Face Image Anonymization as an Application of Multidimensional Data K-Anonymizer

Taichi Nakamura
Graduate School of Science and Technology
Keio University
3-14-1 Hiyoshi, Kouhoku, Yokohama,
Kanagawa 223-8522, Japan
taichi@west.sd.keio.ac.jp

Yuiko Sakuma
Graduate School of Science and Technology
Keio University
3-14-1 Hiyoshi, Kouhoku, Yokohama,
Kanagawa 223-8522, Japan
sakuma@west.sd.keio.ac.jp

Hiroaki Nishi
Graduate School of Science and Technology
Keio University
3-14-1 Hiyoshi, Kouhoku, Yokohama,
Kanagawa 223-8522, Japan
west@sd.keio.ac.jp

***Abstract*— Recently, the development of data communication networks and advances in computer processing capacity have significantly increased the amount of data to be managed. Although future innovations using data are expected, privacy violation of data has become a problem. For example, image disclosure in Social Networking Service may result in infringement of portrait rights. Previously, studies on anonymization have been conducted to disclose data for protecting personal information. However, conventional anonymization, even for high-dimensional data such as faced images, uses an averaging operation in anonymization and does not consider complex relationships between dimensions. Therefore, the loss of semantic meaning increases because it is caused by the anonymization process, assuming an Euclidean data space. We herein propose Multidimensional Inputs K-anonymizing Unit(MIKU), an anonymization algorithm focusing on face image anonymization as a typical example of high-dimensional datMIKU enables anonymization that retains the image quality. As the comparison method directly anonymizes images, the quality of images is deteriorated. MIKU considers the relation between dimensions using the latent space of StyleGAN. The effect of using latent space was confirmed by comparing the quantitative results of Fréchet Inception Distance(FID) and the qualitative evaluation of the output image with the comparison method. The quantitative results by FID proved that MIKU achieved better performance when K-anonymity was large. When K-anonymity is small, we clarified that the image quality of the comparison method such as FID could not be measured correctly and was overestimated because of the effect of the inception model's linearity. In addition, the qualitative evaluation of anonymized images shows that MIKU generates a more natural image in the contour and hair expressions than the comparison method, and the anonymized images of MIKU contain no unnatural edge lines on a face such as those generated in the comparison method.**

Keywords*— *K-Anonymization, Face Image, High-Dimension, StyleGAN, Neural Network

I. INTRODUCTION

Computing capacity is progressing daily;high-precision images can now be captured anywhere even if small terminals are used. The image can be distributed worldwide over the Internet. Similarly, any type of large data can be shared easily. Secondary use of these data is expected to result in further economic development. For example, face images can be obtained from various devices, such as surveillance cameras and smartphone cameras. In these situations, disclosing the face images without the permission of the individuals results in privacy issues. Hence, the noise-insertion approach is often used. For a face image, blurring and blacking part of faces are general methods. However, the images processed using these methods are not natural and their image quality is degraded.

Data anonymization technology is studied widely to distribute data while considering privacy issues. Many of these technologies protect the privacy of individuals by altering data such that they are indistinguishable. However, in general, conventional anonymization techniques use the Euclidean data space. Therefore, the anonymization techniques are ineffective for data with large dimensions. In addition, the recent development of machine learning represented by neural networks (NNs) has been remarkable. Although these techniques appear to be different from anonymization, both of them extract statistical information from a dataset. In particular, an NN has a hidden layer, which is expected to obtain intermediate information between the input and output of the target NN. In this study, a face image is used as an example of multidimensional data for anonymization. The aim of the proposed method is to anonymize the face image while retaining its quality. The proposed method maps the face image to the latent space of StyleGAN, which is one of the NNs, and anonymizes in the space.

II. RELATED RESEARCH

A. Natural Face Image Anonymization

Several studies have been conducted to anonymize face images using NNs. A face image anonymization method that generates natural images is briefly explained as a baseline of face image anonymizations in [1]. This method consists of three NNs: NN_M, which modifies the face; NN_D, which identifies the individual; and NN_A, which identifies the individual's actions. The distinct advantage of this method is the anonymization of

978-1-7281-5268-4/19/$31.00 ©2019 IEEE
DOI 10.1109/CANDARW.2019.00035

face images without quality compromise. This feature is achieved because NN_M outputs modified images that can be detected by NN_A correctly and cannot be detected by NN_D. However, the authors of the paper concluded that data are anonymized when their NN_D cannot identify the target individuals from the anonymized images. This does not comply with any definition of anonymity. Further, the resulting data by the method in proposed herein may not be suitable for secondary use. In fact, input face images can be almost similar to output images in some cases when using the method. Therefore, to guarantee anonymity, it is necessary to apply the conventional anonymization method in face image anonymization.

B. K-anonymity

Table 1 Row example of data for ***K***-anonymity

ID	ZIP-CODE	AGE	GENDER	DISEASE
t1	0123	22	FEMALE	CANCER
t2	0124	24	MALE	FLU
t3	0125	26	MALE	AIDS
t4	1220	31	MALE	COLD
t5	1221	39	MALE	FLU

Table 2 Anonymized example for Table 1 on ***K***-anonymity

ID	ZIP-CODE	AGE	GENDER	DISEASE
t1	0***	24	*	CANCER
t2	0***	24	*	FLU
t3	0***	24	*	AIDS
t4	122*	35	MALE	COLD
t5	122*	35	MALE	FLU

K-anonymity [2] is a typical method of privacy preservation considering anonymization level. Before explaining K-anonymity, the definition of **data table**, **index**, **attribute**, **identifier**, and **quasi-identifier** are given as follows.

1) Data table

A data table is a table constituting a database. The columns and rows of a data table are called the tuple and field, respectively. Table 1 is an example of a data table.

2) Index and Attribute

The heading of each tuple and field are called the index and attribute, respectively. Typically, an index is assigned to each user or each data sample, and an attribute indicates the data content. For example, in Table 1, ID is an index, and zip code, birthday, gender, and disease are attributes.

3) Identifier, quasi-identifier, and sensitive attribute

An identifier is an attribute directly connected to personal information that is unique to an individual. A social security number can be a typical example of such information. The identifiers are typically deleted when the data are anonymized. A quasi-identifier is an attribute that is used to identify individuals by combining it with other quasi-identifiers, such as zip code, gender, position information, and purchase history. Quasi-identifiers are anonymized when the anonymized data satisfy a given anonymization level completely. By contrast, sensitive attributes are not anonymized because they are important for secondary use and data analysis.

K-anonymity guarantees that the data have at least K-1 or more identical quasi-identifiers for any individuals. The process to obtain K-anonymity is called K-anonymization. Here, the data of Table 1 are used for explanation. Table 2 shows an example of K = 2 anonymized data generated from the data of Table 1. ID is an identifier and has to be deleted when it is anonymized. However, in this table, ID is left for the convenience of the before and after comparison of anonymization. In Table 2, disease information is protected by editing the zip code, age, and gender. Here, (t1, t2, t3) and (t4, t5) can be grouped together. As these groups share the same quasi-identifiers (i.e., zip code, age, and gender), an individual cannot be identified from these quasi-identifiers. In K-anonymization, individuals with similar quasi-identifiers are first divided into groups of size K or more; subsequently, each group's quasi-identifier is unified. Here, unification is a replacing operation of a quasi-identifier with a value computed from a set of quasi-identifiers in the same group. For example, the following processes are conceivable for anonymization: only the upper digits of a zip code are retained by masking; age is approximated using average values; and gender is erased.

In K-anonymization, grouping is important for minimizing information loss. However, the optimal grouping has been indicated as an NP-hard problem [3]. In fact, heuristics methods have been proposed when the optimal method is not required [4]. However, this heuristic method only considers hierarchical structures. Therefore, it cannot be applied to the vector data (i.e., image data) used in this study because the vector data does not have hierarchical structures. In addition, the computation cost will be increased because the data vector has a relatively higher dimension. Therefore, in this study, Mondrian is used for grouping. Although various Mondrian implementations exist, the grouping process as outlined in Algorithm 1 is used in this study.

Algorithm 1 Mondrian

i ($i \in \mathbb{N}$) denotes an individual, and v_i denotes his/her data ($v_i \in \mathbb{R}^d$). The number of dimensions to search is represented by N_s ($N_s \leq d, N_s \in \mathbb{N}$), and V denotes the set of individuals. Here, $v_{i,j}$ indicates the value of the j-th dimension of the data of individual i, and the initial value of V is $\{1,2,3,\dots\}$. K represents K-anonymity, and G is a group set that is the result of this grouping algorithm.

Step 1 If the number of elements in V is less than $2K$, add V to G.

Step 2 Create a set A of N_s integers at random without duplication from 1 to d.

Step 3 On the dimension j contained in A, calculate j^* by the following equation.

$$j^* = \underset{j \in A}{\operatorname{argmax}} \left(\max_{i \in V} v_{i,j} - \min_{i \in V} v_{i,j} \right)$$

Step 4 V is sorted by the j^*-th dimension and divided into V_a and V_b as the first and last half of V, respectively.

Step 5 Regard V_a and V_b as V and repeat Step 1, recursively.

Algorithm 1 is a recursive algorithm that outputs each grouping result in Step 1. In Step 1, if the size of set V is 2K or more, then the subsequent steps are performed because V can be divided into two sets having K or more elements. If the size of set V is less than 2K, V is added to G. This is because K-anonymity cannot be satisfied when it is further divided. In Steps 2 and 3, N_s dimensions are randomly selected. Subsequently, one of them (j^*) is selected with the largest difference between the maximum and minimum values. This random selection reduces the calculating cost compared with the full selection. In Step 4, V is sorted by j^* and divided into halves. In Step 5, Step 1 is performed recursively on each of the divided sets.

Algorithm 1 can specify the number of dimensions N_s to perform grouping at high speed even for high-dimensional data. This enables comparatively large dimensional data, such as face images used in this study ($3 \times 1024 \times 1024$), to be processed in a constant calculation time; namely, the calculation time is not affected by the size of the images.

C. *The problem of high-dimensional anonymization*

It is generally difficult to anonymize high-dimensional data [5], based on the following two perspectives. The first is unnecessary information in an actual analysis. The second is information that has nonlinear correlations. For example, in the case of face images, unnecessary information corresponds to the information of background images. Although the background image should have little relation to the analysis of a face image, the background and the face must be managed equally if anonymization is performed without pre-processing. Consequently, the groups of face images are affected by the background, and the quality of the anonymized images are deteriorated.

The second perspective has an adverse effect on anonymization because many grouping methods investigated in this study, including Mondrian, implicitly assume a Euclidean space in the data space. The space of actual data does not necessarily require the Euclidean distance to measure the semantic distance between data. When a sufficient amount of data exists, the space can be approximated as a Euclidean space around the data of an individual. However, in the case of high-dimensional data, data tend to be sparse, and such assumptions may not be applicable. Thus, the proposed method uses an actual knowledge space based on the real-world data for the case of sparse data. When supposing face images, we use StyleGAN as the actual knowledge space.

D. *StyleGAN*

StyleGAN [6] is an NN architecture proposed by Tero Karras et al. It generates high-resolution (1024×1024) face images. StyleGAN has two latent spaces, Z and W. Z is generated from a normal distribution, and W is obtained by mapping Z through a mapping network. In this study, we use StyleGAN to anonymize face images. StyleGAN obtains a face image by mapping W through a synthesis network. In a conventional GAN, face images are often obtained directly from Z, which is constrained by a normal distribution. This is because the face images of a conventional GAN are an entanglement in the Z space. In StyleGAN, the problem is solved by obtaining the latent space W by mapping with a mapping network from Z. In [6], it was experimentally confirmed that the latent space W is a disentanglement. Therefore, it is easier to obtain independent elements such as facial expression and gender linearly using the latent area W of StyleGAN than using the latent area of a conventional GAN. Consequently, face images with intermediate facial expressions and of different genders can be obtained by linear interpolation in latent space W.

III. PROPOSED METHOD

A. *Multidimensional Inputs K-anonymizing Unit (MIKU)*

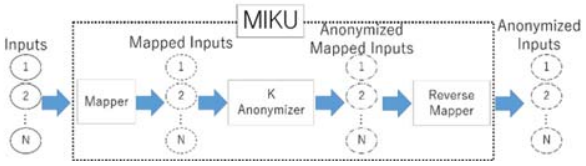

Figure 1 Architecture of multidimensional inputs K-anonymizing unit

We herein propose multidimensional inputs K-anonymizing unit (MIKU) as a new K-anonymization method. MIKU is divided into three modules: mapper, K-anonymizer, and reverse mapper, as shown in Figure 1. First, the mapper maps the input data. This mapping is performed to move data from the original space where they exhibit complex correlations between their elements to a new space that comprises independent components. For example, in a face image, the pixels of the face image are mapped to a space comprising independent components such as facial expression and gender. Next, the K-anonymizer anonymizes the mapped data by the same method as conventional K-anonymization. As described in Section II.C, the conventional K-anonymization method cannot effectively process high-dimensional data. Preferable anonymization results will be achieved compared with the case without mapping because the mapped data are in the space of

independent components. Finally, the reverse mapper returns the anonymized data to their original space. This module is used for releasing the original format data after anonymization. Therefore, the reverse mapper can be omitted when performing anonymization regardless of the data format.

MIKU adapts relatively advanced machine learning research to anonymization research; it is a method similar to the kernel method in machine learning. Therefore, it should demonstrate good performance for data with nonlinear correlations, comparable to the kernel method.

In this study, the mapper maps the original data to the space W^+, which extends the latent space W of the learned StyleGAN. The explanation of W^+ is given in Section B. In K-anonymizer, grouping is performed by Mondrian and the values are unified by the average value. The reverse mapper uses the learned StyleGAN's synthesis network.

B. Mapping to StyleGAN's latent space

StyleGAN has a function to generate face images using a mapping network and a synthesis network from Z that follows a normal distribution. However, a function to generate latent spaces W and Z from face images does not exist. In [7], the method to map face images to a latent space is discussed. The latent space W of StyleGAN is given as a 512-dimensional vector. The vector is used by 18 different layers in the synthesis network. As reported in [7], it is difficult to calculate W from face images. Therefore, W^+ is calculated instead of W. W^+comprises 18 different 512-dimensional vectors and these dimensional vectors correspond to these 18 layers. Two methods can be used to calculate $W^+$from face images: obtain a function that performs inverse mapping; and gradually changing from a suitably selected W^+ to obtain the optimal W^+, which can create the target face using a synthesis network. In [7], the method to change gradually is adopted. This means that W^+ is updated by the gradient method to obtain W^{+*} in (1).

$$W^{+*} = \underset{W^+}{\operatorname{argmin}} Loss\left(I, G(W^+)\right) \tag{1}$$

The function G represents the synthesis network of a trained StyleGAN, and I is the target face image of an inverse mapping. Loss is the difference between I and $G(W^+)$, which will be described in detail in Section IV.B.

IV. EXPERIMENT

A. Preprocessing

Face images often include not only faces, but also background images. However, background information is not required to determine the latent space of StyleGAN. To remove the background of an image, we used the learned FCN-Resnet 101 [8] and masked it such that the background was not included in the learning of W^{+*} in (1). Subsequently, StyleGAN generates face images, in which the positions of the eye, nose, and mouth are fixed. Therefore, referring to [9], the face is clipped into a rectangle and the positions of the eyes and nose are fixed. In addition, the size of the rectangle was resized to 1024×1024.

B. Loss function

The sum of L_2 and $L_{percept}$ was used as the loss function(2) with reference to [7].

$$\text{Loss}(I_1, I_2) = L_2(I_1, I_2) + L_{percept}(I_1, I_2) \tag{2}$$

L_2 is a function that takes the sum of L_2 norms of pixels between images I_1 and I_2. $L_{percept}$ is the sum of L_2 norms of the difference of the output values of conv1_1, conv1_2, conv3_2, conv4_2 of VGG-16 [10]. $L_{percept}$ is added because it can learn face image details such as wrinkles and hair [7] easier.

C. Fréchet Inception Distance (FID)

To evaluate the performance of the proposed method, an index that indicates the image quality is required. For this index, we use the Fréchet inception distance (FID)[11], which is also used as a performance indicator for StyleGAN. FID is an index that evaluates the perceptual difference between two image sets using the output h (2048 dimension) of the pool in the last hidden layer of the learned inception model [12]. The FID is calculated by (3).

$$\begin{aligned} \mu_{diff} &= |\mu_A - \mu_B|^2 \\ \Sigma_{diff} &= tr\left(\Sigma_A + \Sigma_B - 2(\Sigma_A \Sigma_B)^{\frac{1}{2}}\right) \\ \text{FID} &= \mu_{diff} + \Sigma_{diff} \end{aligned} \tag{3}$$

Here, the mean and the variance–covariance matrix of h are μ_A, μ_B, Σ_A, and Σ_B, respectively. Typically, when measuring the FID, A or B represents a set of images used for learning. In this study, sets A and B refer to the set of face images before and after anonymization, respectively. Therefore, when the FID is low, B is composed of images showing the same distribution as the image before anonymization, and it is clear that B is a set of images of higher quality. We calculated the FID according to [13].

D. Comparison method (DIRECT)

Conventional methods exist such as those described in [1] [14] [15]. All these conventional methods are not based on k-anonymity. In [1] and [14], only the amount of information was reduced and well-known anonymity indexes such as k-anonymity, l-diversity, or differential privacy were not considered. Although k-anonymity was applied in [15], the anonymity index and the method to calculate the index were not disclosed. Therefore, these methods are not comparable. In this study, we created a method called DIRECT as a comparison method of MIKU. DIRECT uses the identity function as a mapper.

E. Experimental environment

We selected 5749 images of individuals randomly from LFW [16] to use for the evaluations. We used one face image

of each individual. However, as a result of preprocessing, only 5722 face images were used in this experiment because there were face images not recognized as faces.

The experiment was conducted for two anonymized images, one is anonymized by MIKU and the other by DIRECT. Both methods observe the definition of K-anonymity. The parameters were K = [2, 4, 8, 16, 32, 64, 128] for K-anonymization, and N_s= 9216 for Mondrian. After evaluating the FID, a qualitative evaluation of anonymized images was performed. The experiment used a machine with one NVIDIA V100 and a machine with four NVIDIA P100s.

V. Results

A. FID

Table 3 FID for DIRECT and MIKU. MIKU is the proposed method, and DIRECT is the comparison method. The leftmost column shows the level of K-anonymity.

K	DIRECT	MIKU
2	61.17	111.8
4	128.8	127.6
8	178.0	146.1
16	190.6	162.8
32	200.5	176.1
64	227.9	191.7
128	245.1	202.6

The measured FIDs are as shown in Table 3. As shown, MIKU has a lower FID compared with DIRECT except when K = 2, and DIRECT has a lower FID compared to MIKU only when K = 2. However, even when K = 2, the proposed method demonstrates good performance qualitatively, as described in Section B. Therefore, reasons contributing to a difference between qualitative evaluation and FID evaluation will be discussed.

If the function f (.), which outputs h of the inception model, is linear, the average value of h of the image anonymized by DIRECT is equal to that of the face image before anonymization because of the linearity of the function f, as shown in (4):

$$\frac{1}{N}\sum_{q\in Q}|q|f\left(\frac{1}{|q|}\sum_{i\in q}I_i\right)=\frac{1}{N}\sum_{q\in Q}\sum_{i\in q}f(I_i)$$
$$=\frac{1}{N}\sum_{i}^{N}f(I_i), \quad (4)$$

where N is the total number of images to be anonymized, Q is a set of face image ID groups that share the same quasi-identifier after anonymization, $|q|$ is the number of elements of q, and I_i is a face image of i. If the function f is linear, it is clear that μ_{diff} in (3) will be zero. Therefore, we discuss the conditions where the linearity of the function f is satisfied. An NN typically learns nonlinear functions, and the inception model can be categorized as such an NN. However, the convolution operation and the linear mapping that compose the inception model are both linear processes; namely, the inception model can exhibit nonlinearity because of the Relu function used as the activation function.

The Relu function is a function defined by the following equation (5).

$$\text{Relu}(x)=\begin{cases}x & x>0\\ 0 & x\le 0\end{cases} \quad (5)$$

This shows that if the domain is $x > 0$ or $x \le 0$, then the Relu function becomes a linear function.

$$\frac{1}{N}\text{Relu}\left(\sum_i X_i\right)=\text{Relu}\left(\frac{1}{N}\sum_i X_i\right) \quad (6)$$

If (6) is satisfied, all N values $(X_1, X_2, \ldots, X_N)$ must have the same sign. For example, assuming that the probability of X_i having a positive value is p, the probability of all values having the same sign is

$$p^N + (1-p)^N$$

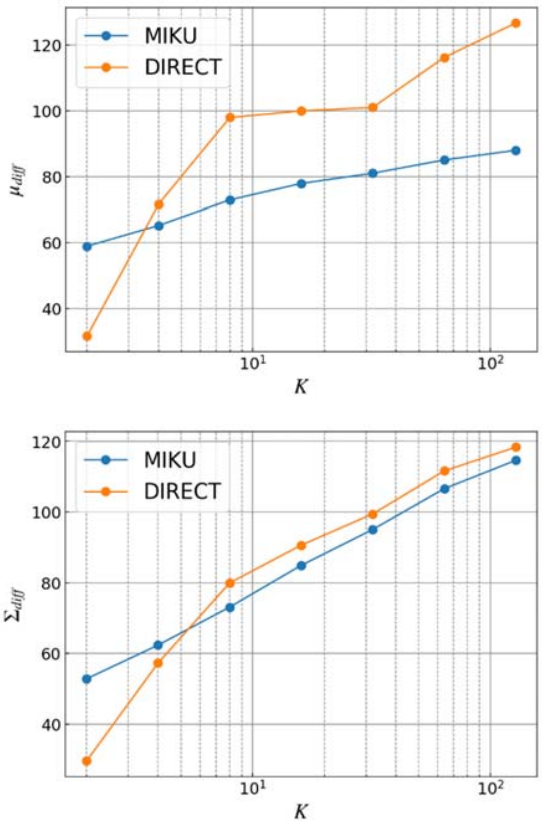

Figure 2 Trends of μ_{diff} and Σ_{diff} relative to K

As p is less than 1, it decreases as N increases. It can be regarded that the linearity of the Relu function is lost as N

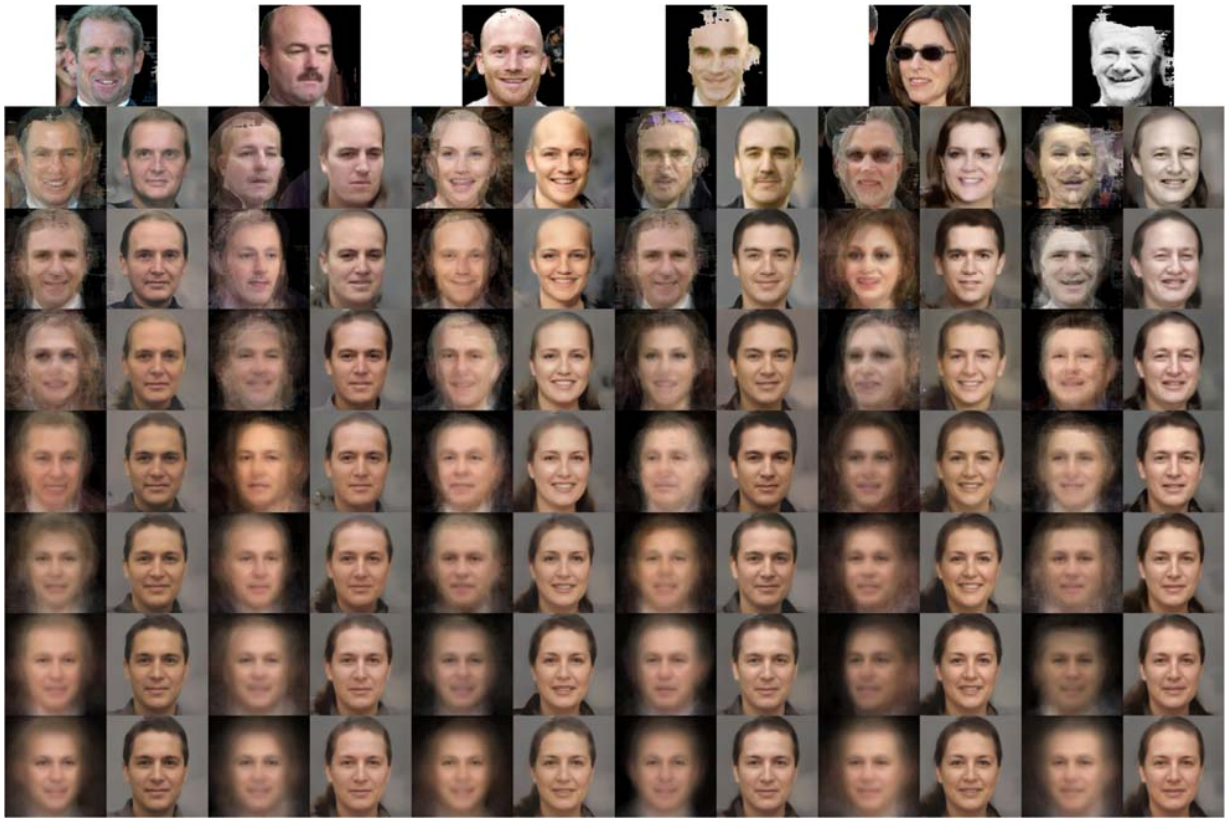

Figure 3 Output result of DIRECT and MIKU: The top row represents the original face images, and the following rows represent the anonymized image with $K = [2, 4, 8, 16, 32, 64, 128]$ in order from the top. The odd column is the anonymized image by DIRECT, and the even column is the anonymized image by MIKU.

increases. In DIRECT, increasing N corresponds to increasing K of the anonymization index.

Figure 2 shows the transition of μ_{diff} and Σ_{diff} in (3) when K is varied. It shows that the increase in μ_{diff} in DIRECT is larger than the increase in MIKU when K increases from 2 to 4. It can be inferred that the linearity of the function f is lost owing to the loss of Relu's linearity in the previous argument. Therefore, when K = 2, DIRECT obtains an abnormally low FID because of the linearity of the Relu function, and thus the FID cannot correctly indicate the quality of DIRECT. In addition, although Σ_{diff} is unverified in the previous discussion, Figure 2 shows that the principle similar to μ_{diff} applies for Σ_{diff}.

B. Qualitative evaluation

In addition to evaluating the FID, we evaluated the anonymized image qualitatively. Figure 3 shows the anonymized image by DIRECT and MIKU as the proposed method. The top row represents the original image, and the following rows represent the anonymized face image with $K = [2, 4, 8, 16, 32, 64, 128]$ in order from the top. The odd and even columns were created using DIRECT and MIKU, respectively.

Figure 3 shows that the eye, nose, and mouth are naturally synthesized even in DIRECT because their positions were aligned during pre-processing. However, the expressions of the face contour and the hair are unnatural. In addition, because the average value is used for unification, an unnatural edge appears on the face, especially when K is small. The anonymized image of MIKU expresses not only the eyes, nose, and mouth correctly, but also the hair and contour naturally. Further, unnatural edges do not appear on the face. This is because StyleGAN's latent space comprises a space suitable for outputting a natural face image. Based on these results, we can conclude that MIKU improves the quality of anonymized images even though K-anonymity is considered.

VI. CONCLUSIONS

First, we confirmed a problem in the anonymization of high-dimensional data. Hence, we proposed MIKU, which maps data by a specific function and anonymizes on a mapped space. As typical multidimensional data, face images were used

as the target of anonymization. Moreover, StyleGAN's latent space was used as the mapper of MIKU. To evaluate the quality of the created anonymized face images, the FID by the inception model was used. Consequently, except when $K = 2$, MIKU yielded higher quality images than DIRECT. Furthermore, we discussed the linearity of the inception model when $K = 2$ and clarified why the FID value of DIRECT was lower than that of MIKU. In addition, a comparison using actual synthesized images confirmed that problems such as unnatural contours, hair, and face edges occurred in DIRECT but not in MIKU.

VII. FUTURE WORKS

In this study, only the FID value was used to evaluate the quality of face images. As a next step, we plan to evaluate changes in information such as facial expression and gender, which can be estimated clearly when looking at face images. In addition, approximately 30 s was required to map a face image to the latent space of StyleGAN. Therefore, it may be difficult to adapt MIKU to a large face database. The method of inverse mapping may be developed, for example, to accelerate mapping by obtaining the inverse function without using the gradient method used in this study. Moreover, to demonstrate the general performance of MIKU, we will adapt MIKU to data other than face images.

ACKNOWLEDGMENT

This work was supported by JST CREST Grant Number JPMJCR19K1, MEXT/JSPS KAKENHI Grant (B) Number JP16H04455, and JP17H01739.

REFERENCE

[1] Z. Ren, Y. J. Lee, and M. S. Ryoo, "Learning to Anonymize Faces for Privacy Preserving Action Detection," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11205 LNCS, pp. 639–655, 2018.

[2] L. SWEENEY, "k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY," Int. J. Uncertainty, Fuzziness Knowledge-Based Syst., vol. 10, no. 05, pp. 557–570, Oct. 2002.

[3] A. Meyerson and R. Williams, "On the complexity of optimal K-anonymity," in Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems - PODS '04, 2005, p. 223.

[4] B. Kenig and T. Tassa, "A practical approximation algorithm for optimal k-anonymity," Data Min. Knowl. Discov., vol. 25, no. 1, pp. 134–168, Jul. 2012.

[5] C. C. Aggarwal, "On k -anonymity and the curse of dimensionality," Proc. 31st VLDB Conf., no. January 2005, pp. 901–909, 2005.

[6] T. Karras, S. Laine, and T. Aila, "A Style-Based Generator Architecture for Generative Adversarial Networks," IEEE Conf. Comput. Vis. Pattern Recognit., 2019.

[7] R. Abdal, Y. Qin, and P. Wonka, "Image2StyleGAN: How to Embed Images Into the StyleGAN Latent Space?," arxiv, Apr. 2019.

[8] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 3431–3440.

[9] "ffhq-dataset/download_ffhq.py at master · NVlabs/ffhq-dataset · GitHub." [Online]. Available: https://github.com/NVlabs/ffhq-dataset/blob/master/download_ffhq.py. [Accessed: 05-Jul-2019].

[10] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," arxiv, Sep. 2014.

[11] M. Heusel, H. Ramsauer, T. Unterthiner, B. Nessler, and S. Hochreiter, "GANs trained by a two time-scale update rule converge to a local Nash equilibrium," in Advances in Neural Information Processing Systems, 2017, vol. 2017-Decem, pp. 6627–6638.

[12] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the Inception Architecture for Computer Vision," in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, vol. 2016-Decem, pp. 2818–2826.

[13] "GitHub - bioinf-jku/TTUR: Two time-scale update rule for training GANs." [Online]. Available: https://github.com/bioinf-jku/TTUR. [Accessed: 05-Jul-2019].

[14] H. Hukkelås, R. Mester, and F. Lindseth, "DeepPrivacy: A Generative Adversarial Network for Face Anonymization," Sep. 2019.

[15] T. Li and L. Lin, "AnonymousNet: Natural Face De-Identification with Measurable Privacy," Apr. 2019.

[16] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments," 2007.