Differential Privacy and Machine Learning: a Survey and Review

Xinkui Wu
School of Electronic Information and Communications,
Huazhong University of Science and Technology, Wuhan, China
Email: wxk96@qq.com

(2018 年 7 月 22 日)

I. Differentially Private Unsupervised Learning

A. K-means clustering

K-means clustering is widely used in many applications such as classification and feature learning. It aims to cluster proximate data together.

The first differentially private K-means clustering algorithm was proposed by Blum et al. [1] as SuLQ K-means. Observe that only two queries are required explicitly: 1) the number of points in each new cluster and 2) the sum of the data points for each cluster to compute the centroid.

Privacy definitions provide ways for trading-off the privacy of individuals in a statistical database for the utility of downstream analysis of the data. In [2], they present Blowfish, a class of privacy definitions inspired by the Pufferfish framework as a substantial generalization of differential privacy, that provides a rich interface for this trade-off. They use the SuLQ K-means mechanism with the appropriate policy specific sensitivity and thus satisfy privacy under the Blowfish policy while ensuring better accuracy. That's to say, using the example of K-means clustering illustrate the gains in accuracy for Blowfish policies having weaker sensitive information specifications.

In [3], they proposes an (ϵ,δ)-differentially private K-means clustering algorithm using the sample and aggregate framework. The mechanism is based on the assumption that the data are well-separated. 'Well separated' means that the clusters can be estimated easily with a small number of samples. This is a prerequisite of the sample and aggregate framework. The mechanism randomly splits the training set into many subsets, runs the non-private k-means algorithm on each subset to get many outputs, and then uses the smooth sensitivity framework to publish the output from a dense region differentially privately. This step preserves privacy while the underlying k-means algorithm is unchanged.

In recent years, a large and growing body of literature has investigated differentially private data analysis. Broadly, they can be classified into two approaches. The interactive approach aims at developing customized differentially private algorithms for specific data mining tasks. The non-interactive approach aims at developing an approach to compute, in a differentially private way, a synopsis of the input dataset, which can then be used to generate a synthetic dataset, or to directly support various data mining tasks.

In [4]，they propose to combine the non-interactive differentially private synopsis algorithms with K-means clustering. They introduce a hybrid approach to differentially private data analysis, which is efficient approach to K-means clustering that further improves these cluster centroids.

In [5], they introduce GUPT, a platform that allows organizations to allow external aggregate analysis on their datasets while ensuring that data analysis is performed in a differentially private manner. They show using results from running common machine learning algorithms such as K-means clustering that GUPT does not significantly affect the accuracy of data analysis. When performing K-means clustering on the same dataset and the same iteration, the data accuracy of GUPT is higer than the other differential privacy system(PINQ).

Trajectory data, i.e., human mobility traces, is extremely valuable for a wide range of mobile applications. However, publishing raw trajectories without special sanitization poses serious threats to individual privacy. Recently, researchers begin to leverage differential privacy to solve this challenge.

In [6], they aim to remove the assumption that the trajectories contain a lot of identical prefixes or n-grams, which is not true in many applications and propose a differentially private publishing mechanism for more general time-series trajectories. In this paper, they use classic K-means clustering to partition the original trajectories into m group based on their pairwise Euclidean distances to significantly improve the efficiency. The partition approach the optimum since K-means prefers to grouping closer trajectories. Meanwhile, adding or removing a single trajectory cannot significantly change the partition result.

Models of human mobility have broad applicability in urban planning, ecology, epidemiology, and other fields. Starting with Call Detail Records (CDRs) from a cellular telephone network that have gone through a straightforward anonymization procedure, the prior WHERE modeling approach produces synthetic CDRs for a synthetic population. The accuracy of WHERE has been validated against billions of location samples for hundreds of thousands of cell phones in the New York and Los Angeles metropolitan areas. In [7], they introduce DPWHERE, which modifies WHERE by adding controlled noise to achieve differential privacy and use differentially private K-means clustering to cluster datas of phone users. [8] is a similar paper to protect the information of human trajectories data using differentially private K-means clustering.

From what has been discussed above, K-means clustering algorithm is fast and simple to realize. The time complexity is close to linear and is suitable for mining large data sets. However, in the K-means algorithm, K is given in advance, and the selection of K value is very difficult to estimate. Most of the time, it's best not to know in advance how many categories a given data set should fall into. Besides, in the K-means algorithm, an initial partition should be determined according to the initial clustering center, and then the initial partition should be optimized. The selection of the initial clustering center has a great influence on the clustering results. Once the initial value selection is poor, the effective clustering results may not be obtained. What can be seen from the K-means algorithm framework is that the algorithm needs to constantly adjust sample classification and calculated the adjusted new clustering center, so when is a large amount of data, the algorithm of time overhead is very large.

B. DBSCAN(Density-Based Spatial Clustering of Applications with Noise)

DBSCAN (Density-Based Spatial Clustering of Applications with Noise), introduced by Ester et al., is a non-parametric, densitybased clustering technique. Along with partitioning methods and hierarchical clustering, DBSCAN belongs to the third category of clustering methods and assumes that a cluster is a region in the data space with a high density.

One main concern for individuals participating in the data collection of personal location history records (i.e., trajectories) is the disclosure of their location and related information when a user queries for statistical or pattern mining results such as frequent locations derived from these records.

In [9], they investigate how one can achieve the privacy goal that the inclusion of his location history in a statistical database with interesting location mining capability does not substantially increase risk to his privacy. They use a standard spatial decomposition such as a quadtree, with DBSCAN clustering to achieve both tree-based density-based spatial objects clustering and to demonstrate the differential privacy mechanism on a tree-based location mining approach. The DBSCAN density-based clustering algorithm is used to extract the likely interesting regions.

Another approach to apply differential privacy to location privacy is differentially private data mining inside the traces as proposed in [10]. They introduce a way to build a quad-tree and use it to perform a DBSCAN clustering whose result is differentially private. Like in classical differential privacy, the goal here is to protect the result of an aggregate function and not to access directly to the whole data set.

Differential privacy is a new paradigm of privacy tailored for statistical databases independent of the adversaries' background knowledge or computational power, which definnes a rigorous attack model, reducing the risk of privacy disclosure and meanwhile ensuring the availability of data successfully.

Based on differential privacy and data mining techniques, many algorithms have been presented, such as Differential Privacy Preservation K-means clustering method (DP-Kmeans), Differential Privacy Preservation DBSCAN clustering method (DP-DBSCAN)[11], etc. These algorithms can achieve effective clustering via adding noise that conforms to differential privacy. However, when DP-Kmeans faces a dataset with an unknown number of clusters and uneven density distribution, the clustering effect decreases. DP-DBSCAN is more time-consuming with less clustering for larger datasets and smaller privacy budget parameters.

In [12], they put forward a differential privacy preservation multiple cores DBSCAN clustering(DP-MCDBSCAN) schema based on the powerful differential privacy and DBSCAN algorithm for network user data to effectively leverage the privacy leakage issue in the process of data mining, enhancing data clustering efficaciously by adding Laplace noise. Privacy analysis demonstrates that their DP-MCDBSCAN clustering schema can not only meet the publishers' query needs but also prevent the data of publishers from being attacked. Different from DP-DBSCAN, DP-MCDBSCAN solves the randomness and blindness of DP-DBSCAN effectively by optimizing the selection of the initial core points.

Compared with the K-means method, DBSCAN does not need to know the number of cluster classes to be formed in advance and can find clusters of any shape. At the same time, DBSCAN can identify noise points. DBSCAN is not sensitive to the order of samples in the database, that is, the input order of pattern has little effect on the result. However, for the sample at the boundary between cluster classes, it may fluctuate according to which cluster class is detected first and whose attribution. Besides，DBSCAN does not reflect high dimensional data well and if the density of the sample set is not uniform and the cluster spacing difference is large, the cluster quality is poor.

C. Hierarchical Clustering

In order to avoid the problem of K value selection and initial clustering center selection in K-means clustering method, the hierarchical clustering is a kind of clustering that can be divided into large clusters from top to bottom which is called division method. It can also aggregate small categories from bottom to top, which is called condensation method. However, the most commonly used method is the condensation method from the bottom up.

In [13]，it mentions that cluster analysis is the process of grouping a set of data objects into multiple groups or clusters so that objects within a cluster have high similarity, but are very dissimilar to objects in other clusters. Dissimilarities and similarities are assessed based on the attribute values describing the objects and often involve distance measures. Similar to the K-means clustering method, the hierarchical clustering method also can be applied to differential privacy data protection and it doesn't need select k value and initial clustering center.

The integration of information dispersed among multiple repositories is a crucial step for accurate data analysis in various domains. In support of this goal, it is critical to devise procedures for identifying similar records across distinct data sources. In [14], they introduce a novel model for practical private record linkage (PRL), which 1) affords controlled and limited information leakage, 2) avoids false matches resulting from data transformation. Besides, applied obfuscation relies on differential privacy which provides strong privacy guarantees against adversaries with arbitrary background knowledge. Once the partitioning identifier is selected, the third party Charlie who helps the execution of the protocol without learning any record from either A or B applies agglomerative hierarchical clustering on the set of values in the public domain of the partitioning identifier. Partitioning the data sources into blocks is to eliminate comparisons for records that are unlikely to match. During blocking, Charlie forms the global block basis through a hierarchical clustering over the domain of the selected public identifier. The hierarchical clustering can make blocking performed efficiently without significant computational cost.

Database as a service (DAS) model where data management is outsourced to cloud service providers has become more prevalent. Although DAS model offers lower cost and flexibility, it necessitates the transfer of potentially sensitive data to untrusted cloud servers.

In [15], they introduce a novel construction for practical and privacy-aware selective record retrieval over encrypted databases. Their approach leaks obfuscated access pattern to enable efficient retrieval while ensuring individual privacy. Applied obfuscation is based on differential privacy which provides rigorous individual privacy guarantees against adversaries with arbitrary background knowledge. To reduce overall obfuscation cost by distributing initial query interfaces among distinct replicas is an instance of a clustering problem. Their replication strategy is based on a common clustering technique, known as agglomerative hierarchical clustering. Initially, a distinct cluster is formed for each query interface.After initial construction, clusters are successively combined until no improvement is achieved on the obfuscation cost. Once final query interfaces and associated replicas are identified, private indexes are formed on them.

Hierarchical clustering is often portrayed as the better quality clustering approach, but is limited because of its quadratic time complexity. In contrast, K-means and its variants have a time complexity that is linear in the number of documents, but are thought to produce inferior clusters. That's to say, K-means is used because of its run-time efficiency and agglomerative hierarchical clustering is used because of its quality.

II. Differentially Private Dimensionality Reduction

A. Feature Selection

So-called dimension disaster is when the feature dimension exceeds a certain limit, the performance of the classifier with the increase of feature dimension is worse instead. The higher the dimension, the greater the time cost of training model. What leads to the decrease the perfomance of the classifier is often because the cause of the high dimension features contain irrelevant and redundant features, so the main purpose of the feature selection is to remove features of irrelevant and redundant features.

Irrelevant feature refers to the feature that is irrelevant to the current learning task (the information provided by this feature is useless for the current learning task). For the student achievement, the student number is irrelevant feature. Redundant feature refers to the characteristics of the information contained in can marked out from other aspects, such as for the characteristics of ”area”, can from ”long” and ”wide”, then it is redundant feature.

In [16], they propose an ϵ-differentially private feature selection, PrivateKD, for classification. PrivateKD is based on the assumption that all features are categorical and each feature has finite possible values. For any set of features S, it defines a function $F(S)$ which tells how many pairs of samples from different classes can features in S distinguish. The set of selected features S' is initialized to Φ. Then a greedy algorithm adds new features one by one to S'. When selecting a feature to add, the algorithm uses the exponential mechanism to select the feature that can lead to the largest increase of $F(S')$. The paper provides a utility guarantee for the special case where the cardinality of sample space m and the number of features d have the relation $m = d - 1$. In that case, except probability $O(1/poly(m))$ ($poly(m)$ means a polynomial expression of m), $F(S') \geqslant (1 - 1/e) * F(Soptimal) - O(logm/\epsilon)$.

The privacy-preserving data analysis has been gained significant interest across several research communities. The current researches mainly focus on privacy-preserving classification and regression. However, feature selection is also an essential component for data analysis, which can be used to reduce the data dimensionality and can be utilized to discover knowledge, such as inherent variables in data. In [17], in order to efficiently mine sensitive data, a privacy preserving feature selection algorithm is proposed and analyzed in theory based on local learning and differential privacy.

Within exiting privacy models, differential privacy is considered one of the strongest privacy protection techniques that does not make any assumption about the attacker's background knowledge. This approach, however, is not suitable for high-dimensional data with large domains as the added noise substantially destroys the utility of the data.

There are two broad categories of feature selection techniques, namely, filters and wrappers. Filter approach attempts to assess the merits of features from the data without considering the induction algorithm. The wrapper model, on the other hand, uses a target learning algorithm in order to estimate the worth of attribute subsets.

In [18], they propose the TOP-Diff algorithm which offers a trade-off between anonymization level K and the privacy budget ϵ, and enables us to publish privacy preserving datasets with high utility. They propose a novel technique for privacy preserving data publishing satisfying differential privacy and use feature selection in order to minimize the negative impact of injecting noise into the contingency table. They propose the TOP-Diff algorithm which incorporates the ultimate usage of the data and employs feature selection in order to achieve a differentially private dataset on K-anonymous dataset, thus maintaining high utility for further data analysis according to a given task.

In [19], they focus on filter methods so that an analyst does not need to know the internals of the private classifier. Filters compute a ranking or a score for features based on their correlation with their label. Filter methods may rank/score individual features or sets of features. They focus on methods that score individual features. Features can be selected by choosing the top values or those above some threshold. They show that private feature selection indeed leads to significant improvement in the classifiers prediction accuracy with two differentially private classifiers (Naive Bayes and logistic regression)

In [20], they propose an (ϵ, δ)-differentially private algorithm for feature selection when the target function is stable. Unlike the previous paper, this paper doesn't explicitly state the algorithm for feature selection. Instead, it only requires the selection algorithm to be stable. By 'stable', it means that either the value of function as calculated on the input dataset doesn't change when some samples in the set change, or that the function can output the same result on a random subset from the input dataset with high probability.

In conclusion, feature selection brings the immediate effects of speeding up a machine learning or data mining algorithm, improving learning accuracy, and enhancing model comprehensibility. Various studies show that features can be removed without performance deterioration. Moreover, feature selection also leads to better data visualization, reduction of measurement and storage requirements.

B. Principal Component Analysis

Principal Component Analysis (PCA) is a popular method in dimension reduction. It finds k orthogonal directions on which the projections of data have largest variance. The original data can then be represented by its projection onto those k directions. Usually k is much smaller than the dimension of sample space. Thus the projection greatly reduces the dimensionality of the data. It is well-known that this analysis is closely related to eigen-decomposition: if we rank the eigenvectors of matrix $A = Var[X]$ according to the corresponding eigenvalues $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_p$, then the first k eigenvectors are the k directions.

The extant privacy-preserving PCA algorithms have been devised based on two major features: the notion of differential privacy and the stage of randomization.

The notion of differential privacy has two types: (ϵ, 0)-DP (also called pure DP) and (ϵ, δ)-DP (also called approximate DP). (ϵ, δ)-DP is a weaker version of (ϵ, 0)-DP as the former allows the privacy guarantee to be broken with tiny probability (more precisely, δ). In the seminal work on privacypreserving PCA (Dwork et al. 2014; Hardt and Roth 2012; 2013; Hardt and Price 2014; Blum et al. 2005), the authors used the notion of (ϵ, δ)-DP. In contrast, there is only a few work (Chaudhuri, Sarwate, and Sinha 2012; Kapralov and Talwar 2013), which is based on (ϵ, 0)-DP.

In terms of the stage of randomization, there are two mainstream classes of approaches. The first is randomly computing the eigenspace (Hardt and Roth 2013; Hardt and Price 2014; Chaudhuri, Sarwate, and Sinha 2012; Kapralov and Talwar 2013). The noise is added in the computing procedure. An alternative way is directly adding noise to the covariance matrix. Then one runs the non-private eigenspace computing algorithm to produce the output. This class of approaches is called input perturbation. The input perturbation algorithms publish a noisy sample covariance matrix before computing the eigenspace. Thus, any further operation on the noisy covariance matrix does not violate privacy guarantee. So far as the flexibility is concerned, the input perturbation has better performance because it is not limited only to computing eigenspace. Besides, the input perturbation approach is efficient because it merely takes extra efforts on generating the noise.

In [21], they propose a new input perturbation mechanism for publishing a covariance matrix to achieve (ϵ, 0)- differential privacy. Their mechanism uses a Wishart distribution to generate matrix noise. In particular, they apply this mechanism to principal component analysis. Besides, they show that the Wishart mechanism is effective input perturbation approach for (ϵ, 0)-differentially private PCA. PCA reduces the data dimension while keeping the optimal variance. More specifically, it finds a projection matrix by computing a low rank approximation to the sample covariance matrix of the given data points. In the scenario of PCA, their Wishart mechanism adds less noise than the Laplace, which leads to better utility guarantee. Compared with the privacy-preserving PCA algorithm in (Chaudhuri, Sarwate, and Sinha 2012), their mechanism has reliable rank-k utility guarantee while the former (Chaudhuri, Sarwate, and Sinha 2012) only has rank-1.

There are two differentially private mechanisms to select eigenvectors iteratively. The iterative methods are based on the spectral decomposition, which ensures that if the components corresponding to the first $i - 1$ eigenvectors of A are subtracted from A, then the i-th largest eigenvector becomes the largest eigenvector of what remains. Therefore the process of selecting the largest k eigenvectors can be replaced by repeatedly finding the first eigenvector and removing the component corresponding to the selected eigenvector. The following two mechanisms both make use of this idea but differ on how to select the first eigenvector.

An (ϵ, δ)-differentially private mechanism is proposed in [22]. The mechanism uses the power method: $A^n v \;/\; ||A^n v||$ converges to the first eigenvector of A if v is not orthogonal to the first eigenvector. It randomly starts with a unitlength vector v, then iteratively updates v with $(A_v{+}\eta_i) \;/\; ||(A_v{+}\eta_i)||$ while η_i is Gaussian noise in the i-th iteration. Since it is exceedingly improbable that a random vector is orthogonal to the first eigenvector, the vector v will get close to the first eigenvector. However due to the noise, v cannot converge with arbitrary accuracy. Thus it outputs v after a fixed number of iterations and proceed to find the next largest eigenvector. A utility guarantee is provided on the power method, which outputs the first eigenvector. However there is no direct guarantee on the k eigenvectors. For each eigenvector a output by running the power method on matrix A, the distance from the first eigenvector ($||A_a|| \;/\; ||a|| - \lambda_1$ while λ_1 is the first eigenvalue) is $O\left(\left(\sqrt{log\left(1/\delta\right)logn}\right)/\epsilon\right)$

[23] provides an ϵ-differentially private mechanism for principal component analysis. According to the property that the first eigenvector v of A is the unitlength vector that maximizes $v^T Av$, the mechanism uses $H(X,v) = v^T Av$ as the score function in the exponential mechanism to select the first eigenvector from the set $\left\{v : v^T v = 1\right\}$ differentially privately. The selection algorithm is specially designed to be computable in reasonable time. This paper also provides two proofs on utility of this mechanism. For any $0{<}\delta{<}1$ and privacy budget ϵ, if the first eigenvalue of matrix A, $\lambda_1 > O\left(ln\left(1/\delta\right)/\left(n\epsilon\delta\right)\right)$, then the first eigenvector v has the property $E\left[v^T Av\right] \geq \left(1-\delta\right)\lambda_1$. For any $0{<}\delta{<}1$ and privacy budget ϵ, if the first eigenvalue $\lambda_1 > O\left(1/\left(n\epsilon\delta^6\right)\right)$, the $k+1$-th eigenvalue is denoted λ_{k+1}, and the k-rank approximation matrix output is denoted A_k, then the largest eigenvalue of $A - A_k$ is smaller than $\lambda_{k+1} + \delta\lambda_1$ with large probability.

Often, the training of models requires large, representative datasets, which may be crowdsourced and contain sensitive information. The models should not expose private information in these datasets. In [24], they develop new algorithmic techniques for learning and a refined analysis of privacy costs within the framework of differential privacy. PCA is a useful method for capturing the main features of the input data. They implement the differentially private PCA algorithm. They incur a privacy cost due to running a PCA. However, they find it useful for both improving the model quality and for reducing the training time, as suggested by their experiments on the MNIST data. Accuracy is quite stable over a large range of choices for the projection dimensions and the noise level used in the PCA stage.

In [25], they investigate the theory and empirical performance of differentially private approximations to PCA and propose a new method which explicitly optimizes the utility of the output. The PCA algorithm is very sensitive in this sense because the top eigenvector can change by 90 degree by changing one point in the data set. They assume that the algorithm is given n data points and a target dimension k and must produce a k-dimensional subspace that approximates that produced by the standard PCA problem. They propose a new algorithm, PPCA, which is an instance of the exponential mechanism of McSherry and Talwar. PPCA explicitly takes into account the quality of approximation that outputs a k-dimensional subspace which is biased towards subspaces close to the output of PCA. By combining results on the exponential mechanism along with properties of PCA algorithm, they can show that this procedure is differentially private. They propose the algorithm, PPCA, which is an instance of the exponential mechanism and show that PPCA is nearly optimal.

In [26], they consider the problem of privately releasing a low dimensional approximation to a set of data records, represented as a matrix A in which each row corresponds to an individual and each column to an attribute. Their goal is to compute a subspace that captures the covariance of A as much as possible, classically known as principal component analysis (PCA). They assume that each row of A has L_2 norm bounded by one, and the privacy guarantee is defined with respect to addition or removal of any single row. They show that the well-known, but misnamed, randomized response algorithm, with properly tuned parameters, provides nearly optimal additive quality gap compared to the best possible singular subspace of A. They further show that when A^TA has a large eigenvalue gap – a reason often cited for PCA - the quality improves significantly. In practice, allowing such ”overpowering” individuals often goes against the purpose of PCA for discovering the global structure of many data records, and row normalization is often recommended before applying PCA.

Principal component analysis is the simplest method to analyze multivariate statistical distribution by eigenvalue. The result can be interpreted as an explanation of the variance in the original data, which direction of data value has the greatest influence on the other side difference. In other words, PCA provides an effective way to reduce data dimensions. If the analyst removes the components corresponding to the smallest eigenvalues from the original data, the resulting low-dimensional data must be optimized.

Except principal component analysis (PCA), linear discriminant analysis (LDA) is widely used as the representative feature projection technique. PCA is for unsupervised learning and LDA is for classification. PCA is an orthonormal transformation of data to a low-dimensional space such that maximum variance of the original data is preserved. PCA works well for a lot of data analysis problems but does not fit well for classification purposes. LDA and other supervised feature selection techniques are better positioned for classification in that they reduce the input features in such a way that maximum separability between target classes is preserved.

A reasonable compromise of privacy and utility exists at an ”appropriate” resolution of the data. In [27], they proposed novel mechanisms to achieve privacy preserving data publishing (PPDP) satisfying ϵ-differential privacy with improved utility through component analysis. The mechanisms studied in this article are Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). The differential PCA-based PPDP serves as a general-purpose data dissemination tool that guarantees better utility (i.e., smaller error) compared to Laplacian and Exponential mechanisms using the same ”privacy budget”. Their second mechanism, the differential LDA-based PPDP, favors data dissemination for classification purposes.

C. Singular Value Decomposition

PCA is the solution to the eigenvector of the covariance matrix, which happens to be the representation of the covariance. The eigenvector solution is the process of Singular Value Decomposition(SVD), and the column vectors of the decomposed matrix correspond to the eigenvectors. So the solution of the covariance of PCA becomes the sample matrix of SVD.

In the setting of large data analysis, one of the desired goals is to design a sub-linear space algorithm to perform computation while receiving the data online. There are many non-private algorithms in this setting. Such algorithms are called online algorithms or streaming algorithms.

The focus of [28] is on differential privacy of streaming data using sketch-based algorithms. They work in the well studied streaming model of computation, where the database is stored in the form of a matrix and a curator can access the database row-wise or column-wise. It is common to perform a procedure that computes a full or partial singular value decomposition (SVD) of the covariance matrix corresponding to the input data matrix, and then appeal to standard statistical model selection criterion, like getting the top half of the spectrum of the matrix, to quantify its significance.

[29] proves that an ”old dog”, namely, the classical Johnson-Lindenstrauss transform, ”performs new tricks”, it gives a novel way of preserving differential privacy. They show that if taking two databases, D and D' , such that 1) $D - D'$ is a rank-1 matrix of bounded norm and 2) all singular values of D and D' are sufficiently large,

then multiplying either D or D' with a vector of iid normal Gaussians yields two statistically close distributions in the sense of differential privacy. Furthermore, a small, deterministic and public alteration of the input is enough to assert that all singular values of D are large. And SVD is used to solve transformation of matrix in order to decrease the dimensionality. Besides, throughout those papers[30][31][32], they use the singular value decomposition of a matrix, which is a classic tool of matrix analysis.

Low rank approximation is a fundamental computational primitive widely used in data analysis. In many applications the dataset that the algorithm operates on may contain sensitive information about contributing individuals (e.g. user/movie ratings in the Netflix challenge), motivating the need to design low rank approximation algorithms that preserve privacy of individual entries of the input matrix.

In [30], they give a polynomial time algorithm that, given a privacy parameter $\epsilon > 0$, for a symmetric matrix A, outputs an ϵ-differentially approximation to the principal eigenvector of A, and then show how this algorithm can be used to obtain a differentially private rank-k approximation. They give algorithms for releasing an ϵ-differentially private low-rank approximation to a symmetric matrix. Their algorithm for general k relies on an algorithm for outputting a differentially private vector most of whose mass is concentrated in the few most signifficant eigenvalues. They then use this primitive to iteratively subtract rank-1 approximations from the input matrix, obtaining an approximate differentially private SVD.

References

[1] A. Blum, C. Dwork, F. McSherry, and K. Nissim, “Practical privacy: the sulq framework,” in *Proceedings of the twenty-fourth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*. ACM, 2005, pp. 128–138. I-A

[2] X. He, A. Machanavajjhala, and B. Ding, “Blowfish privacy: Tuning privacy-utility trade-offs using policies,” in *Proceedings of the 2014 ACM SIGMOD international conference on Management of data*. ACM, 2014, pp. 1447–1458. I-A

[3] K. Nissim, S. Raskhodnikova, and A. Smith, “Smooth sensitivity and sampling in private data analysis,” in *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*. ACM, 2007, pp. 75–84. I-A

[4] D. Su, J. Cao, N. Li, E. Bertino, and H. Jin, “Differentially private k-means clustering,” in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*. ACM, 2016, pp. 26–37. I-A

[5] P. Mohan, A. Thakurta, E. Shi, D. Song, and D. Culler, “Gupt: privacy preserving data analysis made easy,” in *Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data*. ACM, 2012, pp. 349–360. I-A

[6] J. Hua, Y. Gao, and S. Zhong, “Differentially private publication of general time-serial trajectory data,” in *Computer Communications (INFOCOM), 2015 IEEE Conference on*. IEEE, 2015, pp. 549–557. I-A

[7] D. J. Mir, S. Isaacman, R. Cáceres, M. Martonosi, and R. N. Wright, “Dp-where: Differentially private modeling of human mobility,” in *Big Data, 2013 IEEE International Conference on*. IEEE, 2013, pp. 580–588. I-A

[8] P. Xiong, T. Zhu, W. Niu, and G. Li, “A differentially private algorithm for location data release,” *Knowledge and information systems*, vol. 47, no. 3, pp. 647–669, 2016. I-A

[9] S.-S. Ho and S. Ruan, “Preserving privacy for interesting location pattern mining from trajectory data,” 2013. I-B

[10] ——, “Differential privacy for location pattern mining,” in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*. ACM, 2011, pp. 17–24. I-B

[11] W.-m. Wu and H. Huang, “A dp-dbscan clustering algorithm based on differential privacy preserving,” *Computer Engineering & Science*, vol. 37, no. 4, pp. 830–834, 2015. I-B

[12] L. Ni, C. Li, H. Liu, A. G. Bourgeois, and J. Yu, “Differential private preservation multi-core dbscan clustering for network user data,” *Procedia Computer Science*, vol. 129, pp. 257–262, 2018. I-B

[13] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, “Information security in big data: privacy and data mining,” *IEEE Access*, vol. 2, pp. 1149–1176, 2014. I-C

[14] M. Kuzu, M. Kantarcioglu, A. Inan, E. Bertino, E. Durham, and B. Malin, “Efficient privacy-aware record integration,” in *Proceedings of the 16th International Conference on Extending Database Technology*. ACM, 2013, pp. 167–178. I-C

[15] M. Kuzu, M. S. Islam, and M. Kantarcioglu, “Efficient privacy-aware search over encrypted databases,” in *Proceedings of the 4th ACM conference on Data and application security and privacy*. ACM, 2014, pp. 249–256. I-C

[16] S. A. Vinterbo, “Differentially private projected histograms: Construction and use for prediction,” in *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*. Springer, 2012, pp. 19–34. II-A

[17] J. Yang and Y. Li, "Differentially private feature selection," in *Neural Networks (IJCNN), 2014 International Joint Conference on*. IEEE, 2014, pp. 4182–4189. II-A

[18] Y. Jafer, S. Matwin, and M. Sokolova, "Using feature selection to improve the utility of differentially private data publishing," *Procedia Computer Science*, vol. 37, pp. 511–516, 2014. II-A

[19] B. Stoddard, Y. Chen, and A. Machanavajjhala, "Differentially private algorithms for empirical machine learning," *arXiv preprint arXiv:1411.5428*, 2014. II-A

[20] J. Czerniak and H. Zarzycki, "Application of rough sets in the presumptive diagnosis of urinary system diseases," *Artificial Intelligence and Security in Computing Systems*, pp. 41–51, 2003. II-A

[21] W. Jiang, C. Xie, and Z. Zhang, "Wishart mechanism for differentially private principal components analysis." in *AAAI*, 2016, pp. 1730–1736. II-B

[22] M. Hardt and A. Roth, "Beyond worst-case analysis in private singular vector computation," in *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*. II-B

[23] M. Kapralov and K. Talwar, "On differentially private low rank approximation," in *Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete algorithms*. SIAM, 2013, pp. 1395–1414. II-B

[24] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 308–318. II-B

[25] K. Chaudhuri, A. D. Sarwate, and K. Sinha, "A near-optimal algorithm for differentially-private principal components," *The Journal of Machine Learning Research*, vol. 14, no. 1, pp. 2905–2943, 2013. II-B

[26] C. Dwork, K. Talwar, A. Thakurta, and L. Zhang, "Analyze gauss: optimal bounds for privacy-preserving principal component analysis," in *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*. ACM, 2014, pp. 11–20. II-B

[27] X. Jiang, Z. Ji, S. Wang, N. Mohammed, S. Cheng, and L. Ohno-Machado, "Differential-private data publishing through component analysis," *Transactions on Data Privacy*, vol. 6, no. 1, pp. 19–34, 2013. II-B

[28] J. Upadhyay, "Differentially private linear algebra in the streaming model," *arXiv preprint arXiv:1409.5414*, 2014. II-C

[29] J. Blocki, A. Blum, A. Datta, and O. Sheffet, "The johnson-lindenstrauss transform itself preserves differential privacy," in *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on*. IEEE, 2012, pp. 410–419. II-C

[30] M. Kapralov and K. Talwar, "On differentially private low rank approximation," in *Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete algorithms*. SIAM, 2013, pp. 1395–1414. II-C

[31] M. Hardt, K. Ligett, and F. McSherry, "A simple and practical algorithm for differentially private data release," in *Advances in Neural Information Processing Systems*, 2012, pp. 2339–2347. II-C

[32] C. Li and G. Miklau, "Optimal error of query sets under the differentially-private matrix mechanism," in *Proceedings of the 16th International Conference on Database Theory*. ACM, 2013, pp. 272–283. II-C