"Differentially Private Heatmaps", by Ghazi et al. (2022) [1]

Alexandre Ngau, Mathilde Kretz, Thomas Boudras

PSL Research University

May 17, 2024

Introduction

Article

"Differentially Private Heatmaps", by Ghazi et al. (2022) [1]

- **Problem:** In the field of Differential Privacy, creating meaningful data visualizations like heatmaps without compromising individual privacy poses a significant challenge.
- **Motivation:** With datasets becoming increasingly large and personal, the ability to draw conclusions without exposing individual data becomes essential.
- **Solution:** A novel algorithm for generating differentially private heatmaps that aggregate data with near-optimal error bounds (under certain assumptions), using the Earth Mover's Distance (EMD) metric, preserving privacy but also ensuring relevance and perceptual similarity of the generated heatmaps.

Literature Review

- **Foundational Contributions:** Differential privacy's foundational work by Dwork et al. (2006) [2; 3] sets the stage for its application in high-stakes scenarios like the 2022 US Census [4].
- **Challenges in Data Visualization:** Applying DP to data visualization introduces challenges in balancing data utility and privacy, with the impact of various factors including the noise addition algorithm and privacy the level ϵ on visual utility [5; 6].
- **Preliminary Approaches to Privacy-preserving Heatmaps:** Zhang et al. (2016) [7] are the first to suggest a privacy-preserving heatmap-generating algorithm for user location data.
- **Gap in Methodology for Optimizing Visual Fidelity:** Bagdasaryan et al. (2022) [8] addresses the private heatmaps problem but without formal utility guarantees or generality, while our paper [1] proposes a method optimizing for Earth Mover's Distance (EMD), advancing both privacy and utility in heatmap visualization.

The Paper's Main Results I

Experimental Context

- Consider a heatmap composed of various points.
- At each point, there is p_i, the likelihood of a user being present there
- Calculate the probability of a user being at a specific point, denoted by $a := \frac{1}{n} \sum_{i=1}^{n} p_i$

Goal Find a method to estimate a, the error of which will be calculated using the EMD (Earth Mover's Distance).

The Paper's Main Results II

Definition (Earth Mover's Distance (EMD))

Given two non-negative vectors $\mathbf{p}, \mathbf{q} \in \mathbb{R}_{\geq 0}^{G_\Delta}$ such that $\|\mathbf{p}\|_1 = \|\mathbf{q}\|_1$, their *Earth Mover's Distance* (EMD) is

$$EMD(\mathbf{p}, \mathbf{q}) := \min_{\gamma} \sum_{x \in G_\Delta} \sum_{y \in G_\Delta} \gamma(x, y) \cdot \|x - y\|_1,$$

where G_Δ be the set of grid points $(\Delta \times \Delta)$ in $[0, 1)^2$ and the minimum relates to $\gamma \in \mathbb{R}_{\geq 0}^{G_\Delta \times G_\Delta}$ whose marginals are $\mathbf{p}$ and $\mathbf{q}$.

The Paper's Main Results III

Sparisty Assumption

- A key feature often found in distributions used for aggregations is "sparsity".
- Our approximation guarantee depends on the best k-sparse [a] distribution that closely approximates $a = \frac{1}{n}\sum_{i=1}^{n} p_i$ using EMD.

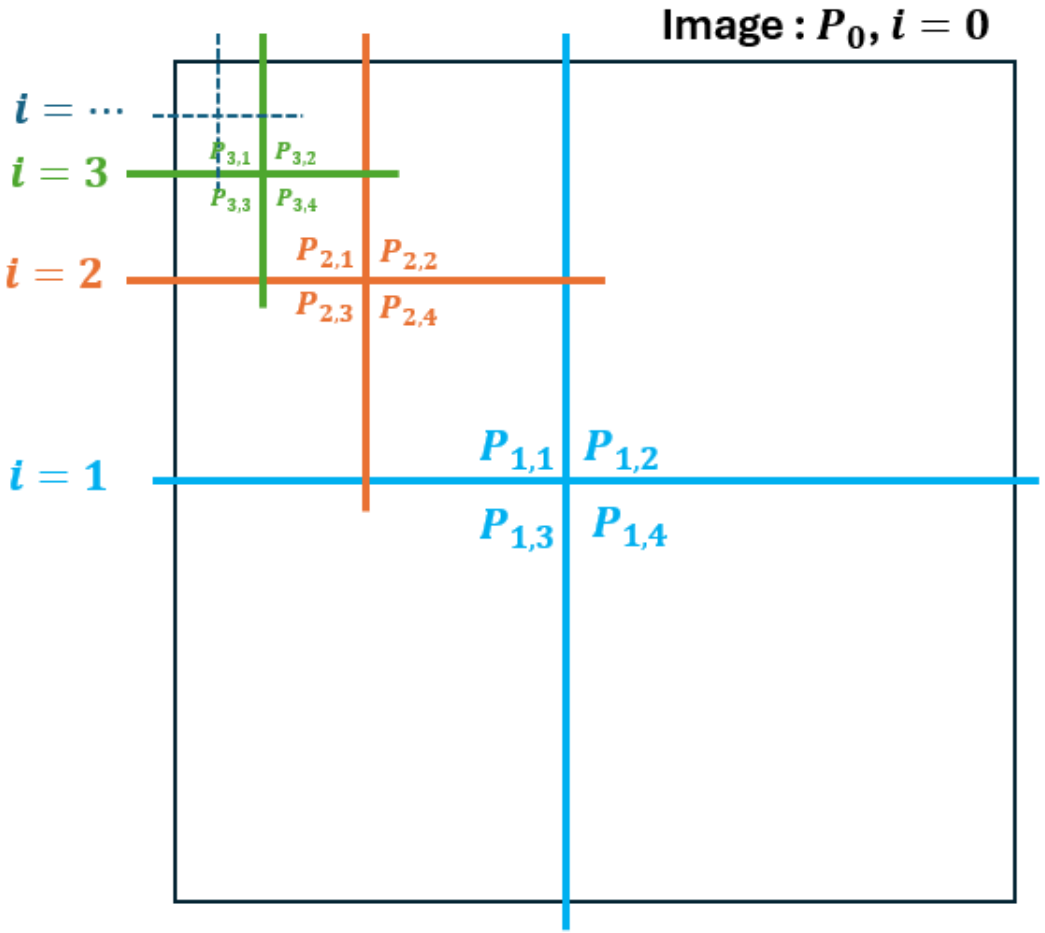
[a] **Def.** A distribution is k-sparse if it is non-zero on at most k points.

Theorem

There exists an ε-differentially private (ε-DP) algorithm that, for any constant $\lambda \in (0,1)$, can output a $(\lambda, O_\varepsilon(\sqrt{k}/n))$-approximation [a] for sparse Earth Mover's Distance (EMD) aggregation with probability at least 0.99.

[a] an output distribution $\hat{\mathbf{a}}$ is a (λ, κ)-*approximation* for sparse EMD aggregation if : $\text{EMD}(\hat{\mathbf{a}}, \mathbf{a}) \leq \lambda \cdot \min_{k\text{-sparse } \mathbf{a}'} (\mathbf{a}', \mathbf{a}) + \kappa$

The Paper's Main Results IV



The Paper's Main Results V

Algorithm 1 DPSparseEMDAgg

Input: distributions $\mathbf{p}_1, \ldots, \mathbf{p}_n$ on G_Δ
Parameters: $\epsilon_1, \ldots, \epsilon_\ell > 0, w \in \mathbb{N}$
$\mathbf{s} \leftarrow \sum_{i=1}^{n} \mathbf{p}_i$
for $i = 0, \ldots, \ell$ **do**
    $\nu_i \leftarrow \mathrm{Lap}(1/\epsilon_i)^{\otimes m_i}$
    $\mathbf{y}'_i \leftarrow \frac{1}{2^i} (\mathbf{P}_i \mathbf{s} + \nu_i)$
end for
$\mathbf{y}' \leftarrow [\mathbf{y}'_0 \cdots \mathbf{y}'_\ell]$
$\hat{\mathbf{s}} \leftarrow \textsc{Reconstruct}(\mathbf{y}'; w)$
return $\hat{\mathbf{a}} := \hat{\mathbf{s}} / \|\hat{\mathbf{s}}\|_1$

The Paper's Main Results VI

Algorithm 2 RECONSTRUCT

Input: noisy measurements $\mathbf{y}' \in \mathbb{R}^{\bigcup_{i\in[\ell]} C_{2^i}}$
Parameters: $w \in \mathbb{N}$
$S_0 \leftarrow C_1$
for $i = 1, \ldots, \ell$ **do**
    $T_i \leftarrow \text{children}(S_{i-1})$
    $S_i \leftarrow$ the set of $\min\{w, |T_i|\}$ coordinates in T_i with maximum values in $\mathbf{y}'$
end for
$S \leftarrow \bigcup_{i\in[\ell]} S_i$ and $\hat{\mathbf{y}} \leftarrow \mathbf{y}'|_S$
return $\hat{\mathbf{s}} \leftarrow \arg\min_{\mathbf{s}'\geq\mathbf{0}} \|\hat{\mathbf{y}} - \mathbf{P}\mathbf{s}'\|_1$

Experiment Replication I

Paper Dataset

The GOWALLA [a] dataset (by [9]) consists of geolocations (or geographical check-ins) of the users from the location-based social networking website Gowalla, over the period of February 2009 to October 2010.

[a] `http://snap.stanford.edu/data/loc-Gowalla.html`

Paper Results Reproduction

Heatmaps generated for $l = 4$ (16×16 grid) and for $n = 200$ (number of users).

Experiment Replication II

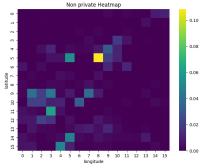


Figure 1: Non-private heatmap

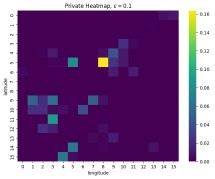


Figure 2: Private heatmap for $\epsilon = 0.1$

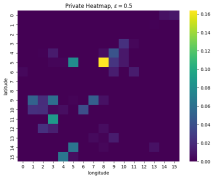


Figure 3: Private heatmap for $\epsilon = 0.5$

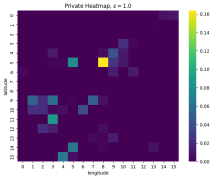


Figure 4: Private heatmap for $\epsilon = 1$

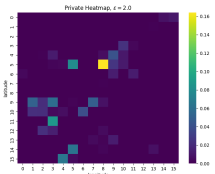


Figure 5: Private heatmap for $\epsilon = 2$

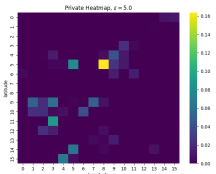


Figure 6: Private heatmap for $\epsilon = 5$

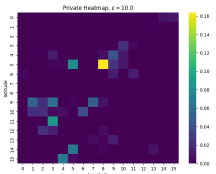


Figure 7: Private heatmap for $\epsilon = 10$

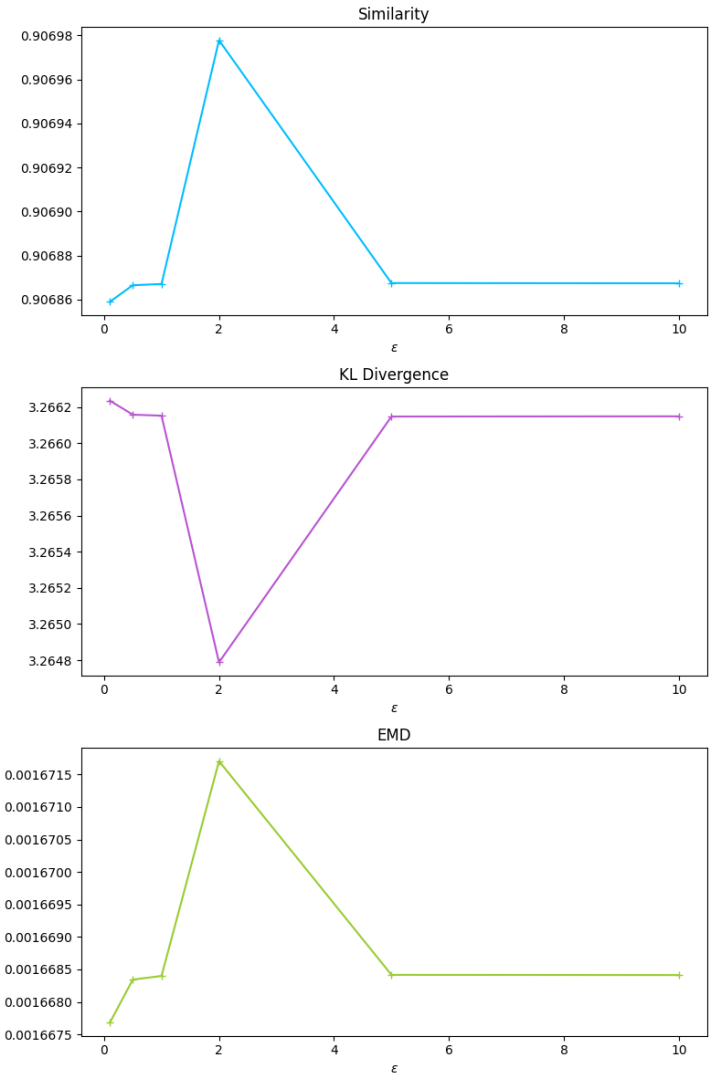


Figure 8: Metrics when varying ϵ

Experiment Replication III

New Dataset

The *COVID 19 Cases US* [a] dataset by [10], represents the evolution of the COVID-19 Cases in the US during the pandemic from March 21^{st}, 2020 to March 10^{th}, 2023. To emulate the users, we decided to count each individual `county` having records in the dataset as an individual user (there are exactly 1795), and to use the number of deaths on the whole period as the number of check-ins per user (per county in this case). Although it was not the case for the COVID-19 pandemic, we can easily imagine other contexts in which such numbers might need to remain private.

[a] `https://prep-response-portal.napsgfoundation.org/datasets/628578697fb24d8ea4c32fa0c5ae1843_0/about`

New Dataset Results

Heatmaps generated for $l = 4$ (16×16 grid) and for $n = 1795$ (number of users).

Experiment Replication IV

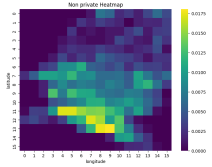


Figure 9: Non-private heatmap

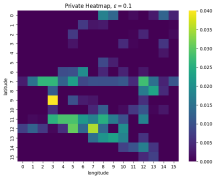


Figure 10: Private heatmap for $\epsilon = 0.1$

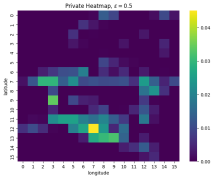


Figure 11: Private heatmap for $\epsilon = 0.5$

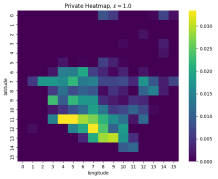


Figure 12: Private heatmap for $\epsilon = 1$

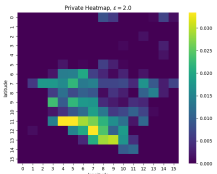


Figure 13: Private heatmap for $\epsilon = 2$

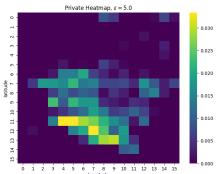


Figure 14: Private heatmap for $\epsilon = 5$

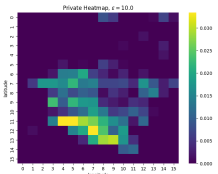


Figure 15: Private heatmap for $\epsilon = 10$

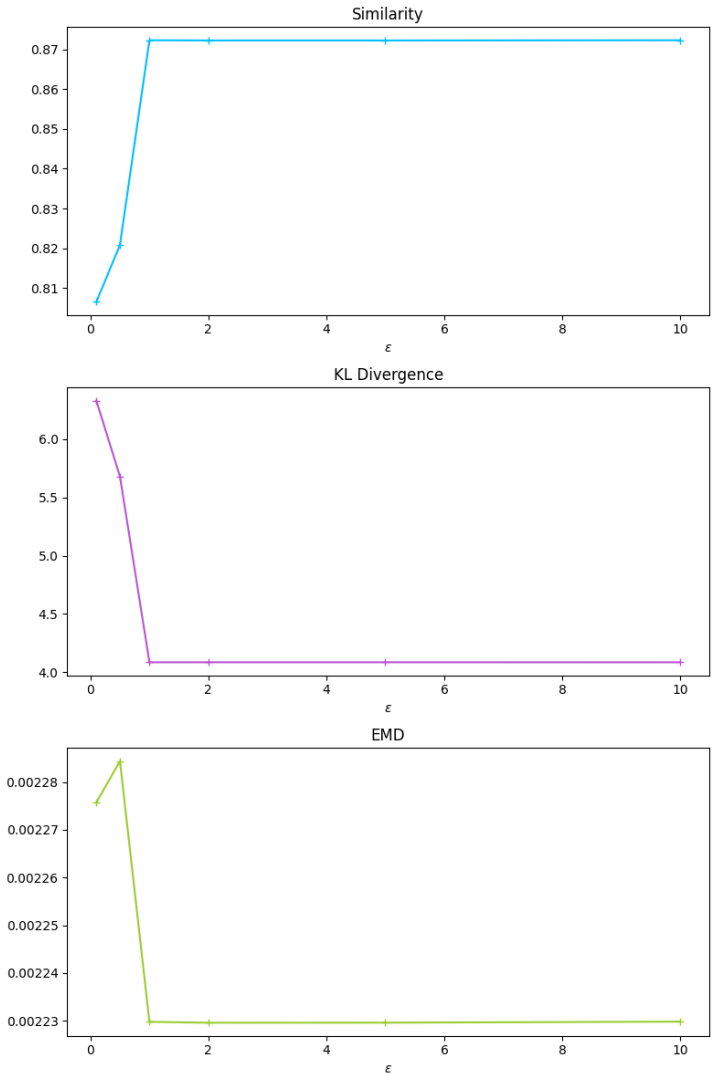


Figure 16: Metrics when varying ϵ

Critical Analysis : Merits

- **Innovative Approach:** Introduces a groundbreaking algorithm for generating heatmaps that ensure individual privacy while preserving the utility of aggregated data, addressing a critical need in the field of differential privacy and data visualization.
- **Optimized for EMD:** The algorithm optimizes under Earth Mover's Distance (EMD) aggregation, representing a methodological leap in creating visual representations that maintain high visual fidelity and relevance.
- **Enhanced Privacy and Utility Guarantees:** Offers a robust solution for privacy-preserving data visualization by enhancing privacy guarantees without sacrificing the quality and perceptual similarity of heatmaps compared to the baseline.
- **Solid Theoretical Foundation:** Provides a comprehensive theoretical background, including a formal proof of privacy and utility guarantees, setting a clear framework for its effectiveness under specific conditions.

Critical Analysis : Limits

- **Dependency on Sparse Data Distributions:** The algorithm's performance is optimal for sparse data distributions, which may not always be representative of real-world datasets.
- **Implementation Clarity:** The paper provides unclear explanations for the algorithm's practical implementation steps, particularly in constructing the pyramidal transform, which may hinder understanding and replication efforts.
- **Technical Barriers to Reproduction:** The complexity and technical nature of both the proposed algorithm (especially the Pyramidal Transform) and the baseline adaptation from previous work raise concerns about the ease of reproducing the results without a significant level of expertise.
- **Computational Demands of EMD Solution:** Finding the EMD solution through a linear program is time-consuming and computationally intensive, making the algorithm less accessible for real-time applications or for use by individuals with limited technical resources.

Conclusion

- **Innovative Algorithm for Differential Privacy:** Introduced an innovative algorithm improving differential privacy for sparse distributions using a tree-level Laplace mechanism, demonstrating a notable preservation of heatmap distribution data.
- **Success in Replication and Enhanced Results on Different Datasets:** Successfully replicated the original study's findings to some extent. Observed improved results when applying the algorithm to datasets different from the original study, highlighting its privacy-utility balance efficiency.
- **Limitation to Sparse 2D Datasets and Demand on Computing Resources:** The algorithm is specifically designed for sparse 2D datasets, making its application to other data types unfeasible, while its demand in computing resources potentially limits broader application.
- **Broadening Applicability:** Improving computational efficiency to make the algorithm more applicable to extensive datasets beyond sparse geographical distributions is critical to enable widespread adoption of this novel method.

References I

[1] B. Ghazi, J. He, K. Kohlhoff, R. Kumar, P. Manurangsi, V. Navalpakkam, and N. Valliappan, "Differentially private heatmaps," 2022.

[2] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," vol. 4004, pp. 486–503, 05 2006.

[3] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," vol. Vol. 3876, pp. 265–284, 01 2006.

[4] J. M. Abowd, "The u.s. census bureau adopts differential privacy," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, KDD '18, (New York, NY, USA), p. 2867, Association for Computing Machinery, 2018.

[5] L. Panavas, T. Crnovrsanin, J. Adams, A. Sarvghad, M. Tory, and C. Dunne, "Visual utility evaluation of differentially private scatterplots," 08 2022.

References II

[6] D. Zhang, A. Sarvghad, and G. Miklau, "Investigating visual analysis of differentially private data," *IEEE Transactions on Visualization and Computer Graphics*, vol. PP, pp. 1–1, 10 2020.

[7] D. Zhang, M. Hay, G. Miklau, and B. Bo O'Connor, "Challenges of visualizing differentially private data," 2016.

[8] E. Bagdasaryan, P. Kairouz, S. Mellem, A. Gascón, K. Bonawitz, D. Estrin, and M. Gruteser, "Towards sparse federated analytics: Location heatmaps under distributed differential privacy with secure aggregation," 2022.

[9] E. Cho, S. Myers, and J. Leskovec, "Friendship and mobility: User movement in location-based social networks," pp. 1082–1090, 08 2011.

[10] E. Dong, H. Du, and L. Gardner, "An interactive web-based dashboard to track covid-19 in real time," *The Lancet Infectious Diseases*, vol. 20, p. 533–534, May 2020.