the Euler function, $\mathrm{order}()$ is the order of p modulo m. It is difficult to freely control n because p and m strongly dominate n. Our method experimentally searches for p and m until it obtains an n that is larger than or equal to N.

C. Quantization

From the viewpoint of computational cost, we need to represent the features as integers because the FHE library uses a ring of integers. Our method transforms each element of the feature using linear quantization. When computing a distance d^2 between encrypted features, we must be careful to avoid overflow. Prime p needs to satisfy the following conditional expression:

$$N \times 2^{2g} < p \quad (4)$$

where g is the number of quantization bits. Our method uses the conditional expression when searching p and m. We empirically quantize each element of $\boldsymbol{f}'_q$ and $\boldsymbol{f}'_t$ in the range $-1 \leq f'_q \leq 1, -1 \leq f'_t \leq 1$.

III. Evaluation

We evaluated the accuracy of person re-identification using linear quantization and homomorphic encryption. We used the SARC3D dataset, which is included in the PETA dataset [6]. We randomly split the SARC3D dataset into two small sets without overlapping individuals. We used one small set for training a metric matrix and the other small set for evaluating the matching rate. We repeated this procedure 10 times. We set the number of target pedestrian images to only one. We used the remaining the PETA dataset without the SARC3D dataset for learning the co-occurrence attribute classifiers. The dimensionality N of the features was 95.

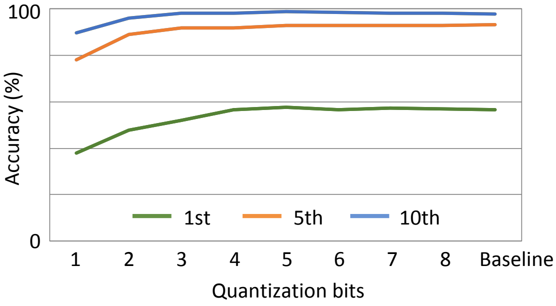

Fig. 2. Accuracy of person re-identification while changing the parameters of linear quantization and homomorphic encryption.

We evaluated the accuracy while changing the number of quantization bits g. The baseline accuracy was also evaluated without the use of linear quantization and homomorphic encryption. Figure 2 shows the average and standard deviation of the n-th matching rate (%). We see that the accuracy decreases when the number of bits was less than four. For example, we set the parameters as $g = 4$, $p = 65,537$, and $m = 14,089$. We confirmed that there is no significant decrease in accuracy using our method.

IV. Conclusions

We proposed a method for computing the distance between encrypted features using linear quantization and homomorphic encryption. We confirmed that the accuracy of person re-identification is almost unchanged using four or more bits for quantization. As part of our future work, we intend to evaluate the computational costs when the number of features increases.

Acknowledgment This work was partially supported by JSPS KAKENHI under grant number JP17K00238 and MIC SCOPE under grant number 172308003.

References

[1] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "Fully homomorphic encryption without bootstrapping," in *Proceedings of 3rd Innovations in Theoretical Computer Science Conference*, 2012, pp. 309–325.

[2] N. Dowlin, R. Gilad-Bachrach, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "Cryptonets: applying neural networks to encrypted data with high throughput and accuracy," in *Proceedings of 33rd International Conference on Machine Learning*, 2016, vol. 48, pp. 201–210.

[3] W. Lu, S. Kawasaki, and J. Sakuma, "Using fully homomorphic encryption for statistical analysis of categorical, ordinal and numerical data," in *Proceedings of Network and Distributed System Security Symposium*, 2016, pp. 201–210.

[4] M. Nishiyama, S. Nakano, T. Yotsumoto, H. Yoshimura, Y. Iwai, and K. Sugahara, "Person re-identification using co-occurrence attributes of physical and adhered human characteristics," in *Proceedings of 23rd International Conference on Pattern Recognition*, 2016, pp. 2086–2091.

[5] K. Weinberger, J. Blitzer, and L. Saul, "Distance metric learning for large margin nearest neighbor classification," *Journal of Machine Learning*, vol. 10, pp. 207–244, 2009.

[6] Y. Deng, P. Luo, L. Ping, C. C. Loy, and X. Tang, "Pedestrian attribute recognition at far distance," in *Proceedings of 22nd ACM International Conference on Multimedia*, 2014, pp. 789–792.

[1] HElib https://github.com/shaih/HElib