Labeling-Free Comparison Testing of Deep Learning Models

Yuejun Guo, Qiang Hu, Maxime Cordy, Xiaofei Xie, Mike Papadakis, and Yves Le Traon
SnT, University of Luxembourg, Luxembourg
Singapore Management University, Singapore

ABSTRACT
Various deep neural networks (DNNs) are developed and reported for their tremendous success in multiple domains. Given a specific task, developers can collect massive DNNs from public sources for efficient reusing and avoid redundant work from scratch. However, testing the performance (e.g., accuracy and robustness) of multiple DNNs and giving a reasonable recommendation that which model should be used is challenging regarding the scarcity of labeled data and demand of domain expertise. Existing testing approaches are mainly selection-based where after sampling, a few of the test data are labeled to discriminate DNNs. Therefore, due to the randomness of sampling, the performance ranking is not deterministic. In this paper, we propose a labeling-free comparison testing approach to overcome the limitations of labeling effort and sampling randomness. The main idea is to learn a Bayesian model to infer the models’ specialty only based on predicted labels. To evaluate the effectiveness of our approach, we undertook exhaustive experiments on 9 benchmark datasets spanning in the domains of image, text, and source code, and 165 DNNs. In addition to accuracy, we consider the robustness against synthetic and natural distribution shifts. The experimental results demonstrate that the performance of existing approaches degrades under distribution shifts. Our approach outperforms the baseline methods by up to 0.74 and 0.53 on Spearman’s correlation and Kendall’s τ, respectively, regardless of the dataset and distribution shift. Additionally, we investigated the impact of model quality (accuracy and robustness) and diversity (standard deviation of the quality) on the testing effectiveness and observe that there is a higher chance of a good result when the quality is over 50% and the diversity is larger than 18%.

KEYWORDS
deep neural network, comparison testing, labeling-free, Bayesian model

1 INTRODUCTION
Deep learning (DL) has achieved great success in various domains, such as computer vision [29], natural language processing [26], code understanding [30], and autonomous driving [18]. Due to the outstanding performance of deep neural networks (DNNs), researchers from the software engineering (SE) community have attempted to apply DNNs for diverse SE tasks, such as source code processing [7, 30], automatic software testing [41, 42], and GUI designs [40]. Generally, for developers, compared with designing a new DNN architecture that requires tremendous DL knowledge, reusing publicly available models is an efficient and popular strategy to avoid preparing everything from scratch. Moreover, it is practical in real-world applications concerning the training cost and difficulty due to the increasing size and complexity of DNNs.

With the fast-growing of DNNs, it is easy to collect massive DNNs by either pre-trained model files (e.g., .h5 and .pth) or training scripts from public sources like GitHub [4]. Thus, there is a high demand in testing the performance of collected models for practical use. However, as the contributors and developing constraints are diverse, their performance is rarely given or is not reliable by unknown testing conditions. For example, only 21 of the 165 DNNs we collected and evaluated in this paper have a performance report. Testing the DNNs requires test data especially out-of-distribution (OOD) data [9, 13, 17]. In practice, when deploying DNNs in real scenarios, the distribution shift is inevitable. Namely, the test data can be OOD compared to the initial test data which by default come from the same distribution as the training data. As a result, these models may exhibit remarkably different behaviors, which raises the concern of quality and reliability [6]. For instance, for the same dataset iWildCam (please refer to Section 4.3 for more details), two DNNs exhibit 75.74% and 76.60% accuracy on initial test data, while with distribution shift, their performance turns to 76.82% and 65.30%, respectively, on new test data. Test data can be from the real world and unlabeled [35]. For example, AOJ [1] receives submissions in different programming languages all the time. However, manual labeling is expensive and tedious, especially when domain knowledge is in demand. For example, a Java developer can easily annotate the source code in Java but may have difficulties with other programming languages as C++. How to precisely and efficiently test and rank the performance of DNNs when only given the predictions is our key point of problem definition.

Some approaches have been proposed for comparison testing of multiple DNNs. For example, a recent approach named sample discrimination based selection (SDS) [25] achieves positive model ranking results on three benchmark datasets. SDS selects a set of
data to label based on the majority voting [31] and item discrimination [14]. These data are considered as the most discriminative in terms of distinguishing the accuracy between DNNs. Finally, DNNs are ranked based on their accuracy on these selected and labeled data. However, there are three main limitations. First, it is sample-selection-based which requires the labeling effort. Second, the rank is only based on the accuracy of in-distribution (ID) data that follow the same distribution as the training data. However, for model deployment, the performance (robustness) on out-of-distribution (OOD) remains uncertain and should be considered. Third, the evaluation is limited to the image domain, its effectiveness for software tasks is unclear.

Concerning the above three issues, in this paper, we propose a labeling-free and reliable approach to rank multiple DNNs. To summarize, the main contributions of our work are:

1. We proposed a novel approach for comparison testing and ranking multiple DNN models to facilitate the reuse of DNNs from public sources.

2. In addition to the ranking by accuracy based on ID data, our proposed approach is flexible and stable to deal with the ranking concerning robustness based on OOD data with both synthetic (15 types of corruptions \( \times 5 \) levels of severity) and natural distribution shifts.

3. Our approach is labeling-free. To overcome the challenge of labeling effort, our approach infers the specialties of DNNs by building a Bayesian model using only the observed predicted labels. The Bayesian model estimates the most likely model specialty for the predictions of DNNs. In addition, compared to existing approaches, such as SDS, our approach does not require random sampling in the procedure, which avoids the sampling randomness.

4. We experiment on 9 benchmark datasets for comparison testing of DNNs. These datasets span different domains including image, text, and source code with different programming languages (Java and C++). To the best of our knowledge, this is the first DNN comparison testing work containing datasets other than image.

2 BACKGROUND AND RELATED WORK

We review the work on deep learning testing and especially comparison testing.

2.1 Deep Learning Testing

Deep learning (DL) testing refers to evaluating the quality of developed deep neural networks (DNNs) for further deployment [39]. A simple and local testing strategy is to split a dataset into training, validation, and test sets. The training and validation sets contribute to the training process to tune parameters. The test set is untouched by the training process to provide an unbiased evaluation of the accuracy. Typically, this testing is built on the assumption that the training and test sets are independent and identically distributed.

However, in practical scenarios, the testing always suffers from distribution shifts where the quality (robustness) of models can degrade significantly [29]. For instance, adding a minor Gaussian noise to an image can mislead a DNN to the wrong function [16]. Another example is about the customer comments. With new collected comments, since new customers may have appeared [28], the model needs to be rechecked for its quality and reliability. Given these concerns, the robustness of DL systems has recently received considerable attention from researchers [9, 15, 20].

Roughly speaking, there are two types of distribution shifts, synthetic and natural. Synthetic distribution shift mainly comes from adding artificial perturbations (corruptions) into raw data. Dan and Thomas [16] proposed to add 15 types of algorithmically generated corruptions with 5 levels of severity into image data to mimic realistic situations, such as noise, blur, snow, and zoom. Based on these corruptions, different benchmark datasets, such as CIFAR-10-C [16] and MNIST-C [27], have been developed for testing the robustness of DNN models. On the other hand, natural distribution shift is usually induced by the change of environment or population and exists in raw data, such as the change of camera traps [8] and new customers [28]. A recent benchmark [20] provides in-the-wild distribution shifts covering diverse data domains and applications.

2.2 Comparison testing

In conventional software engineering, comparison testing [19, 32, 33] aims at figuring out the strength and weaknesses of a newly developed software product compared with existing products. The end goal is to facilitate the deployment of a product with high functionality and reliability.

Regarding a DNN as a software product, we can take the same testing by testing different DNNs with the same test. However, the obstacle is that usually, the test data are numerous but unlabelled. Thus, there is no prior information to reveal the underlying performance. Recently, Meng et al. [25] proposed to compare the performance of multiple DNNs based on a few labeled data. Concretely, the problem turns into how to find out the most discriminative data that can amply distinguish the difference. In their proposed sample discrimination based selection method, the majority voting [31] is first applied to produce pseudo labels based on which DNNs are classified to top, middle, and bottom groups following the item discrimination [14]. Via the prediction difference by the top and bottom DNNs, each data has a unique discrimination score and the high ones are selected for the final ranking.

A close topic to comparison testing is test selection [24, 34, 36] where a few data are selected and annotated to approximate the performance of a DNN. For instance, Li et al. [23] proposed the cross Entropy-based sampling to identify the most representative data of a test set. Similarly, Chen et al. [10] developed the practical accuracy estimation. The difference is that in test selection, the objective is a single DNN, while in comparison testing, the objective is multiple DNNs. Undoubtedly, one can first approximate the performance of each DNN by selecting its corresponding representative set then undertake the comparison. However, this will largely increase the effort in labeling and is less practical than selecting once.

3 METHODOLOGY

3.1 Problem Formulation

In this paper, we are interested in the classification task. Given a \( C \)-class task over a sample space \( \mathcal{X} = \mathbb{X} \times \mathbb{Y} \rightarrow \mathcal{R} \), where \( \mathbb{x} \in \mathbb{X} \) is an input data and \( y \in \mathbb{Y} \) is its class label. Let \( f : \mathbb{x} \rightarrow y \) be a deep
neural network (dnn) that maps x to the problem domain. Given n models, \( f_1, f_2, \ldots, f_n \), extracted from public sources and a set of unlabeled test data \( T \), the problem we study is to estimate the rank of models regarding their performance on \( T = \{x_1, x_2, \ldots, x_m\} \). Figure 1 illustrates the workflow.

We assume that the manual labeling is expensive especially when domain knowledge is required. To this end, we propose to tackle the ranking problem by only querying the predictions, which is highly applicable in practical scenarios. Remarkably, in this paper, we consider the performance of both accuracy and robustness. The accuracy and robustness are the correctness ratio of prediction on ID and OOD data, respectively.

### 3.2 Our Approach

Figure 2 gives an example of our approach. In this simple 3-class example, there are 3 DNN models \( (f_1, f_2, f_3) \) given 6 unlabeled samples \( (x_1, x_2, \ldots, x_6) \). The goal is to rank the 3 models concerning their accuracy on these samples in the absence of true labels. First, we compute the predicted label of each sample by each model and remove \( x_6 \) where all the models have the same prediction. Second, we initialize the two parameters, \( \alpha \) and \( \beta \), contained in our approach. \( \alpha \) refers to how difficult a sample is for all models to predict the correct label. \( \beta \) indicates how good a model is to output the correct labels of all samples. Initially, we use the simplest and most commonly used majority voting heuristic [31] to give a pseudo label to each sample. For instance, the pseudo label of \( x_1 \) is 6 because 2 \( (f_1, f_2) \) of 3 models predict the label as 0. \( \alpha \) is defined as the ratio of mismatched models that output a different label instead of the pseudo one. \( \beta \) is calculated as the ratio of correctly predicted samples over the entire set. Third, since the pseudo labels are not the true labels, \( \alpha \) and \( \beta \) cannot truly reflect the data difficulty and model ability. We optimize these two parameters by a likelihood estimation method in the presence of true labels. Finally, based on the optimized \( \beta \left( \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \right) \), we obtain the ranking 1, 3, and 2 for \( f_1, f_2, \) and \( f_3 \), respectively.

Given that no label is available in the test data, the main idea of our approach is to infer the specialties of DNNs by approximately maximizing the likelihood between the predictions and true labels via the expectation-maximization (EM) algorithm [12]. Let \( \tilde{Y} = \left\{ \tilde{y}_{ij} \right\}_{1 \leq i \leq m, 1 \leq j \leq n} \) be the predicted labels of \( T \) and \( Y = \{y_i\}_{1 \leq i \leq m} \) be the true labels. Here, \( \tilde{y}_{ij} \) refers to \( x_i \) and model \( f_j \). Given the observed \( \tilde{Y} \) and latent \( Y \) governed by unknown parameters \( \theta \), the likelihood function is defined as \( L(\theta; \tilde{Y}) = p(\tilde{Y} | \theta) = \sum_{\tilde{y}_i} p(\tilde{Y} | y_i | \theta) \).

The goal is to search the best \( \theta \) that maximizes the likelihood, in other words, the probability of observing \( \tilde{Y} \). As for \( \theta \), inspired by [37], we consider two factors, data difficulty \( \alpha = \{\alpha_i\}_{1 \leq i \leq m} \) and model specialty \( \beta = \{\beta_j\}_{1 \leq j \leq n} \), that influence the performance of DNNs. Namely, \( \theta = (\alpha, \beta) \). Algorithm 1 presents the pseudo code of our approach.

**Step 1: Pruning.** Inevitably, some data will receive the same predictions by all models, which is useless for discriminating the performance and causes computational cost. For this reason, we filter these data without losing any information for ranking and obtain a smaller set \( T' \) (Lines 1-6 in Algorithm 1).

**Step 2: Initializing.** First, for each data \( x_i \), a pseudo label is voted by the majority of DNNs, namely, \( \hat{y}_i' = \text{mode} \left( \left\{ \tilde{y}_{ij} \right\}_{1 \leq j \leq n} \right) \) (Lines 7-9). Next, \( \alpha_i \) is the number of DNNs that gives a different label from the pseudo label and \( \beta_j \) is the accuracy based on pseudo labels (Lines 10-15). Formally, the definitions are:

\[
\alpha_i = \frac{\left| \left\{ j \mid \tilde{y}_{ij} \neq y_i', 1 \leq j \leq n \right\} \right|}{n}, \beta_j = \frac{\left| \left\{ i \mid \tilde{y}_{ij} = y_i', 1 \leq i \leq |T'| \right\} \right|}{|T'|}
\]

**Step 3: Optimizing.** The EM algorithm solves the optimization problem by iteratively performing an expectation (E) step and a maximization (M) step (Lines 16-20). In the E-step, it estimates the expected value of the log likelihood:

\[
Q(\theta, \theta_{last}) = \mathbb{E} \left[ \log L(\theta; \tilde{Y}, Y) \right] = \sum_{i=1}^{|T'|} \mathbb{E} \left[ \log p(y_i) \right] + \sum_{j=1}^n \mathbb{E} \left[ p(y_i | y_j, \alpha_i, \beta_j) \right]
\]

where \( \theta = (\alpha, \beta) \) and \( \theta_{last} \) is from the last E-step. For the computation, we use the definition from [37] where \( p(\tilde{y}_{ij} = y_j | \alpha_i, \beta_j) = \frac{1}{1 + e^{-\alpha_i \beta_j}} \). Besides, as \( \tilde{y}_{ij} \) and \( \beta \) are independent given \( \alpha \), \( p(y_i) = p(y_i | \alpha, \beta_j) \). Remarkably, \( y_i \) represents the true label of a sample.

In the ranking problem, \( y_i \) is absent but the probability of taking it as a true label is can be inferred by \( p(y_i | \alpha, \beta_j) \).

In the M-step, the gradient ascent is applied to search for \( \alpha \) and \( \beta \) that maximize \( Q \).

**Step 4: Ranking.** Finally, as \( \beta \) well estimate the abilities of each DNN given the observed labels, we use this vector to rank DNNs (Line 27). In other words, a high specialty indicates a good performance on the data.

### 4 EXPERIMENTAL SETUP

#### 4.1 Implementation

All experiments were conducted on a high-performance computer cluster and each cluster node runs a 2.6 GHz Intel Xeon Gold 6132 CPU with an NVIDIA Tesla V100 16G SXM2 GPU. We implement the proposed approach and baseline methods based on the state-of-the-art frameworks, Tensorflow 2.3.0 and PyTorch 1.6.0. To allow for reproducibility, our full implementation and evaluation subjects are available on GitHub. For synthetic data distribution shift, we consider two benchmark datasets where each includes 15 types of natural corruption with 5 levels of severity. In other words, we test on 150 datasets with the synthetic distribution shift. Due to the space limitation, we only report the average results on corrupted data for baseline methods. The remaining results corroborate our findings and are freely available on our companion project website.

#### 4.2 Research Questions

In this study, we focus on the following three research questions:

- **RQ1 (effectiveness given ID test)**: How does our proposed approach ranking multiple DNNs given ID test data?

---

1 We will make the implementation publicly available upon acceptance.
We choose 7 datasets, MNIST [22], Fashion-MNIST [38], CIFAR-10 [21], iWildCam [8], Amazon [28], Java250, and C++1000 [30] that are widely studied in previous work. These datasets cover the image (first 4), text (Amazon), and source code (Java250 and C++1000) domains. The test data that follow the same distribution as the training set are the so-called in-distribution (ID) data. The test data with data distribution shift are out-of-distribution (OOD). In our work, we consider two types of distribution shifts: synthetic and natural. For the synthetic distribution shift, we use two benchmark datasets, MNIST-C [27] and CIFAR-10-C [16], for MNIST and CIFAR-10, respectively. Each benchmark includes 75 datasets with 15 types of natural corruptions, such as Gaussian noise, shot noise, impulse noise, defocus blur, frosted glass blur, motion blur, zoom blur, snow, frost, fog, brightness, contrast, elastic, pixelate, and jpeg. Besides, each type of corruption has 5 levels of severity. For the natural distribution shift, we use two datasets for iWildCam and Amazon from a recent-published benchmark, WILDS [20]. The distribution shift comes from new came traps in iWildCam and new users in Amazon. Table 1 lists the details of datasets.

DNNs. From Github, we collect, in total, 165 models, 30 for MNIST, 25 for Fashion-MNIST, 30 for CIFAR-10, 20 for iWildCam, 20 for Amazon, 20 for Java250, and 20 for C++1000. In concrete, the models of MNIST and CIFAR-10 are extracted using the github links in [25]. The 25 models of Fashion-MNIST are extracted from [2] provided by Meng et al. [25]. For iWildCam and Amazon, we train models using the implementation in the benchmark WILDS [20]. For Java250 and C++1000, we train models using the implementation in the benchmark Project CodeNet [30]. Table 1 presents the accuracy and robustness of DNNs on ID test data and OOD test data with natural distribution shift, respectively. Table 2 summarizes the robustness on MNIST-C and CIFAR-10-C with the synthetic distribution shift.

### 4.4 Baseline Methods

In our study, we compare our approach to 3 baseline methods, random sampling, SDS, and CES. All baseline methods are sample-selection-based. Following [25], the labeling budget of the baseline methods ranges from the number of DNNs (i.e., 30 DNNs in MNIST) to 180 at intervals of 5. Let $n$ be the number of DNNs, $m$ be the number of unlabeled test data, and $b$ be the number of data selection (e.g., 31 in MNIST).

Random sampling is a basic and model-independent method for data selection where each data has an equal probability to be considered. A subset of data is randomly selected and annotated to rank DNNs.
Algorithm 1: Labeling-free comparison testing

```
Input : (f_1, f_2, ..., f_n): DNNs for comparison
       T = {x_1, x_2, ..., x_m}: test set
       Γ: performance criterion

Output : (r'(f_1), r'(f_2), ..., r'(f_n)): Rank of DNNs

/* Step 1: Pruning */
1 T' = {}
2 for i = 1 → m do
3   if |{y_{ij}| y_{ij} ∈ T_i ∩ T_j}| > 1 then // y_{ij} is the predicted label by f_j
4       T' ← x_i ;
5     end
6 end
/* Step 2: Initializing */
7 for i = 1 → |T'| do
8   y'_i = mode({y_{ij}| y_{ij} ∈ T_i ∩ |T'|}) ; // Data difficulty
9 end
/* Step 3: Optimizing */
10 for i = 1 → |T'| do
11    a_i = |y_{ij} ∩ y'_j|/n ; // Model specialty
12 end
13 for j = 1 → n do
14    b_j = |y_{ij} ∩ y'_j|/|T'| ;
15 end
/* Step 4: Ranking */
16 r'(f_1), r'(f_2), ..., r'(f_n) = Sort(b)
17 return (r'(f_1), r'(f_2), ..., r'(f_n))

Sample discrimination based selection (SDS) [25] is the state-of-the-art approach in ranking multiple DNNs with respect to the accuracy. Following [25], among data in the top 25% with high discrimination scores, we randomly select a given budget of data to label and annotate to perform the ranking task.

Cross Entropy-based Sampling (CES) [23] is designed to select a set of representative data to approximate the actual performance given a single DNN. We follow the same procedure as [25] to adapt CES for multi-DNN comparison. First, for each model, we utilize CES to select b subsets of data with respect to the labeling budgets. Then, we rank all the models using each selected subset and produce b ranking results. Next, Spearman’s rank-order correlation is applied to each ranking (see Section 4.5), and therefore, we obtain b correlation coefficients. After that, for each model, we calculate the average of the b correlation coefficients. Finally, the model with the largest average correlation is regarded as the best, and the ranking performance based on this model is the baseline. Due to the random manner in the sampling methodology, each experiment of the baseline methods is repeated 50 times.

4.5 Evaluation Measures

To evaluate the effectiveness of each method, we employ three statistical analyses, Kendall’s τ rank correlation [11], Spearman’s rank-order correlation [11], and Jaccard similarity [25]. The first two evaluate the general ranking on all models, while the last one specifically estimates the ranking on top-k DNNs.

Given n DNNs, f_1, f_2, ..., f_n, let r(f_1), r(f_2), ..., r(f_n) be the ground truth ranking and r'(f_1), r'(f_2), ..., r'(f_n) be the estimated ranking. The Spearman’s rank-order correlation coefficient is computed as

\[
\rho = \frac{n \sum_{i=1}^{n} r(f_i) r'(f_i) - \left( \sum_{i=1}^{n} r(f_i) \right) \left( \sum_{i=1}^{n} r'(f_i) \right)}{\sqrt{n \sum_{i=1}^{n} r(f_i)^2 - \left( \sum_{i=1}^{n} r(f_i) \right)^2} \sqrt{n \sum_{i=1}^{n} r'(f_i)^2 - \left( \sum_{i=1}^{n} r'(f_i) \right)^2}}
\]

A large ρ indicates that the correlation between the ground truth and estimation is strong.

Kendall’s τ is

\[
\tau = \frac{P - Q}{\sqrt{(P + Q + T)(P + Q + U)}}
\]

where P and Q are the numbers of ordered and disordered pairs in \{r(f_i), r'(f_i)\}, respectively. T and U are the numbers of ties in \{r(f_i)\} and \{r'(f_i)\}, respectively. A large τ indicates a strong agreement between the ground truth and estimation.

Meng et al. proposed to apply the Jaccard similarity for measuring the similarity between the top-k models. The similarity coefficient is defined as:

\[
J_k = \frac{|\{f_i | r(f_i) <= k \} \cap \{f_i | r'(f_i) <= k \}|}{|\{f_i | r(f_i) <= k \} \cup \{f_i | r'(f_i) <= k \}|}, \ 1 \leq i \leq n
\]

A large J_k implies a high success in identifying the top-k models.

5 RESULTS AND DISCUSSION

5.1 RQ1: Effectiveness Given ID Test Data

First, we compare the effectiveness of four methods in ranking multiple DNNs based on the accuracy of ID data. Figure 3 shows the result measured by Spearman’s rank-order correlation. The first conclusion we can draw is that, over seven datasets, all methods succeed in outputting positively correlated rankings. By comparison, our proposed approach continuously outperforms (by up to 0.74) the baseline methods regardless of the labeling budget. Namely, the ranking by our approach is strongly correlated with the ground truth. In general, for the three sample-selection-based baseline methods, the correlation between the estimated rank and the ground truth increases when more data are labeled. However, for some datasets, the performance is still far from our approach. For example, in Amazon, our approach obtains a correlation coefficient of 0.80, while the best baseline, SDS, only achieves 0.48 using the maximum labeling budget of 180. Besides, due to the...
sampling randomness, each baseline method obtains different ranking results over 50 experiments, which is indicated by the large standard deviation (up to 0.36, shaded area in the figure) at each sampling randomness. The performance is highlighted in gray. The higher the better.

Table 3: Jaccard similarity of ranking the top-k DNNs based on the clean accuracy. For Random, SDS, and CES, we report the average results over all labeling budgets. The best performance is highlighted in gray. The higher the better.

| Jaccard Method | MNIST | Fashion-MNIST | CIFAR-10 | iWildCam | Amazon | Java250 | C++1000 | Average |
|----------------|-------|----------------|---------|----------|--------|---------|--------|---------|
| k=1            | IDS   | 0.03           | 0.03    | 0.02     | 0.02   | 0.02    | 0.02   | 0.02    | 0.02    | 0.07   |
|                | CES   | 0.11           | 0.12    | 0.13     | 0.11   | 0.13    | 0.13   | 0.13    | 0.13    | 0.09   |
|                | Out   | 0.23           | 0.23    | 0.23     | 0.24   | 0.24    | 0.24   | 0.24    | 0.24    | 0.21   |
| k=2            | IDS   | 0.05           | 0.05    | 0.05     | 0.05   | 0.05    | 0.05   | 0.05    | 0.05    | 0.07   |
|                | CES   | 0.24           | 0.24    | 0.24     | 0.24   | 0.24    | 0.24   | 0.24    | 0.24    | 0.18   |
|                | Out   | 0.24           | 0.24    | 0.24     | 0.24   | 0.24    | 0.24   | 0.24    | 0.24    | 0.21   |
| k=3            | IDS   | 0.06           | 0.11    | 0.06     | 0.09   | 0.09    | 0.08   | 0.08    | 0.08    | 0.13   |
|                | CES   | 0.09           | 0.09    | 0.09     | 0.09   | 0.09    | 0.09   | 0.09    | 0.09    | 0.09   |
|                | Out   | 0.09           | 0.09    | 0.09     | 0.09   | 0.09    | 0.09   | 0.09    | 0.09    | 0.09   |
| k=5            | IDS   | 0.11           | 0.12    | 0.11     | 0.11   | 0.11    | 0.11   | 0.11    | 0.11    | 0.12   |
|                | CES   | 0.11           | 0.11    | 0.11     | 0.11   | 0.11    | 0.11   | 0.11    | 0.11    | 0.11   |
|                | Out   | 0.11           | 0.11    | 0.11     | 0.11   | 0.11    | 0.11   | 0.11    | 0.11    | 0.11   |
| k=10           | IDS   | 0.11           | 0.12    | 0.11     | 0.11   | 0.11    | 0.11   | 0.11    | 0.11    | 0.11   |
|                | CES   | 0.11           | 0.11    | 0.11     | 0.11   | 0.11    | 0.11   | 0.11    | 0.11    | 0.11   |
|                | Out   | 0.11           | 0.11    | 0.11     | 0.11   | 0.11    | 0.11   | 0.11    | 0.11    | 0.11   |

Table 1: Summary of datasets. *#DNN* is the number of DNNs collected for each dataset. *#ID* is the number of in-distribution test data. *#OOD* is the number of out-of-distribution test data with synthetic or natural distribution shifts. MNIST-C and CIFAR-10-C are two benchmark datasets and the robustness is summarized in Table 2.

| Dataset | Data Type | #Classes | #DNN | #ID | Accuracy (%) | Distribution Shift | Robustness (%) |
|---------|-----------|----------|------|-----|-------------|--------------------|----------------|
| MNIST   | Image of handwritten digits | 10 | 30 | 10k | 85.27-99.54 | 570k | Synthetic |
| Fashion-MNIST | Image of fashion products | 10 | 25 | 10k | 90.09-93.38 | - | - |
| CIFAR-10 | Image of animals and vehicles | 10 | 30 | 10k | 69.90-95.92 | 750k | Synthetic |
| iWildCam | Image of wildlife | 182 | 20 | 8.154k | 75.72-77.76 | 42.791k | Natural |
| Amazon  | Text of comments | 5 | 20 | 46.95k | 73.60-74.84 | 100.05k | Natural |
| Java250 | Source code in Java | 250 | 20 | 15k | 64.73-87.39 | - | - |
| C++1000 | Source code in C++ | 1000 | 20 | 99.997k | 51.91-92.10 | - | - |

Table 2: Summary of MNIST-C and CIFAR-10-C with the synthetic distribution shift and robustness. Each dataset includes 15 types of natural corruptions (e.g., Gaussian Noise) with 5 levels of severity (1-5). The number in each cell presents the minimum and maximum robustness of multiple DNNs given the corruption type and severity.
Figure 3: Spearman’s rank-order correlation coefficient of ranking results based on ID test data. The higher the better. The shaded area represents the standard deviation. “Budget” is the number of labeled data (only apply to Random, SDS, and CES).

Figure 4: Kendall’s $\tau$ of ranking results based on ID test data. The higher the better. The shaded area represents the standard deviation. “Budget” is the number of labeled data (only apply to Random, SDS, and CES).

**Answer to RQ1:** Based on the accuracy of ID test data, our approach outperforms all the 3 selection-based baseline methods in outputting strongly correlated ranking. In addition, statistical analysis demonstrates that the outperforming is significant.

5.2 **RQ2: Effectiveness Under Distribution Shift**

For the synthetic distribution shift, Tables 4 and 5 summarize the results of Spearman’s rank-order correlation and Kendall’s $\tau$ on MNIST-C and CIFAR-10-C, respectively. We observe that our approach achieves the best performance in most cases, for instance, 291 of 300 cases in MNIST-C and 289 of 300 cases in CIFAR-10-C concerning Spearman’s correlation, and 287 of 300 and 288 of 300, respectively, in two benchmarks concerning Kendall’s $\tau$. Furthermore, as shown in RQ1, SDS performs the second-best among four ranking approaches. However, in these two tables, compared to random and CES, SDS tend to lose its performance (highlight in yellow). For example, in MNIST-C with Defocus Blur, severity-2,
SDS ranks the models wrongly with a correlation of -0.03 (Table 4), while both random and CES can achieve comparable ranking performance as our approach. In short, this existing state-of-the-art approach is sensitive to synthetic distribution shifts, which calls for the testing under distribution shifts of existing approaches.

Figure 5 shows the performance measured by Jaccard similarity of MNIST-C and CIFAR-10-C, respectively. In the 75 corruptions of MNIST-C (Figure 5(a)), both our approach and CES outperform the random sampling and SDS to precisely identify the top DNNs. On the other hand, in CIFAR-10-C (Figure 5(b)), our approach achieves the best performance (similarity of 1) in most cases (173 of 300).

For the natural distribution shift, the results on iWildCam and Amazon are shown in Figure 6. Our approach can better distinguish the performance of DNNs than the baseline methods. In particular, in Amazon, our approach is significantly better by up to 0.70 and 0.53 based on Spearman’s correlation and Kendall’s 𝜏, respectively. In addition, concerning the Jaccard similarity in Table 6, our approach is consistently the best in identifying the top DNNs. Note that in ranking the top 10 DNNs, our approach is not the best but is close to the best with a difference of 0.01 or 0.02 in iWildCam and Amazon, respectively.

In addition, compared to the effectiveness given ID test data, the ranking by all methods is different since the performance of DNNs changes given OOD test data. However, we notice the opposite phenomenon in iWildCam and Amazon. Given ID test data, our approach achieves 0.39 and 0.80 concerning Spearman’s rank-order correlation coefficient for iWildCam and Amazon, respectively. While given OOD test data, the results are 0.91 and 0.71, respectively. In other words, the effectiveness improves on the OOD test data in iWildCam but degrades in Amazon. To make clear the reason behind this, we analyze the accuracy and robustness of multiple DNNs on ID and OOD test data (Table 1), respectively. In iWildCam, the performance difference of its 20 DNNs becomes larger on OOD test data, from 1.54% to 11.52%. In Amazon, the performance of all 20 DNNs degrades, from 74.84% to 72.35%. Besides, the performance difference in Amazon becomes smaller. Therefore, we believe that the model’s ability and the performance difference among DNNs have an impact on the ranking effectiveness, which leads to the investigation in RQ3.

5.3 RQ3: Impact factors
As mentioned in RQ2, by comparing the ranking effectiveness given ID and OOD test data, we raise the demand of investigating the two impact factors, the quality and diversity of multiple DNNs. The quality refers to the model’s performance given the test data and is calculated as the average accuracy or robustness over all DNNs on each dataset. For instance, in MNIST without distribution shift, the quality is the average accuracy of 30 DNNs on the ID test data, and in MNIST-C with Gaussian Noise (severity=1), the quality is the average robustness of 30 DNNs on the corresponding OOD data.

The diversity indicates the performance difference among DNNs and is the standard deviation of accuracy or robustness over all DNNs on each dataset.

Figure 7 plots the distribution of ranking performance (Spearman’s correlation) concerning the quality and diversity. In Figure 7(a), most good rankings happen with a high model quality (greater than 50%). The reason is that in our scenario, we only have the access to the predictions of test data of multiple DNNs, which setups the initial inference of data difficulty and model specialty. Therefore, the learned Bayesian model can be more precise when the qualities of DNNs are high. Furthermore, this also explains why our approach outperforms the selection-based methods. For example, the state-of-the-art SDS selects a few discriminative data to annotate to rank DNNs and the selection of data highly relies on the predicted labels. As a result, since the low qualities of DNNs always give a wrong estimation of the discrimination ability of data, the ranking performance is poorer. For instance, in Java250 and C++1000, SDS only reaches 0.82 and 0.79 on Spearman’s correlation with 20 labeled data, respectively. However, our approach achieves 0.96 and 0.95 in two datasets, respectively, with no labeling effort.

On the other hand, Figure 7(b) reveals that there is a high chance of a good ranking when DNNs are diverse (larger than 18%). Additionally, a poor ranking mostly happens when DNNs are too close to each other, which confirms the result of iWildCam with ID data (Figure 3(d) and Figure 4(d)) that all ranking methods obtain poor ranking.

Answer to RQ3: By investigating the impact factors, model quality and model diversity, of ranking performance, we observe that when the multiple DNNs have high quality (e.g., the average accuracy/robustness is over 50%), the performance of DNNs can be discriminated better. On the other hand, there is a higher chance of a good ranking when DNNs are more diverse (larger than 18%).

6 THREATS TO VALIDITY
The internal threat is mainly due to the implementation of the baseline methods, our proposed approach, and the evaluation metrics. For SDS, we use the original implementation on GitHub provided by Meng et al. [25]. For random sampling and CES, we implement it based on the description in [25] and carefully check the result to be consistent with that in [25]. Regarding the evaluation metrics, we adopt popular libraries, such as SciPy [5].

The external threat comes from the evaluated tasks, datasets, DNNs, and baseline methods. Regarding the classification tasks, we consider three different ones, image, text, and source code. For the datasets, we select the publicly available datasets. In particular, for datasets with the synthetic distribution shift (15 types of natural corruptions) and natural distribution shift, we employ four public benchmarks. Concerning the DNNs, we collect them (either the off-the-shelf models or train with the provided scripts) from different repositories on GitHub. These models are with different architectures and parameters. For the comparison, we consider three sample-selection-based baseline methods and apply different numbers of labeling budgets to imply their performance.

The construct threat mainly lies in the sampling randomness in the baseline methods and the evaluation measures. To reduce the impact of randomness, for each baseline method, we repeat each
Table 4: Spearman’s rank-order correlation coefficient of ranking results based on MNIST-C and CIFAR-10-C. For Random, SD, and CES, we compute the average and standard deviation over all labeling budgets and 50-time experiments. The best performance is highlighted in gray. The values highlighted in yellow are where CES or random outperform SDS. The higher the better.

| Corruption Type | Security-1 | Security-2 | Security-3 | Security-4 | Security-5 |
|----------------|------------|------------|------------|------------|------------|
|                | Random     | CES        | Random     | CES        | Random     | CES        | Random     | CES        | Random     | CES        | Random     | CES        | Random     | CES        | Random     | CES        | Random     | CES        | Random     | CES        |
|                |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |
|                |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |

Table 5: Kendall’s τ of ranking results based on MNIST-C and CIFAR-10-C. For Random, SD, and CES, we compute the average and standard deviation over all labeling budgets and 50-time experiments. The best performance is highlighted in gray. The values highlighted in yellow are where CES or random outperform SDS. The higher the better.

| Corruption Type | Security-1 | Security-2 | Security-3 | Security-4 | Security-5 |
|----------------|------------|------------|------------|------------|------------|
|                |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |
|                |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |             |

experiment concerning the labeling budgets, datasets 50 times and report the results of both average and standard deviation. Since our proposed approach does not rely on sampling data to annotate, there is no sampling randomness. Considering the randomness (gradient ascent search) in the EM algorithm, we repeat our approach 50 times and found that the randomness was negligible (less than 1.8E-03). Regarding the evaluation measures, we consider three popular statistical analyses. The Kendall’s τ rank correlation and Spearman’s rank-order correlation can infer the effectiveness of the methods concerning the general ranking, while the Jaccard similarity can specifically check the performance concerning the top-k ranking. Besides, for the statistical analyses, we report the p-value to demonstrate the significance.
Figure 5: Jaccard similarity of ranking the top-5 DNNs. For Random, SDS, and CES, we report the average results over all labeling budgets. At each corruption, we report the performance of 5 levels of severity (e.g., Gaussian Noise-3). The higher the better.

Figure 6: Spearman’s rank-order correlation coefficient (first row) and Kendall’s $\tau$ (second row) of ranking results based on OOD test data. The higher the better. The shaded area represents the standard deviation. “Budget” is the number of labeled data (only apply to Random, SDS, and CES).

Table 6: Jaccard similarity of ranking the top-$k$ DNNs based on the OOD test data of iWildCam and Amazon with natural distribution shift. For Random, SDS, and CES, we report the average results over all labeling budgets. The best performance is highlighted in gray. The higher the better.

| Jaccard | Dataset       | Random | SDS | CES | Our |
|---------|---------------|--------|-----|-----|-----|
| $k=1$   | iWildCam      | 0.66   | 0.96| 0.68| 1.0 |
|         | Amazon        | 0.1    | 0.22| 0.15| 1.0 |
| $k=3$   | iWildCam      | 0.4    | 0.63| 0.41| 1.0 |
|         | Amazon        | 0.16   | 0.28| 0.21| 1.0 |
| $k=5$   | iWildCam      | 0.44   | 0.61| 0.47| 0.67|
|         | Amazon        | 0.23   | 0.39| 0.29| 1.0 |
| $k=10$  | iWildCam      | 0.62   | 0.83| 0.65| 0.82|
|         | Amazon        | 0.41   | 0.44| 0.45| 0.43|

Figure 7: The impact of model quality/diversity on the ranking performance of our approach. Each blue point indicates the Spearman’s correlation coefficient of a specific dataset and the corresponding DNNs. All 159 datasets are included. For each figure, we annotate the point by the (a) diversity and (b) quality where the correlation is lower than 0.7.

7 CONCLUSION

Observing the limitations (labeling effort, sampling randomness, and performance degradation on out-of-distribution data) of existing selection-based methods, we proposed a labeling-free approach to undertake the task of ranking multiple deep neural networks (DNNs) without the need of domain expertise. The main idea is to build a Bayesian model given the predicted labels of data, which allows for free labeling and non-sampling randomness. The experimental results on various domains (image, text, and source code) and different performance criteria (accuracy and robustness against synthetic and natural distribution shifts) demonstrate that...
our approach significantly outperforms the three baseline methods concerning both Spearman’s correlation and Kendall’s τ. In addition, the results of the Jaccard similarity show the efficiency of our approach in identifying the top-k (k ∈ {1, 3, 5, 10}) DNNs. To promote replication of our study, we make the source code and its documentations available².

Observing the ranking difference on ID and out-of-distribution (OOD) test data, our approach might be useful to detect the existence of distribution shifts. We will consider this in the future work.

REFERENCES

[1] 2018. AIZU online judge. https://judge.u-aizu.ac.jp/judge/ Online, accessed 10 January 2021.
[2] 2021. DNN models for Fashion-MNIST. https://github.com/Tensorflow/Multiple-Model/ Online, accessed 2 December 2021.
[3] 2021. Project website of ranking multiple DNNs. https://sites.google.com/view/ ranking-of-multiple-dns.
[4] 2022. Github. https://github.com/. Online, accessed 25 January 2022.
[5] 2022. Scipy. https://scipy.org/. Online, accessed 27 January 2022.
[6] Rob Alexander, Rob Ashmore, Andrew Banks, Ben Bradshaw, John Bragg, John Tudor, Stuart Tushingham, John Birch, Lavinia Burski, Timothy Coley, Neil Lewis, Ken Neal, Ashley Price, Stuart Reid, and Rod Steel. 2020. Safety-assurance objectives for autonomous systems.
[7] Uni Alon, Meital Zilberstein, Omer Levy, and Eran Yahav. 2019. codezvec: Learning distributed representations of code. Proceedings of the ACM on Programming Languages 3, POPL (2019), 1–29. https://doi.org/10.1145/3290053.
[8] Sara Beery, Elijah Cole, and Arvi Jokka. 2020. The WildCam 2020 Competition Dataset. arXiv preprint arXiv:2004.10340 (2020).
[9] David Berend, Xiaofei Xie, Lei Ma, Lingjun Zhou, Yang Liu, Chi Xu, and Jianjun Zhao. 2020. Cats are not fish: deep learning testing calls for out-of-distribution awareness. Association for Computing Machinery, New York, NY, USA, 1041–1052. https://doi.org/10.1145/3342884.3346109.
[10] Junjie Chen, Zhiou Wu, Zan Wang, Hammo You, Lingming Zhang, and Ming Yan. 2020. Practical accuracy estimation for efficient deep neural network testing. ACM Transactions on Software Engineering and Methodology 29, 4, Article 30 (October 2020), 35 pages. https://doi.org/10.1145/3394112.
[11] W. Wayne Daniel. 1990. Applied nonparametric statistics. PWS-KENT Pub.
[12] A. P. Dempster, N. M. Laird, and D. B. Rubin. 1977. Maximum likelihood from incomplete data via the EM algorithm. Journal of the Royal Statistical Society: Series B (Methodological) 39, 1 (1977), 1–38. https://www.jstor.org/stable/2984875.
[13] Robert L. Ebel. 1954. Procedures for the analysis of classroom tests. A. P. Dempster, N. M. Laird, and D. B. Rubin. 1977. Maximum likelihood from incomplete data via the em algorithm. Journal of the Royal Statistical Society. Series B (Methodological).
[14] Pang Wei Koh, Shiori Sagawa, Henrik Marklund, Sang Michael Xie, Marvin Zhang, Akshay Balasubramanian, Weihu Hu, Michihiro Yasunaga, Richard Lans Phillips, Irena Gao, Tony Lee, Etienne David, Ian Stavness, Wei Guo, Barton E. Ashburn, Imran S. Haque, Sara Beery, Jure Leskovec, Anushl Kushande, Emma Pierson, Sergey Levine, Chelsea Finn, and Percy Liang. 2021. WILDS: A benchmark of in-the-Wild Distribution Shifts. In International Conference on Machine Learning (ICML).
[15] Alex Krizhevsky. 2009. Learning multiple layers of features from tiny images. Technical Report. University of Toronto, Toronto.
[16] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. 1998. Gradient-based learning applied to document recognition. Proc. IEEE 86, 11 (November 1998), 2278 – 2324.
[17] Zenan Li, Xiaoming Ma, Chang Xu, Chun Cao, Jingwei Xu, and Jian Liu. 2020. Boosting operational run testing efficiency through conditioning. In Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2019). Association for Computing Machinery, New York, NY, USA, 499–509. https://doi.org/10.1145/3383690.338390.
[18] Wei Ma, Mike Papadakis, Anestis Tsakmalis, Maxime Cordy, and Yves Le Traon. 2021. Test Selection for Deep Learning Systems. ACM Trans. Softw. Eng. Methodol. 30, 2 (2021), 13:1–13:22. https://doi.org/10.1145/3417330.
[19] Linghan Meng, Yanhui Li, Lin Chen, Zhi Wang, Di Wu, Yunming Zhou, and Baaswen Xu. 2021. Measuring discrimination to boost comparative testing for multiple deep learning models. In IEEE/ACM 43rd International Conference on Software Engineering (ICSE). IEEE Computer Society, Los Alamitos, CA, USA, 385–396. https://doi.org/10.1109/ICSE5024.2021.00045.
[20] Shervin Minaei, Nai Kalchbrenner, Erik Cambria, Narjes Nikzad, Meysmen Chenaghlu, and Jianfeng Gao. 2021. Deep learning–based text classification: a comprehensive review. Comput. Surveys 54, 3 (April 2021). https://doi.org/10.1145/3439726.
[21] Omer Sag and Lior Rokach. 2018. Ensemble learning: a survey. WIREs Data Mining and Knowledge Discovery 8, 4 (2018). https://doi.org/10.1002/widm.1249.
[22] Abhijit Sawant, Pranit Bar, and Pramala Chawan. 2012. Software testing techniques and strategies. International Journal of Engineering Research and Applications (IJERA) 2 (06 2012), 980–986.
[23] PB Selvapriya. 2013. Different software testing strategies and techniques. International Journal of Science and Modern Engineering 2, 1 (2013).
[24] Weijun Shen, Yanhui Li, Lin Chen, Yuanle Han, Tae Son, and Baaswen Xu. 2020. Multiple-source and multi-objective aware testing of neural networks using generative models. In Proceedings of the 22nd International Conference on Neural Information Processing Systems (ICNIP2020). Association for Computing Machinery, New York, United States, 406–422. https://doi.org/10.1145/3394112.
[25] Linghan Meng, Yanhui Li, Lin Chen, Zhi Wang, Di Wu, Yunming Zhou, and Baaswen Xu. 2021. Measuring discrimination to boost comparative testing for multiple deep learning models. In IEEE/ACM 43rd International Conference on Software Engineering (ICSE). IEEE Computer Society, Los Alamitos, CA, USA, 385–396. https://doi.org/10.1109/ICSE5024.2021.00045.
[26] Jacob Whitehill, Paul Ruvelo, Tingfan Wu, Jacob Bergsma, and Javier Movellan. 2009. Whose vote should count more: optimal integration of labels from labelers of unknown expertise. In Proceedings of the 22nd International Conference on Neural Information Processing Systems (NIPS’09). Curran Associates Inc., Red Hook, NY, USA, 2035–2043. https://proceedings.neurips.cc/paper/2009/file/89913dfedfe5059634415e75e70c6dd-Paper.pdf.
[27] Han Xiao, Kashif Rasul, and Roland Vollgraf. 2017. Fashion-MNIST: a novel image dataset for benchmarking machine learning algorithms. arXiv preprint arXiv:1708.07747 (2017). https://arxiv.org/abs/1708.07747.
[28] Jie M. Zhang, Mark Harman, Lei Ma, and Yang Liu. 2019. Machine Learning Testing: Survey, Landscapes and Horizons. CoRR abs/1906.10742 (2019). arXiv:1906.10742. http://arxiv.org/abs/1906.10742.
[29] Lei Chen, Zhao, Chunyuan Liu, and Xiaodong Zhu. 2021. GUIGAN: learning to generate GUI designs using generative adversarial networks. In 2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE). IEEE, 748–760. https://doi.org/10.1109/ICSE5024.2021.00074.

²We will make the implementation publicly available upon acceptance.
[41] Yan Zheng, Yi Liu, Xiaofei Xie, Yepang Liu, Lei Ma, Jianye Hao, and Yang Liu. 2021. Automatic web testing using curiosity-driven reinforcement learning. In 2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE). 423–435. https://doi.org/10.1109/ICSE43902.2021.00048

[42] Yan Zheng, Xiaofei Xie, Ting Su, Lei Ma, Jianye Hao, Zhaopeng Meng, Yang Liu, Ruimin Shen, Yingfeng Chen, and Changjie Fan. 2019. Wuji: automatic online combat game testing using evolutionary deep reinforcement learning. In 2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE). 772–784. https://doi.org/10.1109/ASE.2019.00077