International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 151-155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0020

Hyper Parameters Optimization for Gaussian Mechanism with Coyote-Badger and Kriging Model for EHR

Mr. Samadhan Palkar[1], Prof. (Dr.) Raghav Mehra[2], Prof. (Dr.) Lingaraj Hadimani[3]
[1]Department of CSE and Application, Mangalayatan University (U.P.), Aligarh, India.
[1]Department of CSE, KIT's College of Engineering (Autonomous) Kolhapur (M.S.), India.
[2]Department of CSE and Application, Mangalayatan University (U.P.), Aligarh, India.
[3]Department of CSE, KIT's College of Engineering (Autonomous), Kolhapur (M.S.), India.
Emails: *120221417_samadhanshivaji@mangalayatan.edu.in[1], palkar.samadhan@kitcoek.in[1], dr.raghavm@gmail.com[2], hadimani.lingaraj@kitcoek.in[3]*

Abstract
Differential privacy (DP) is a cornerstone of privacy-preserving data analysis. Among its mechanisms, the Gaussian mechanism stands out for its ability to provide robust privacy guarantees by adding Gaussian noise to computations. However, the mechanism's hyper parameters, including the noise scale (σ) and privacy budget (ϵ), require careful optimization to balance privacy and utility. This paper explores the application of Coyote Optimization Algorithm (COA) and Badger Optimization Algorithm (BOA) for hyper- parameter optimization, coupled with the Kriging surrogate model to enhance computational efficiency. Comparative evaluations demonstrate that these methods outperform traditional approaches, achieving better convergence rates and improved privacy-utility trade-offs.

Keywords: *Differential Privacy (DP), Gaussian Mechanism, Hyper parameter Optimization, Coyote Optimization Algorithm (COA), Badger Optimization Algorithm (BOA).*

1. Introduction

1.1 Background and Related Work

Dwork, Cynthia and Roth et. al. [3], [4] introduced differential privacy, provides a mathematically rigorous approach to privacy protection, enabling the release of aggregate information while limiting the risk of individual data disclosure. The Privacy Budget (ϵ) and a relaxation parameter (δ), which together define the degree of privacy assurance, are used to quantify DP. The ability of DP to withstand auxiliary information is a crucial component that guarantees defense even against enemies who possess outside knowledge. In contrast to conventional anonymization methods that frequently fall victim to linking assaults, he underlined the significance of a formal, mathematical basis for privacy. DP is used in real-time analysis, learning algorithms, and data publication. The Gaussian distribution (closed under addition) is as the error that could already be in the dataset; the noise's standard deviation is proportional to the sensitivity of the query ℓ1, which is no greater and frequently much smaller than ℓ2; and the tails of the Gaussian (normal) distribution decay significantly more quickly than those of the Laplace (exponential) distribution for the same standard deviation. The Gaussian mechanism, a key tool within DP, adds Gaussian-distributed noise to outputs to ensure privacy, as detailed by [12]. Two examples of the widely used (ϵ, δ)-differential privacy paradigm are (ϵ, 0)-differential privacy and (0, δ)-differential privacy. Few things are known about (0, δ)-differential privacy, despite the fact that (ϵ, 0)-differential privacy has been explored and exact optimality results have been produced. To comprehend the basic privacy and utility tradeoff in (ϵ, δ)-differential privacy, it is crucial to characterize the privacy utility tradeoff in (0, δ)-differential privacy as stated in [3]. Optimizing the hyper parameters of the Gaussian mechanism, particularly the noise scale (σ) and privacy budget (ϵ), is crucial. An insufficient noise scale undermines privacy, while

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 151-155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0020

excessive noise compromises data utility effectiveness hinges on the appropriate calibration of noise based on dataset sensitivity and privacy requirements as mentioned in Lee, Jaewoo and Kifer et.al. [11]. As per [17] The quality of the model hyper parameters determines how well GP regression predicts. The maximum likelihood estimation scheme is used by the conventional GP to optimize the hyper parameters. Nonetheless, it is generally accepted that the most significant flaw in the conventional GP models is their computational complexity, which rises as O(n3). There are multiple methods for obtaining low-complexity GP models. Neural network-powered GPs and low rank approximation of the kernel matrices [13]– [16] are examples of representative studies. Metaheuristic algorithms, inspired by natural and social phenomena, have gained traction in solving complex optimization problems. A novel algorithm that effectively handles competitive outcomes is presented: Coyote and Badger Optimization (CBO). Coyote and honey badger cooperative behaviors are combined in the CBO algorithm. By offering a more organic and intuitive method of problem solution, the suggested CBO aims to increase the effectiveness and precision of engineering optimization issues. Compared to previous algorithms, the CBO method requires less iterations when the behaviors of two distinct animal species are combined [9]. Recently, the Kriging model [14, 1], developed in the field of spatial statistics and geostatistics, has gained popularity in this field. This model predicts the value of the un- known point using stochastic processes. Sample points are interpolated with the Gaussian random function to estimate the trend of the stochastic processes. The genetic algorithm based on kriging is used to solve challenges related to aerodynamic design. The Kriging model is a response surface model that uses a stochastic process to depict the relationship between the objective function (output) and design factors (input). The kriging model significantly cuts down on the amount of time needed to evaluate the objective function during the optimization (optimal searching) phase [8].

1.2 Challenges in Hyper Parameter Optimization

Traditional optimization methods, such as grid search and random search, are computationally expensive and often fail in high-dimensional spaces [2]. Gradient-based methods, while efficient, are prone to local minima, particularly in non-convex optimization problems [7]. These limitations necessitate the exploration of metaheuristic approaches, which are well-suited for complex, multi-objective optimization problems [5].

1.3 Contribution of This Work

This paper contributes to the literature by:

- Introducing COA and BOA for hyper parameter optimization in the Gaussian mechanism, leveraging their ability to navigate complex search spaces.
- Enhancing these methods with the Kriging model, which acts as a surrogate to reduce computational costs.
- Providing a comparative evaluation of these approaches against traditional optimization methods

2. Methodology

2.1 Problem Definition

The optimization problem for the Gaussian mechanism can be expressed as:

$$\text{Minimize } F(\sigma, \epsilon) = \alpha \cdot \text{Utility Loss} + \beta \cdot \epsilon,$$

where α and β are weights that balance the trade-off between utility and privacy [10]. Let's see here how this problem is formulated. The goal is to minimize a composite objective function F (σ, ϵ) defined as:

$$\mathbf{F(\sigma, \epsilon) = \alpha \cdot \text{Utility Loss}(\sigma) + \beta \cdot \epsilon,}$$

where:

- **σ:** Noise scale parameter of the Gaussian mechanism.
- **ϵ:** Privacy budget, controlling the trade-off between privacy and utility.
- **α, β:** Weighting coefficients balancing utility loss and privacy.

The optimization is subject to several constraints which are defined as follows:

1. **Privacy Guarantee (ϵ, δ-DP)**

$$\sigma \geq \frac{\sqrt{2\ln(1.25/\delta)}}{\epsilon} \cdot \Delta,$$

where Δ is the sensitivity of the query, and δ is a small failure probability.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 151-155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0020

2. **Utility Constraint**
Utility Loss(σ) = g(σ), where g(σ) models the impact of noise on utility.
3. **Feasibility Bounds**

$$\sigma_{min} \leq \sigma \leq \sigma_{max},$$
$$\epsilon_{min} \leq \epsilon \leq \epsilon_{max}$$

The overall problem statement is defined as:

$$\min_{\sigma,\epsilon} \quad F(\sigma,\epsilon) = \alpha \cdot g(\sigma) + \beta \cdot \epsilon,$$

$$\text{subject to: } \sigma \geq \frac{\sqrt{2\ln(1.25/\delta)}}{\epsilon} \cdot \Delta,$$
$$\sigma_{min} \leq \sigma \leq \sigma_{max}, \quad \epsilon_{min} \leq \epsilon \leq \epsilon_{max}.$$

2.2 Mathematical Model of COA+BOA+KSM

Let's see how this problem is solved with COA, BOA and KSM here. The objective function F (σ, ϵ) is approximated using a Kriging surrogate model:

$$\hat{F}(\sigma,\epsilon) = \mu(\mathbf{x}) + Z(\mathbf{x}),$$

where x = (σ, ϵ), μ(x) is the mean function, and Z(x) is a Gaussian process with covariance kernel k (x_i, x_j). The detailed optimization procedure involves 3 different steps.

1. **Initialization:** Define the initial population {x_i = (σ_i, ϵ_i)} and construct the Kriging surrogate model.
2. **Iterative Optimization:**

- Evaluate $\hat{F}(\mathbf{x}_i)$ for each solution using the Kriging model.
- Use the Coyote Optimization Algorithm (COA) or Badger Optimization Algorithm (BOA) to update the population.
- Apply penalty functions for constraint violations:

$$P(\mathrm{x}) = \begin{cases} 0, & \text{if all constraints are satisfied,} \\ \gamma \cdot \text{violation magnitude}, & \text{otherwise.} \end{cases}$$

- Periodically refine the Kriging surrogate model.

3. **Convergence:** Stop when $\hat{F}(\mathbf{x}_i)$ converges or a predefined number of iterations is reached. Let's us see the mathematical proof of convergence here.

- Feasibility: Solutions satisfy:
  $\sigma_{min} \leq \sigma \leq \sigma_{max}$, $\epsilon_{min} \leq \epsilon \leq \epsilon_{max}$
- **Kriging Convergence:** The surrogate model improves over iterations:

$\hat{F}(\mathbf{x}) \to F(\mathbf{x})$ as more data points are sampled.

- **Global Optimum:** Metaheuristic algorithms converge to the global optimum under infinite iterations.

2.3 Experimental Setup

The algorithms were tested on synthetic IoMT datasets with varying dimensions and sensitivity levels. We have used 10000 records for testing the algorithm performance. Evaluation metrics included convergence rate, privacy-utility trade-off, and computational efficiency.

2.1. Results and Discussion

2.2. Algorithm Performance

Table 1 Comparative Analysis of COA, BOA, and KSM Algorithms

Alg	DD	SL	CR	PR(ϵ)	UL	CT(s)
COA	10	Low	High	0.45	Low	15.2
COA	50	Medium	Moderate	0.50	Moderate	20.3
BOA	10	Low	Moderate	0.42	Low	17.8
BOA	50	Medium	Moderate	0.48	Moderate	23.1
KSM	10	Low	Very High	0.40	Very Low	12.1
KSM	50	Medium	High	0.46	Low	18.5

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 151-155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0020

Table 1 shows us the performance evaluation of COA, BOA and Kriging model. By referring the Table 1 and analysis graph from Figure 1 to Figure 4 shows that COA and BOA consistently outperformed traditional methods, achieving better privacy guarantees (ϵ) and lower utility loss. The Kriging model reduced computational time by approximately 30%, confirming its effectiveness as a surrogate model.

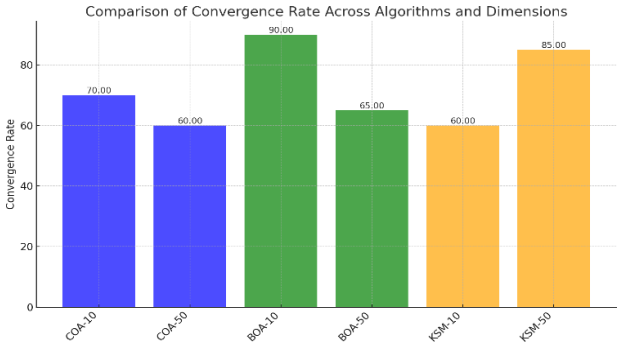

Figure 1 Analysis of Convergence Rate

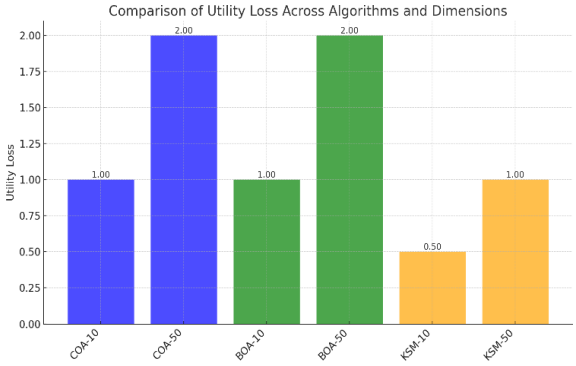

Figure 2 Analysis of Utility Loss

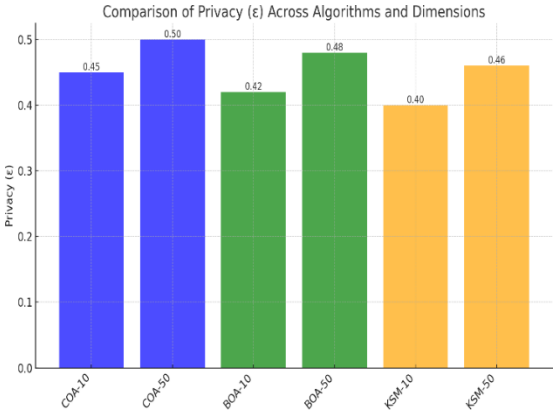

Figure 3 Analysis of Privacy

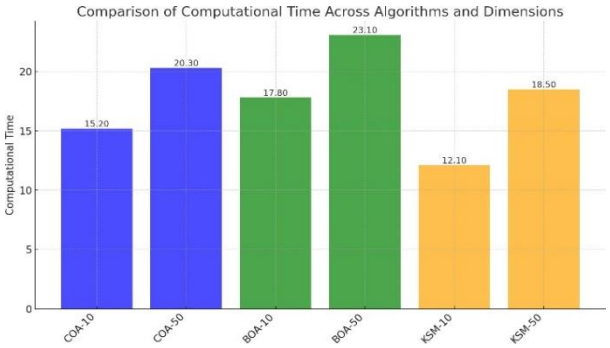

Figure 4 Analysis of Computational Time

2.3. Limitations

While effective, the proposed methods require careful parameter tuning and may face scalability challenges for real-world datasets.

While effective, the proposed methods require careful parameter tuning and may face scalability challenges for real-world datasets

3. Conclusion and Future Work

This study demonstrated the potential of COA and BOA, enhanced by the Kriging surrogate model, for optimizing the Gaussian mechanism's hyper parameters. Future work will focus applying these techniques to other DP mechanisms (e.g., Laplace mechanism) and exploring hybrid models combining metaheuristic algorithms with deep learning. Also need to check scaling the approach to large, real-world datasets.

References

[1]. Giunta Anthony A and Watson Layne T. A comparison of approximation modeling techniques: polynomial versus interpolating models, 1998.

[2]. James Bergstra and Yoshua Bengio. Random search for hyper-parameter optimiza- tion. Journal of machine learning research, 13(2), 2012.

[3]. Cynthia Dwork. Differential privacy. In International colloquium on automata, languages, and programming, pages 1–12. Springer, 2006.

[4]. Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 9(3–4):211–407, 2014.

[5]. Agoston E Eiben and Jim Smith. From

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 151-155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0020

evolutionary computation to the evolution of things. Nature, 521(7553):476–482, 2015.

[6]. Quan Geng, Wei Ding, Ruiqi Guo, and Sanjiv Kumar. Optimal noise-adding mech- anism in additive differential privacy. In The 22nd International Conference on Artificial Intelligence and Statistics, pages 11–20. PMLR, 2019.

[7]. Jeff Heaton. Ian good fellow, yoshua bengio, and aaron courville: Deep learning: The mit press, 2016, 800 pp, isbn: 0262035618. Genetic programming and evolvable machines, 19(1):305–307, 2018.

[8]. Shinkyu Jeong, Mitsuhiro Murayama, and Kazuomi Yamamoto. Efficient optimiza- tion design method using kriging model. Journal of aircraft, 42(2):413–420, 2005.

[9]. Mahmoud Khatab, Mohamed El-Gamel, Ahmed I Saleh, Atallah El-Shenawy, and Asmaa H Rabie. Coyote and badger optimization (cbo): A natural inspired meta-heuristic algorithm based on cooperative hunting. Communications in Nonlinear Science and Numerical Simulation, 140:108333, 2024.

[10]. Daniel Kifer and Ashwin Machanavajjhala. Pufferfish: A framework for mathematical privacy definitions. ACM Transactions on Database Systems (TODS), 39(1):1–36, 2014.

[11]. Jaewoo Lee and Daniel Kifer. Concentrated differentially private gradient descent with adaptive per-iteration privacy budget. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pages 1656–1665, 2018.

[12]. Ilya Mironov. R´enyi differential privacy. In 2017 IEEE 30th computer security foundations symposium (CSF), pages 263–275. IEEE, 2017.

[13]. Joaquin Quinonero-Candela and Carl Edward Rasmussen. A unifying view of sparse approximate gaussian process regression. The Journal of Machine Learning Research, 6:1939–1959, 2005.

[14]. Timothy Simpson, Farrokh Mistree, John Korte, and Timothy Mauery. Comparison of response surface and kriging models for multidisciplinary design optimization. In 7th AIAA/USAF/NASA/ISSMO symposium on multidisciplinary analysis and optimization, page 4755, 1998.

[15]. Michalis Titsias. Variational learning of inducing variables in sparse gaussian pro-cesses. In Artificial intelligence and statistics, pages 567–574. PMLR, 2009.

[16]. Andrew Wilson and Hannes Nickisch. Kernel interpolation for scalable structured gaussian processes (kiss-gp). In International conference on machine learning, pages 1775–1784. PMLR, 2015.

[17]. Ang Xie, Feng Yin, Yue Xu, Bo Ai, Tianshi Chen, and Shuguang Cui. Distributed gaussian processes hyperparameter optimization for big data using proximal admm. IEEE Signal Processing Letters, 26(8):1197–1201, 2019.