International Journal of Innovative
Computing, Information and Control
Volume **12**, Number **4**, August **2016**

ICIC International ©2016 ISSN 1349-4198
pp. 1375–1384

FUZZY CLUSTERING-BASED k-ANONYMIZATION OF EIGEN-FACE FEATURES FOR CROWD MOVEMENT ANALYSIS WITH PRIVACY CONSIDERATION

Katsuhiro Honda, Masahiro Omori, Seiki Ubukata and Akira Notsu

Graduate School of Engineering
Osaka Prefecture University
Sakai, Osaka 599-8531, Japan
{ honda; subukata; notsu }@cs.osakafu-u.ac.jp

Received December 2015; revised May 2016

Abstract. *Clustering-based k-anonymization is a simple but powerful approach for privacy preserving data analysis. In this paper, fuzzy k-member clustering is applied to crowd movement analysis based on face image recognition with privacy consideration. The movement of an individual in such a multipurpose complex as station buildings is tracked by matching face images photographed in different places, and is summed up to crowd movement. Before applying for face image matching, face image features are k-anonymized by utilizing fuzzy cluster partitions. In a numerical experiment, the advantage of fuzzy partition-based model against the conventional crisp one is demonstrated, and the influence of fuzziness degree tuning is investigated such that careful tuning of fuzzy degree can contribute to handling the trade-off between information losses and computational costs.*

Keywords: Privacy preserving data analysis, Fuzzy clustering, k-anonymization, Crowd movement analysis

1. **Introduction.** In handling various sensitive personal information, data mining should be performed with a secure framework for privacy preserving data analysis [1]. A simple but practical approach for applying conventional data mining tools to sensitive information without privacy violation is to analyze them after anonymizing personal data. k-anonymization [2, 3] is a standard technique for quantitatively guaranteeing privacy preservation, where anonymity level k is set so that every sample is indistinguishable from at least $k-1$ other samples.

The process of k-anonymization is reduced to the problem of finding the groups of k homogeneous samples to be packaged into their representative observations with minimum information loss while the process is essentially a combinatorial optimization problem and is often computationally expensive. A practical and greedy approach to k-anonymization is realized by sequential k-member clustering [4], in which k-member clusters are extracted one-by-one by adopting information loss in anonymization as the measure of the degree of cluster compactness. Fuzzy k-member clustering [5] is a fuzzy variant of crisp k-member clustering, in which k-member clusters are extracted with fuzzy memberships of k-members and each sample can belong to multiple clusters with fuzzy memberships in the case of boundary positions. As in the general fuzzy clustering context [6], the fuzzy partition approach was shown to be useful for revealing natural cluster structures.

In this paper, the applicability of the fuzzy clustering-based k-anonymization model to crowd movement analysis based on face image recognition with privacy consideration is studied. In a previous work [7], (crisp) k-member clustering-based anonymization was applied to face recognition with eigen-face features and was demonstrated to be applicable

to capturing crowd movement preserving personal privacy. The movement of an individual in such a multipurpose complex as station buildings is tracked by matching face images photographed in different places, and is summed up to crowd movement. Although face images are informative in personal authentication, their utilization in public space may bring public fear of information abuse [8, 9]. Before applying for face image matching, face image features are k-anonymized by utilizing fuzzy cluster partitions. The goal of this paper is to improve the quality of k-anonymization-based crowd movement analysis by introducing the fuzzy clustering-based scheme. Additionally, the influence of fuzziness degree tuning is investigated such that careful tuning of fuzzy degree can contribute to handling the trade-off between information losses and computational costs.

The remaining parts of this paper are organized as follows. Section 2 briefly reviews the fuzzy clustering-based k-anonymization process, and Section 3 introduces two possible strategies for achieving privacy preserving crowd movement analysis. Characteristic features of the proposed model are demonstrated in a numerical experiment of Section 4 and a summary conclusion is given in Section 5.

2. Fuzzy Clustering-Based k-Anonymization.

2.1. Fuzzy k-member clustering.

k-anonymity [2, 3] is often achieved by packaging observations of k or more samples into a solo observation such as representative values of the samples or generalized categories of nominal observations. From the view point of minimization of information losses, the k or more samples to be packaged into a certain observation should be as similar as possible. Then, the task has close relation to clustering techniques.

k-member clustering [4] is an unsupervised classification model, in which the size of each cluster is constrained to be k or larger although the conventional k-means-type clustering models [6] often pre-fix the number of clusters rather than the size of them. In [4], the information loss to be minimized is measured in cluster G_c as follows:

$$IL_c = |G_c|\left(\sum_i \frac{\max_{ci} - \min_{ci}}{Size_i} + \sum_j \frac{H(\Lambda(\cup_{cj}))}{H(\mathcal{T}_j)}\right), \tag{1}$$

where $Size_i$ is the size of numeric domain of numeric attribute i, and $\max_{ci}$ and $\min_{ci}$ are the maximum and minimum values in G_c. $\mathcal{T}_j$ is the taxonomy tree defined for the domain of categorical attribute j and $H(\mathcal{T})$ is the height of taxonomy tree $\mathcal{T}$. $\Lambda(\cup_{cj})$ measures the deviation in G_c. The sequential cluster extraction was implemented iteratively by selecting a core sample and merging its $k-1$ neighbors such that IL_c is minimized. Then, the number of clusters is nearly equal to (the number of samples/k).

Fuzzy k-member clustering [5] introduced the concept of fuzzy partition [6] into the (crisp) k-member clustering algorithm because fuzzy partition often outperforms crisp one from the view points of noise or initialization sensitivity. Assume that u_{tr} represents the membership degree of sample r to cluster t and can take $u_{tr} \in [0, 1]$ in the fuzzy partition model although the crisp model brings $u_{tr} \in \{0, 1\}$ only. Considering the exclusive constraint of $\sum_t u_{tr} < 1$, each sample tends to belong to at most a solo cluster with large memberships while some boundary samples can also be weakly shared by multiple clusters having very fuzzy memberships.

In order to fairly evaluate the confidence of belongingness to each k-member cluster, the fuzzy membership degrees are estimated with a fuzzy membership function w.r.t. distance from clusters. If a sample is not so familiar with other cluster members but is assigned to the cluster, the assignment has a low confidence, i.e., a small fuzzy membership u_{tr}, and a larger residual membership allows the sample to belong to other (later) clusters.

A sample procedure for the greedy algorithm [5] can be summarized as follows.

[Greedy fuzzy *k*-member clustering algorithm]

1. **Initialization:** Let S be a set of samples and u_i be the residual membership of sample i. Set all u_i to be 1 and the stopping flag to be "$False$". Choose the anonymity level k and randomly select a sample r.
2. **Sequential cluster extraction:** Let a cluster index t be 0. Repeat the following process while the stopping flag is "$False$" and $|S| > 0$.
   (a) **Core selection:** Replace r ($r \in S$) with its furthest sample and remove r from S. $t = t + 1$. Generate cluster G_t with a single element r. Set the fuzzy membership u_{tr} of element r for G_t as $u_{tr} = 1$ and $u_r = 0$.
   (b) ***k*-member merging:** Repeat the following process while the stopping flag is "$False$" and $|G_t| < k$.
      (i) Find the best neighbor sample r of cluster G_t, whose residual membership is $u_r > 0$.
      (ii) Add r to cluster G_t. Remove r from S if $r \in S$. Calculate u_{tr} and set as $u_r = u_r - u_{tr}$.
      (iii) If there is no remaining sample in S, the stopping flag is "$True$".

Step 2-(b) merges neighbor samples into a k-member cluster calculating their fuzzy memberships. Step 2-(b)-(i) searches for the best neighbor in such a way that the typicality is calculated by (similarity s_{it}) $\times$ (residual membership u_i). Step 2-(b)-(ii) is responsible for estimating fuzzy membership u_{tr} considering the distance between sample r and cluster G_t. This fuzzy operation makes it possible for boundary samples to belong to multiple clusters, i.e., a sample can belong to the second or later clusters if it has small membership to the first cluster and is also near to the second or later clusters.

2.2. **Tuning of fuzziness degree of membership function.** In [10], a comparative study on several fuzzy membership functions was performed and it was shown that the following exponential-type function can achieve soft transition from a very fuzzy model to the crisp one:

$$u_{cr} = \exp\left(-\frac{IL_{cr}}{\sigma}\right) \times u_r, \tag{2}$$

where IL_{cr} is the information loss of Equation (1) after merging r. $\exp\left(-\frac{IL_{cr}}{\sigma}\right)$ works for transforming the information loss to a similarity measure and σ tunes the degree of fuzziness.

Figure 1 demonstrates the influence of the fuzzification parameter σ with $u_r = 1$. When σ is large, $u_{cr} \to 1$ and the model is reduced to the crisp one, i.e., each sample has a large membership to the first candidate cluster and cannot belong to other (later) clusters. On the other hand, when σ is small, only a few samples locating very near to cluster cores can have large memberships to their first candidate cluster and many other samples may reserve large residual memberships u_r for second and later ones. Then, many boundary samples having mid-range information losses to multiple clusters tend to belong to multiple clusters.

In this paper, the characteristics of fuzzy partition-based k-anonymization are studied by adopting the fuzzy membership function of Equation (2) with various values of fuzzification parameter σ.

2.3. **Construction of *k*-anonymized data tables.** Once k-member clusters are extracted, a k-anonymized data table can be constructed by packaging observations of each compact cluster into a solo observation, such as a representative value or an interval value.

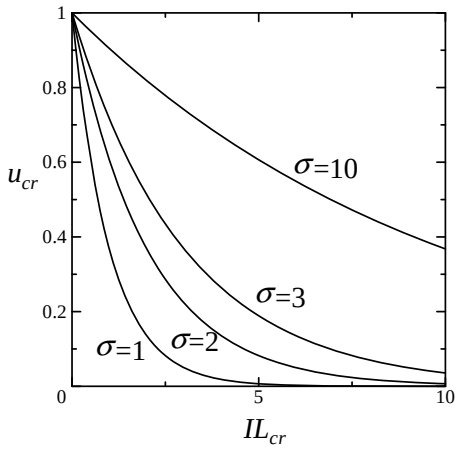

FIGURE 1. Influence of fuzzification parameter σ in membership function

Then, k or more samples have the same observation so that they are not distinguishable in the anonymized data table. In order to guarantee k-anonymity, all k members should be equally handled in each cluster even if some members have very small memberships only. In the experiment of this paper, the k-member merging process was implemented with equal responsibility without consideration of fuzzy membership degrees and the mean values of each k-member cluster were used for the representative values, i.e., exactly k or more samples are coded into their mean vector in each k-member cluster. It is also possible to code the k members into membership-weighted mean vectors although some anonymized records may be almost equivalent to a dominant member of their cluster when only a solo member has a large membership in the cluster.

Here, it should be noted that the fuzzy clustering-based k-anonymization can construct anonymized data tables having more samples than the original one. If the number of k-member clusters is T, the size of the anonymized data table is equal to (or slightly larger than) $T \times k$. In the crisp partition model, the size is always equal to the original one because each sample belongs to one of T clusters only. On the other hand, in the fuzzy clustering-based model, some samples belong to multiple clusters and $T \times k$ may be larger than the original size. The heavier the cluster overlapping is, the larger the anonymized data size is.

In the experimental section, the computational efficiency of the proposed framework is compared using the size of anonymized data tables, i.e., a larger table size causes a heavier cost in pattern matching.

3. *k*-Anonymization-Based Privacy Preserving Crowd Movement Analysis.

3.1. **Problem space.** In such multipurpose complexes as station buildings, it is quite important to capture intrinsic crowd movements in order to better plan for emergency procedures during disasters. In this paper, a face recognition-based approach to crowd movement analysis is considered, where each movement of individuals is tracked by utilizing camera images [11].

Assume that face images are stored by multiple cameras in various places of a multipurpose complex and the goal is to reveal the intrinsic crowd movement. If an individual in a camera image can be identified with one in another camera image, we can find his/her path between the cameras and sum the paths up to crowd movement.

The eigen-face model [12] is a basic face image recognition approach, in which pattern matching among various face images is performed in a low-dimensional eigen-face space.

Let $\boldsymbol{x}_i$, $i = 1, \ldots, n$ be m-dimensional vector observation of pixel intensity values of n face images and $\hat{X} = (\hat{\boldsymbol{x}}_1, \ldots, \hat{\boldsymbol{x}}_n)$ be the $m \times n$ normalized matrix, where rows and columns of X are pre-centered. Principal component analysis (PCA) or singular value decomposition (SVD) can perform lower rank approximation of eigen-decomposition with rank p ($p < m$) as:

$$\hat{X} \approx AF, \tag{3}$$

where $m \times p$ principal eigen basis matrix A is composed of m-dimensional eigen-face vectors $\boldsymbol{a}_j$, $j = 1, \ldots, p$. Each face image $\hat{\boldsymbol{x}}_i$ is assumed to be a linear combination of eigen-faces $\hat{\boldsymbol{x}}_i \approx A\boldsymbol{f}_i$ with p-dimensional score vectors $\boldsymbol{f}_i$. In the eigen-face model [12], face image matching is performed only with lower rank score matrix $F = (\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n)$.

In this paper, personal authentication is achieved by matching face image features $\boldsymbol{f}_i$ in the lower dimensional eigen-face space because the eigen-face approach is efficient from the view points of computational cost and noise sensitivity. (Besides the eigen-face approach, it is obvious that the proposed framework can be implemented straightforward with any other face image features.)

3.2. **Two strategies for implementing k-anonymization.** This paper considers a situation, where a multipurpose complex has several entrance/exit gates and face images of individuals entering/exiting through the gates are stored. Figure 2 shows an experimental situation used in [7], which is also used in the experiment of this paper. In this model, each individual's movement is tracked by matching each face image photographed in exit gates with its corresponding face image of entrance gates. Therefore, all face images photographed in entrance gates must be gathered into a data center and are utilized in the face recognition phase, in which all entrance images can be candidates of the corresponding image for each exit image.

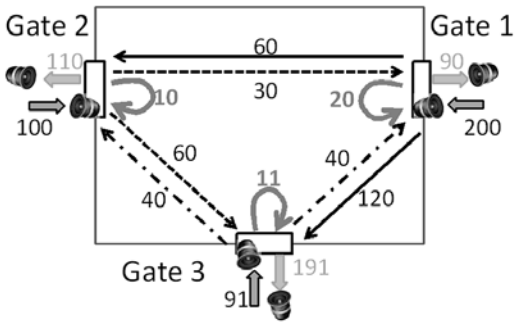

FIGURE 2. An experimental situation of crowd movement in a building [7]

In constructing a large database of personal information such as face images, many people feel fear of information abuse [8]. A promising approach is to construct a face image database considering k-anonymization such that each face image feature is k-anonymized at each camera site before sending to the data center.

Here, two anonymization strategies can be adopted in this situation [7]. In both strategies, it is assumed that eigen-face-based dimension reduction of face images was applied before implementing k-anonymization and face recognition, i.e., the following processes are implemented in low-dimensional eigen-face spaces.

3.2.1. *Strategy 1: Anonymization at entrance gate only.* If we can perform pattern matching among an exit face image and entrance face images at each exit gate, k-anonymization should be applied only in the entrance gates because the exit face images are not sent to and stored in the data center. In this strategy, the face image features generated in each

entrance gate are anonymized before sending to the data center, i.e., k-anonymization is performed in each entrance gate. Then, in the anonymized table, k face images features are coded into an average face of them.

In the recognition phase, whole entrance face features, which were coded into average face features of k faces, are sent to each of the exit gates and pattern matching and individual movement estimation are performed at each exit gate.

Here, k-anonymization also brings another merit of reducing the size of entrance image data table into a $1/k$ scale because k features are coded into a solo observation in each k-member cluster.

3.2.2. *Strategy 2: Anonymization at both entrance and exit gates.* If we want to store all face features in the data center and perform face recognition there, both entrance and exit gates should anonymize their features before sending them to the data center. Once all anonymized face feature vectors are gathered into the data center, pattern matching can be safely performed without fear of privacy violation. In the data center, anonymized face features are stored with their entrance or exit gate indices and pattern matching with entrance data is operated for each exit gate face feature.

This strategy is securely and easily implemented in the data center, but may cause severe information losses in dual anonymization.

4. **Numerical Experiment.** A numerical experiment was performed in the same experimental situation with [7], which is shown in Figure 2. Each arrow and its associated number show the moving path of individuals and the number of individuals with the path, respectively. Two cameras are located in each gateway, which take face images of individuals entering (getting out) through the gate. The goal of this analysis is to estimate the crowd movement (the number of each path) utilizing the face images stored in the gateway cameras, i.e., the goal is to predict the correct crowd movement vector $\boldsymbol{CMV}_o$ ($1\to1$, $1\to2$, $1\to3$, $2\to1$, $2\to2$, $2\to3$, $3\to1$, $3\to2$, $3\to3$) $= (20, 60, 120, 30, 10, 60, 40, 40, 11)$.

In this experiment, it is assumed that face images have already been stored from video images, which were recorded by cameras in entrance/exit gates, by utilizing some face detection algorithms [13]. Then, a face recognition experiment was performed with a face image benchmark data set. The face recognition data presented by University of Essex [14] includes 24bit color JPEG face images of 391 independent individuals with 20 images per individual. Before the experiment, the color JPEG images were transformed into gray-scale ones with 32×32 pixels for reducing computational difficulties. In this experiment, two images were selected for each of 391 individuals and were distributed to the camera of its corresponding entrance (or exit) gate. In the dimension reduction phase, 391 entrance face images with 1024-dimensional intensity value vectors were reduced to 10-dimensional 391 feature vectors ($n = 391, m = 10$) by eigen-face-based dimension reduction. The exit face images were also processed into 10-dimensional vectors using the general eigen-face basis given by the entrance face images, and k-anonymization and pattern matching are performed in the 10-dimensional eigen-face space. Then, crowd movement vectors $\boldsymbol{CMV}_1$ are estimated by counting the number of each path movement, i.e., the matching of entrance/exit images. In order to remove the influences of data distortion, 4 different data sets were also generated by arranging the assignment of individuals and the results of 5 trials are summarized.

The performance of the proposed framework was evaluated under two criteria. The quality of face recognition is measured by the ratio of correct estimation of entrance gates for each exit image. In the case without data anonymization, the ratio of correct estimation was 0.991 in 5 trial average. So, the 10-dimensional eigen-face features are informative

enough to recognize each individual. Be noted that, however, because of k-anonymization, exact authentication of each individual cannot be achieved with anonymized data tables and the degree of degradation is measured through the quality of entrance gate estimation.

Another criterion is the similarity among the estimated $\boldsymbol{CMV}_1$ and the intended $\boldsymbol{CMV}_o$, which is evaluated by the cosine correlation coefficient (CCC) among them. The larger the CCC, the better the prediction quality. In the case without data anonymization, CCC was 0.999 in 5 trial average.

The goal of privacy preserving crowd movement analysis is to reveal the intrinsic characteristics of crowd movement under consideration of privacy preservation. In the proposed framework, personal privacy is preserved by adopting k-anonymization to each face image feature.

4.1. **Strategy 1: Anonymization at entrance gate only.** First, *Strategy 1* was implemented with various anonymity levels $k = \{1, 2, \ldots, 10\}$ and fuzziness parameters $\sigma \in \{0.5, 1.0, 2.0\}$ in Equation (2), and the results are compared with those of the conventional crisp model. Figures 3 and 4 compare the average correct individual identification rates and the average cosine correlation between the estimated $\boldsymbol{CMV}_1$ and the ideal $\boldsymbol{CMV}_o$, where $k = 1$ is the result without anonymization. In the figures, the points depicted by $\odot$ imply the statistically significant advantage of the proposed fuzzy partition approach against the crisp one with significance level 0.05.

Figure 3 implies that the proposed fuzzy partition-based k-anonymization approach can significantly improve the quality of individual's movement estimation, and fuzzier models seem to be plausible. However, from the view point of crowd movement analysis, Figure 4 indicates the result of $\sigma = 0.5$ is comparative with that of $\sigma = 1.0$.

Then, the model efficiency is next considered by comparing the size of the anonymized data tables. Be noted that, in the fuzzy partition-based model, some samples can appear

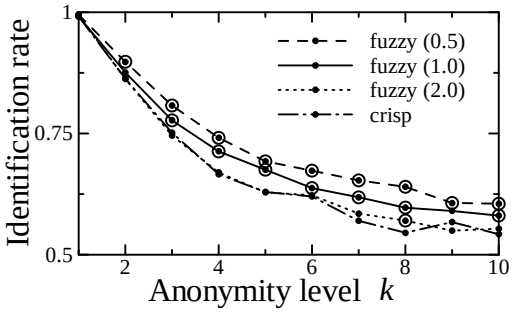

FIGURE 3. Comparison of correct individual identification rates in *Strategy 1*

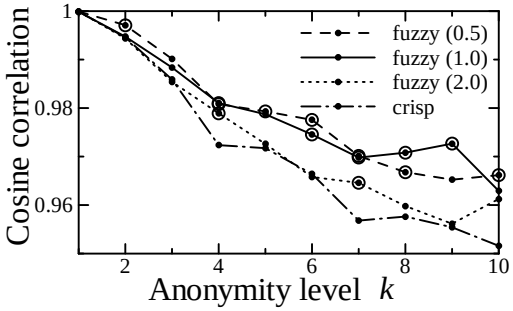

FIGURE 4. Comparison of cosine correlation coefficients in *Strategy 1*

multiple-times in the anonymized table if they belong to multiple k-member clusters with very fuzzy memberships. Figure 5 compares the number of data records in k-anonymized data tables. As seen in Section 2.3, a small σ brings relatively low confidences in sample assignment and causes sharing of samples in multiple k-member clusters. So, in case of $\sigma = 0.5$, the size of anonymized data table became 150% or more than the original one with $k = 7$ or larger. This implies that the proposed fuzzy partition-based approach achieves a higher performance by generating multiple virtual copies of boundary samples in anonymized data tables, and very fuzzy partition models can cause significant decreases of computational efficiency in the face image matching phase.

From the above discussions, a slightly fuzzy model such as $\sigma = 1.0$ seems to be the most plausible one handling the trade-off of the computational efficiency and the analysis quality.

By the way, in the previous study [7], it was implied that the model with $CCC = 0.96$ is still useful for revealing intuitional characteristics of crowd movement vectors. In

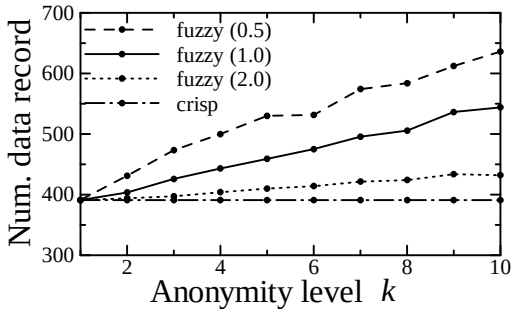

FIGURE 5. Comparison of size of anonymized tables in *Strategy 1*

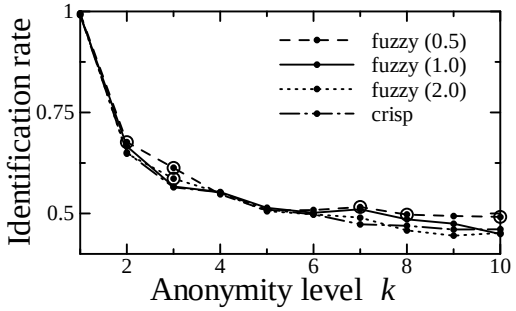

FIGURE 6. Comparison of correct individual identification rates in *Strategy 2*

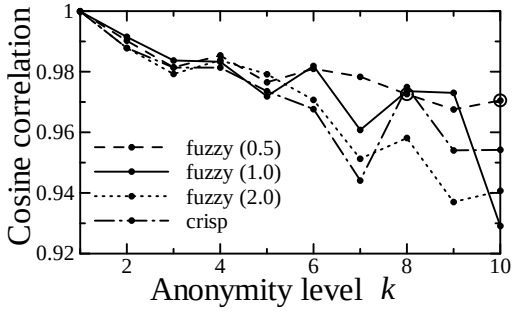

FIGURE 7. Comparison of cosine correlation coefficients in *Strategy 2*

this sense, the proposed fuzzy partition-based model can contribute to achieving privacy preserving crowd movement analysis with higher anonymity levels of $k = 10$ or larger.

4.2. **Strategy 2: Anonymization at both entrance and exit gates.** Second, *Strategy 2* was implemented in the same manner with the previous one. The performances are compared in Figures 6 and 7.

Because of double anonymization of entrance and exit images, the individual identification quality was significantly degraded compared with the result of *Strategy 1* (c.f. Figures 3 and 6). Additionally, the performance of the fuzzy partition-based model is almost comparative with that of the crisp one, and the analysis quality is stable only in low anonymity levels such as $k \leq 5$.

Then, we can say that *Strategy 2* is available only in the cases of low anonymity levels, where the fuzzy partition-based model cannot contribute to improvement of analysis quality.

5. **Conclusions.** In this paper, the previous study on k-anonymization-based crowd movement analysis with face recognition [7] was improved by introducing fuzzy partition-based k-member clustering. For *Strategy 1*, where k-anonymization is adopted only to entrance images, experimental results demonstrated the advantage of fuzzy clustering-based model against the conventional crisp one while very fuzzy model may not be efficient. So, a plausible fuzziness degree can be found in a certain range. On the other hand, for *Strategy 2*, where k-anonymization is adopted to both entrance and exit images, the fuzzy model could achieve only comparative performances with the conventional one. Additionally, the strategy is available only in the cases of low anonymity levels. Therefore, *Strategy 1* seems to be more practical approach in real applications.

Future work includes application to much more realistic situations with larger scale data sets or other face feature values such as Fisher faces [15] and Laplacian faces [16].

Acknowledgment. This work was partially supported by the Okawa Foundation for Information and Telecommunications, Japan, under Research Grant 2014 and the Ministry of Education, Culture, Sports, Science and Technology, Japan, under Grant-in-Aid for Scientific Research (#26330281).

REFERENCES

[1] C. C. Aggarwal and P. S. Yu, *Privacy-Preserving Data Mining: Models and Algorithms*, Springer-Verlag, New York, 2008.

[2] P. Samarati, Protecting respondents' identities in microdata release, *IEEE Trans. Knowledge and Data Engineering*, vol.13, no.6, pp.1010-1027, 2001.

[3] L. Sweeney, k-anonymity: A model for protecting privacy, *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol.10, no.5, pp.557-570, 2002.

[4] J. W. Byun, A. Kamra, E. Bertino and N. Li, Efficient k-anonymization using clustering techniques, *International Conference on Database Systems for Advanced Applications, LNCS*, vol.4443, pp.188-200, 2007.

[5] K. Honda, A. Kawano, A. Notsu and H. Ichihashi, A fuzzy variant of k-member clustering for collaborative filtering with data anonymization, *Proc. of IEEE Int'l Conf. Fuzzy Systems*, pp.121-126, 2012.

[6] J. C. Bezdek, *Pattern Recognition with Fuzzy Objective Function Algorithms*, Plenum Press, 1981.

[7] K. Honda, M. Omori, S. Ubukata and A. Notsu, A privacy-preserving crowd movement analysis by k-member clustering of face images, *Proc. of the 4th International Conference on Informatics, Electronics & Vision*, #77, pp.1-5, 2015.

[8] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk and T. Toft, Privacy-preserving face recognition, *Privacy Enhancing Technologies, LNCS*, vol.5672, pp.235-253, 2009.

[9] T. Hornyak, Osaka train station set for large face-recognition study, *PC World*, http://www.pcworld.com/article/2094660/osaka-train-station-set-for-large-facerecognition-study.html, 2014.
[10] A. Kawano, K. Honda, A. Notsu and H. Ichihashi, Performance comparison of collaborative filtering with k-anonymized data by fuzzy k-member clustering, *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol.18, no.2, pp.239-245, 2014.
[11] National Institute of Information and Communications Technology (NICT), *Social Study on ICT in Multipurpose Complex in Osaka Station City*, http://www.nict.go.jp/press/2013/11/25-1.html, 2013 (in Japanese).
[12] M. A. Turk and A. P. Pentland, Face recognition using eigenfaces, *Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp.586-591, 1991.
[13] C. Zhang and Z. Zhang, A survey of recent advances in face detection, *Microsoft Research Technical Report*, MSR-TR-2010-66, 2010.
[14] *Face Recognition Data*, University of Essex, UK, The Data Archive, http://cswww.essex.ac.uk/mv/allfaces/index.html.
[15] P. Belhumeur, J. Hespanda and D. Kriegman, Eigenfaces vs. fisherfaces: Recognition using class specific linear projection, *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol.19, no.7, pp.711-720, 1997.
[16] X. He, S. Yan, Y. Hu, P. Niyogi and H. Zhang, Face recognition using Laplacianfaces, *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol.27, no.3, pp.328-340, 2005.