VLATest: Testing and Evaluating Vision-Language-Action Models for Robotic Manipulation

ANONYMOUS AUTHOR(S)*

The rapid advancement of generative AI and multi-modal foundation models has shown significant potential in advancing robotic manipulation. Vision-language-action (VLA) models, in particular, have emerged as a promising approach for visuomotor control by leveraging large-scale vision-language data and robot demonstrations. However, current VLA models are typically evaluated using a limited set of hand-crafted scenes, leaving their general performance and robustness in diverse scenarios largely unexplored. To address this gap, we present VLATest, a fuzzing framework designed to generate robotic manipulation scenes for testing VLA models. Based on VLATest, we conducted an empirical study to assess the performance of seven representative VLA models. Our study results revealed that current VLA models lack the robustness necessary for practical deployment. Additionally, we investigated the impact of various factors, including the number of obstacles, lighting conditions, camera poses, and unseen objects, on the VLA model's performance. Our findings highlight the limitations of existing VLA models, emphasizing the need for further research to develop reliable and trustworthy VLA applications.

CCS Concepts: • **Software and its engineering → Software defect analysis**; • **General and reference → Empirical studies**; • **Computer systems organization → Robotics**.

Additional Key Words and Phrases: Vision-Language-Action Models, Robotic Manipulation, Robustness, Empirical Study

ACM Reference Format:
Anonymous Author(s). 2024. VLATest: Testing and Evaluating Vision-Language-Action Models for Robotic Manipulation. 1, 1 (September 2024), 22 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Robotic manipulation is widely regarded as one of the most important areas within cyber-physical systems (CPS). Over the past few decades, robotic manipulation and its applications have been implemented across various domains, such as industrial automation [20, 25], healthcare [33, 40], and logistics and warehousing [15, 62]. With the rapid advancement of AI techniques, researchers and practitioners have been exploring the integration of AI for planning [27, 60] and control [66, 74] in robotic manipulation. For instance, recent studies have employed deep reinforcement learning for robotics control to enhance the adaptability of the system against unseen scenarios [30, 56].

Meanwhile, the emergence of foundation models, such as large language models (LLMs) and vision-language models (VLMs), has introduced new opportunities for advancing AI-enabled robotic manipulation [16, 63]. In particular, LLMs and VLMs have demonstrated promising capabilities to participate in the loop of robotics system development and operation to enhance corresponding reasoning, perception, and task-planning abilities [18, 35, 47]. In contrast to the general purpose-oriented LLMs and VLMs, vision-language-action (VLA) models were developed exclusively to generate robot actions for manipulation based on visual observations from cameras and task instructions provided in users' natural language input. Techniques such as reinforcement learning

ACM XXXX-XXXX/2024/9-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn

from human feedback (RLHF) [4] further enhance these models' ability to interpret human intent from natural language commands. As a result, it is now possible to let robotics perform manipulation tasks simply by prompting natural language commands into the VLA models. Additionally, the large-scale pre-training nature of such foundation models makes it possible to adapt to a diverse range of downstream manipulation tasks without task- and environment-specific niche design. A recent study demonstrates that the state-of-the-art (SOTA) VLA model, RT-2 [8], can be extended to complex tasks such as reasoning, symbol understanding, and human recognition—tasks that were unseen during training [8].

However, the data-driven nature of VLA models makes them difficult to interpret, which hinders the safety and applicability of VLA models to more robotics applications in practice. To enhance the reliability and trustworthiness of VLA models for robotic manipulation, the development of quality assurance techniques such as testing, debugging, and repairing has become an urgent need in both industrial and academic communities. In particular, comprehensive and adequate testing is essential for throughout assessing a VLA model's capabilities and limitations. Unfortunately, current VLA models are typically evaluated using only a limited set of hand-crafted scenes, where the comprehensiveness and effectiveness of such scenes are often inadequate, which subsequently leaves the general performance and behavior characteristics of VLA models largely unexplored. Moreover, unlike conventional LLMs, which only process Natural Language (NL) text inputs, VLA models are empowered by the multimodality perception ability; therefore, when deploying VLA models in real-world scenarios, visual factors such as obstacles, lighting conditions, and camera angles may significantly impact their performance. Despite this, there is currently a lack of deep understanding regarding the robustness of VLA models against the variations among such environmental factors.

To address this gap, we propose VLATest, one of the first testing frameworks specifically designed for evaluating VLA models in robotic manipulation. We introduce a set of ten testing operators and design a generation-based fuzzing framework that automatically produces testing scenes to assess the performance and robustness of VLA models in specific robotic manipulation tasks. VLATest is implemented within the Maniskill2 simulation environment [26]. By leveraging VLATest, we facilitate efficient testing and enable comprehensive evaluation of VLA models under varying conditions. Based on VLATest, we performed a large-scale empirical study to evaluate the overall performance and robustness of popular VLA models. A set of research questions are proposed to examine key factors in reliable robotic manipulation with VLA: *basic performance*, *task complexity*, *perception robustness*, and *OOD (out-of-distribution) robustness*. Specifically, we investigated the following five research questions:

- RQ1 How do VLA models perform in popular robotic manipulation tasks?
- RQ2 How does the number of obstacles affect a VLA model's performance?
- RQ3 Does the change in lighting conditions affect a VLA model's performance?
- RQ4 Does the change of camera pose affect a VLA model's performance?
- RQ5 How robust do VLA models perform against unseen objects?

To investigate these research questions, we generated 18,604 testing scenes across four different robotic manipulation tasks. We selected *seven* popular publicly available VLA models: RT-1-1k, RT-58k, RT-400k [7], RT-1-X [57], Octo-small, Octo-base [72], and OpenVLA-7b [39]. The experiments included a total of 78,604 rounds of simulation execution, which took more than 400 GPU hours.

Our analysis shows that current VLA models exhibit **subpar performance** across the four robotic manipulation tasks studied. As the number of obstacles increases, it becomes more challenging for these models to accurately locate and manipulate the correct objects. Additionally, we observed that the subject VLA models lack robustness when subjected to changes in lighting conditions and

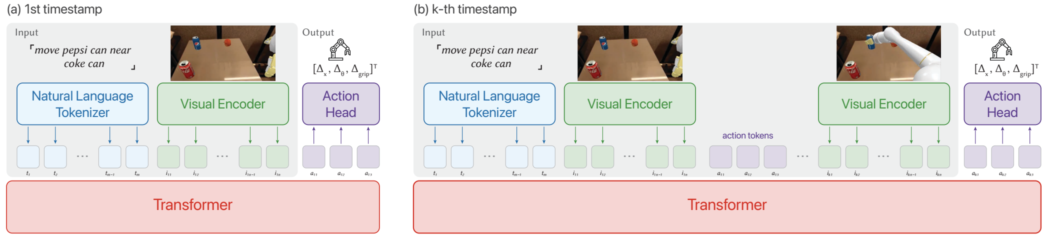


Fig. 1. **Architecture and workflow of a VLA model.** (a) Generating robot actions at the first timestamp. (b) Generating robot actions at the k-th timestamp.

camera angles, performing much worse compared to the default settings. Meanwhile, we found that VLA models with large-scale pre-training generally show better robustness against such changes. Finally, we found that these VLA models struggle significantly with unseen objects, exhibiting a significant drop in performance compared to manipulating seen objects. Our findings provide practical guidelines for developers working with VLA models on specific robotic manipulation tasks and underscore the need for more advanced VLA models, as well as novel quality assurance techniques to enhance the robustness and reliability of the VLA models.

In summary, this paper makes the following contributions:

- **A testing framework.** We designed and implemented a generation-based fuzzing framework, VLATest, to test VLA models by incorporating various operators in robotic manipulation testing scenes.
- **An empirical study.** Based on VLATest, we conducted a large-scale empirical study to evaluate the performance and robustness of seven popular VLA models across four robotic manipulation tasks under various conditions, including variations in the number of obstacles, lighting conditions, camera poses, and the manipulation of both seen and unseen objects.
- **Implications.** We discussed the challenges and limitations of current VLA models, along with the implications and future opportunities for enhancing their robustness and reliability.
- **Artifacts.** Our artifacts, including the replication packages and the generated testing scenes, are available on an anonymous Git repository: https://anonymous.4open.science/r/VLATest-5642.

2 Background: Vision-Language-Action Models

Vision-Language-Action (VLA) models [7, 39, 57, 72] are a type of deep neural network that takes natural language input from the user as task instructions and visual input from a camera as observations. The output of a VLA model is a set of actions to achieve the designated manipulation according to the task instructions, such as moving a robotic arm's joints and opening the gripper.

2.1 VLA Model for Robotic Manipulation

Fig. 1 illustrates the common architecture of a VLA model. Given a natural language input T and an image input I_1 at the first timestamp, the VLA model's natural language tokenizer and visual encoder first project T and I_1 into sets of tokens, $\mathbf{T} = \{t_1, \ldots, t_m\}$ and $\mathbf{I}_1 = \{i_{11}, \ldots, i_{1n}\}$, respectively. These tokens are then concatenated and fed into a transformer model to predict action token(s) $\mathbf{A}_1$. An action head layer then de-tokenizes $\mathbf{A}_1$ into robot action values $[\Delta_{x1}, \Delta_{\theta 1}, \Delta_{grip1}]$, where $\Delta_{x1} \in \mathbb{R}^3$, $\Delta_{\theta 1} \in \mathbb{R}^3$, and $\Delta_{grip1} \in \mathbb{R}^1$ denote the translation (x, y, z movement), rotation, and gripper actions of the end-effector that should be performed after the observation, respectively.

After the robot performs these actions, the action tokens $\mathbf{A}_1$ and a new set of image tokens $\mathbf{I}_2 = \{i_{21}, \ldots, i_{2n}\}$, based on the visual observation at the next timestamp, are concatenated with $\mathbf{T}$

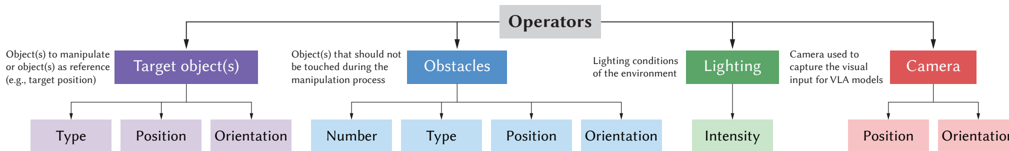


Fig. 2. Operators used for testing VLA models in VLATest.

and $\mathbf{I}_1$. A new input sequence $\{\mathbf{T}, \mathbf{I}_1, \mathbf{A}_1, \mathbf{I}_2\}$ is then fed into the transformer to predict new action tokens $\mathbf{A}_2$. The VLA model continues this process until the task is completed or the pre-defined maximum number of steps is exceeded.

2.2 Training and Evaluation of the VLA Model

Training. There are typically two approaches to training a VLA model: (1) training from scratch and (2) fine-tuning a general-purpose vision-language model (VLM). *Training from scratch* involves building a VLA model directly on robot demonstration data. This approach is commonly applied for models with relatively small-scaled architectures and limited computational resources, such as RT-1 [7] and Octo [72], which typically have fewer than 100 million parameters. By contrast, fine-tuning from an existing VLM leverages the flexibility of re-using a larger model (more than 1 billion parameters), such as Llava [39, 50], which has been pre-trained on massive amounts of image and text data from diverse domains. The large-scale pre-training of these VLMs may enhance the generalizability of the fine-tuned VLA models, particularly when manipulating unseen objects and tasks.

Evaluation. A VLA model is usually evaluated by measuring its performance on specific skills, such as picking up an object in a scene. To evaluate a particular skill, developers must first create an adequate testing scene, which involves configuring target objects, obstacles, and environmental factors like lighting conditions. Additionally, a text prompt should be meticulously crafted before executing the VLA model to perform the manipulation task. To assess the model's performance, developers usually design a set of evaluation metrics. For instance, when performing the task "picking up an object", the metrics might include: (1) whether the robot grasps the correct object, (2) whether the object is successfully lifted, and (3) whether the robot can sustain lifting the object for a short period. The execution of the VLA model and the robot can occur in either a simulated or real-world environment. In real-world scenarios, manual labeling is required to compute these metrics, whereas, in simulated environments, the evaluation process can be automated.

3 VLATest

In this section, we first introduce the operators included in the testing scene for a robotic manipulation task. Next, we describe the algorithm used to generate a testing scene in VLATest.

3.1 Operators

We consider **four** categories of testing operators in VLATest as shown in Fig. 2, resulting in a total of ten testing operators.

- ***Target object(s).*** A target object refers to an object that is required to be manipulated in a task (e.g., an object to pick up) or an object that serves as a reference in a task (e.g., an object to be placed on). For each target object, we consider three different operators: (1) type of object (e.g., *Pepsi can*), (2) position, and (3) orientation.
- ***Obstacles.*** Different from *target object(s)*, obstacles are typically not part of the task, and the robot is expected to avoid contacting these objects during manipulation. In addition to the three

Algorithm 1: Testing scene generation in VLATest.

```
Input: an object database O, the robotic manipulation task T, the
       number of target objects N_target, the number of obstacles
       N_obstacles, the lighting mutation option lighting_flag,
       and the camera mutation option camera_flag, the
       minimum distance between objects safe_dist
Output: a testing scene
1  O ← random_shuffle(O);
2  O_target, O_obstacles ← ∅, ∅;
3  intensity, cam_pos, cam_ori ← default values;
4  while not semantic_valid(O_target, T) do
5  |  for i in 1, ..., N_target do
6  |  |  obj ← O.pop();
7  |  |  pos, ori ← pose_sampler(O_target, safe_dist);
8  |  |  O_target ← O_target ⋃(obj, pos, ori);
9  |  end
10 end
11 if N_obstacles > 0 then
12 |  for i in 1, ..., N_obstacles do
13 |  |  obj ← O.pop();
14 |  |  pos, ori ← pose_sampler(O_target ⋃ O_obstacles,
   |  |    safe_dist);
15 |  |  O_obstacles ← O_target ⋃(obj, pos, ori);
16 |  end
17 end
18 if lighting_flag then
19 |  intensity ← mutate_lighting(intensity);
20 end
21 if camera_flag then
22 |  cam_pos, cam_ori ← mutate_camera(cam_pos, cam_ori);
23 end
24 return {O_target, O_obstacles, intensity, (cam_pos, cam_ori)};
```

operators for *target object(s)*, we also consider the number of obstacles as a distinct operator in the obstacles category.

- ***Lighting.*** The lighting condition affects the rendering of images captured by the camera, thereby influencing the visual input of the VLA models. In VLATest, we consider lighting intensity as one of the operators.
- ***Camera.*** The camera's pose can also affect the visual input of the VLA models. We consider its position and orientation as two separate operators in VLATest.

3.2 Testing Scene Generation

We summarize the algorithm for generating a testing scene in Algorithm 1. Intuitively, there are four distinct steps: (1) sampling semantically valid target object(s), (2) sampling obstacles (optional), (3) mutating lighting conditions (optional), and (4) mutating camera poses (optional).

Sampling semantically valid target object(s). For a robotic manipulation task, we first randomly sample target object(s) without replacement from the object database O (Lines 5-9). We also check if the selected objects are *semantically valid* according to the task requirements (Line 4). For example, in a task requiring object A to be placed over object B, if object B is a ball, object A can never be stably placed on it. Such cases are considered semantically invalid. After selecting the target object(s), we proceed to sample their positions and orientations (Line 7). In our empirical study, we used a random sampler for pose selection. If there are multiple target objects, we ensure they remain far enough apart ($> safe\_dist$) to avoid generating invalid testing scenes. For instance, in the previous example, if object A is already placed on object B during the sampling of their positions, the testing scene becomes invalid.

Sampling obstacles. If the number of obstacles $N_{obstacles}$ is greater than 0 (Line 11), we further randomly sample obstacle objects from O without replacement (Lines 12-16). For each obstacle, we follow the same procedure as used for sampling the target objects to assign their position and orientation (Line 14). In our empirical study, we utilized a random sampler to generate the position and orientation for each obstacle.

Mutating lighting conditions and camera poses. For lighting conditions, we generate a factor α to mutate the lighting intensity value (Lines 18-20). For the camera, we adjust its position by a distance d and rotate it by an angle θ (Lines 21-23). Note that both d and θ are kept small to ensure that the entire scene remains within the camera's view. In our empirical study, we used a random generator to generate α, d, and θ within specified ranges.

4 Empirical Study

Based on VLATEST, we conducted an empirical study to investigate the performance of SOTA VLA models. In this section, we first list our research questions, followed by the empirical setup, which includes subject VLA models, subject robotic manipulation tasks, prompt template, and implementation details.

4.1 Research Questions

Our empirical study investigates the following research questions to examine the key factors in reliable robotic manipulation: *basic performance* (RQ1), *task complexity* (RQ2), *perception robustness* (RQ3 & RQ 4), and *OOD robustness* (RQ5).

- ***RQ1. How do VLA models perform in popular robotic manipulation tasks?***
  This research question seeks to evaluate the performance of SOTA VLA models in various robotic manipulation tasks. While previous studies [7, 72] typically rely on a few hand-crafted test cases, we use VLATEST to generate a large number of test cases. This approach enables a more comprehensive assessment of SOTA VLA models' performance, providing insights into current challenges and opportunities.
- ***RQ2. How does the number of obstacles affect a VLA model's performance?***
  Intuitively, the presence of more obstacles (i.e., objects unrelated to the assigned manipulation task) increases the complexity of a robotic manipulation task for VLA models. However, it remains unclear whether there is an upper limit to the task complexity that a VLA model can handle effectively. To address this, we conduct controlled experiments to help practitioners understand how VLA models perform as the number of obstacles varies.
- ***RQ3. Does the change in lighting conditions affect a VLA model's performance?***
  When deploying robotics and VLA models in real-world environments, external conditions can vary significantly. Ideally, a VLA model should be robust against different lighting conditions, such as varying illumination intensities. This research aims to offer practitioners practical guidelines on the robustness of VLA models under diverse lighting setups.
- ***RQ4. Does the change of camera pose affect a VLA model's performance?***
  Since VLA models are pre-trained on large-scale vision datasets, they are expected to demonstrate robustness when input images are captured from various angles. This research question seeks to determine whether and to what extent current VLA models maintain robustness when operating with different camera poses.
- ***RQ5. How robust do VLA models perform against unseen objects?***
  Objects that were unseen in the robotic demonstration data may present when deploying robotics and VLA models in practical scenarios. It is unclear whether the large-scale pre-training of VLA models can make it generalizable to these unseen objects. Also, there is currently limited understanding of the performance gap between seen-object and unseen-object robotic manipulation tasks. To address this, we investigate this research question by leveraging an external object database to assess the limitations and challenges.

4.2 Subject VLA Models

To investigate our research questions, we studied four different series of open-source VLA models: RT-1 [7], RT-1-X [57], Octo [72], and OpenVLA [39]. For RT-1 [7], we studied three publicly available variants: *RT-1-1k*, *RT-1-58k*, and *RT-1-400k* [1]. We also studied two variants for Octo [72]: *Octo-small* and *Octo-base*. Note that, we were unable to study the SOTA VLA model, RT-2 [8], as it has not

[1]The number denotes the training steps taken for training an RT-1 model.

Table 1. Overview of subject VLA models.

VLA Models	RT-1			RT-1-X	Octo-small	Octo-base	OpenVLA-7b
	1k	58k	400k				
Model Size	35M			35M	27M	93M	7.6B
Release Date	Dec. 2022			Oct. 2023	Dec. 2023	Dec. 2023	Jun. 2024

yet been made publicly available. Thus, we included a total of seven subject VLA models in our empirical study. Table 1 summarizes the characteristics of these models, and we provide more details for each model below.

- **RT-1** [7] model was released by Google Research. The RT-1 model includes a FiLM EfficientNet-B3 [59, 71] pre-trained on the ImageNet dataset [61] for tokenizing visual inputs and language instructions before connecting to a transformer to generate robotic manipulation actions. The RT-1 model was trained on an unpublished set of 130k robot demonstrations collected by Google.
- **RT-1-X** [57] model was released by Google DeepMind. RT-1-X shares the same model architecture as RT-1. However, RT-1-X was trained on the open-source dataset, Open X-Embodiment [57], which includes 160k robot demonstrations collected from 22 different robots.
- **Octo** [72] model, released by UC Berkeley, includes a ViT model [17] as its backbone transformer. It introduces the "readout" token, allowing developers to flexibly add new observation inputs or action output heads to the model during downstream fine-tuning. Octo was trained on a subset of the Open X-Embodiment dataset, which includes about 65k robot demonstrations. Octo-small (27M parameters) and Octo-base (93M parameters) are two variants of Octo, utilizing ViT-S and ViT-B as their backbone transformers, respectively.
- **OpenVLA-7b** [39] is the most recent VLA model released by Stanford University. OpenVLA-7b includes a 600M-parameter visual encoder consisting of pre-trained SigLIP [88] and DinoV2 [55] models and a 7B-parameter Llama 2 [73] as the language model backbone. OpenVLA-7b was then fine-tuned on the Open X-Embodiment dataset.

4.3 Robotic Manipulation Tasks

We included four different robotic manipulation tasks in our study. Now we briefly introduce each of them. We also refer to the supplementary materials for the video demo of each task.

- ***Task 1: Pick up an object.*** This task requires a VLA model to identify the target object and generate the appropriate control signals to grasp and lift it. To succeed, the robotic must grasp the correct object and lift it at least 0.02 meters for five consecutive frames.
- ***Task 2: Move object A to object B.*** This task requires a VLA model to first identify the source object (A) and then output the corresponding control signals to move it near the target object (B). To succeed, the robotic must move the correct object to within 0.05 meters of the target object.
- ***Task 3: Put object A on top of object B.*** Different from Task 2, this task requires the VLA model to output control signals that could stack object A on top of object B. To succeed, object A should be placed stably on top of object B.
- ***Task 4: Put object A into object B.*** Different from Task 3, this task requires the VLA model to generate control signals that place object A inside object B (e.g., into a kitchen sink or a basket). To succeed, object A must be completely inside object B.

4.4 Prompt Templates

For each task, we follow the previous work [7, 39, 43, 57] to use the standard prompt template for each task: (1) `pick up [object name]`, (2) `move [object name] near [object name]`, (3) `put [object name] on [object name]`, and (4) `put [object name] into [object name]`.

Table 2. (**RQ1**) Performance of seven subject VLA models on different manipulation tasks. The top-1, top-2 and top-3 success rates for each step and task are highlighted, respectively.

VLA Models	Task 1: Pick Up			Task 2: Move Near			Task 3: Put On			Task 4: Put In		
	Grasp	Lift	Success	Grasp	Move	Success	Grasp	Move	Success	Grasp	Move	Success
RT-1-1k	10.1%	1.2%	0.7%	9.6%	3.2%	1.4%	0.4%	0.0%	0.0%	1.1%	0.0%	0.0%
RT-1-58k	44.5%	32.6%	28.2%	38.6%	25.2%	10.9%	0.3%	0.0%	0.0%	1.3%	0.0%	0.0%
RT-1-400k	48.4%	41.0%	34.4%	38.8%	23.7%	9.4%	10.4%	1.3%	0.5%	8.9%	0.1%	0.1%
RT-1-X	34.0%	25.8%	19.5%	25.4%	15.2%	5.8%	17.2%	4.4%	2.3%	17.8%	0.7%	0.4%
Octo-small	9.0%	2.0%	0.8%	14.8.9%	4.1%	1.5%	27.5%	4.6%	2.2%	34.6%	1.1%	1.1%
Octo-base	2.3%	0.4%	0.0%	4.9%	1.5%	0.6%	19.1%	2.6%	1.2%	32.5%	1.1%	1.1%
OpenVLA-7b	15.1%	7.1%	5.9%	43.0%	23.3%	12.7%	36.8%	5.4%	2.1%	19.9%	1.1%	1.1%
Avg.	23.3%	15.7%	12.8%	25.0%	13.7%	6.0%	16.0%	2.6%	1.2%	16.6%	0.6%	0.5%

4.5 Implementation Details

We conducted all experiments on a server with an AMD 5955WX CPU and two NVIDIA RTX A6000 GPUs. The operating system is 64-bit Ubuntu 20.04 LTS with Python 3.10 and CUDA 12.2. We implemented VLATest with Maniskill2 simulation environments [26, 43]. We used two object databases: (1) the default object database in Maniskill2 ($N = 18$) in RQ1 ~ RQ4, and (2) YCB object database ($N = 56$) in RQ5. The average execution time of one manipulation task was around 19.8 seconds. Our empirical study took about 410 GPU hours in total.

5 Results

5.1 RQ1: How Do VLA Models Perform in Popular Robotic Manipulation Tasks?

To investigate this research question, we leveraged VLATest to generate 1,000 scenes for each of the four robotic manipulation tasks by randomly selecting target object(s) and sampling 0 to 3 obstacles. We also randomly assigned poses to these objects. To avoid collision overlaps, we maintained a minimum distance of 0.15 meters between objects during the assignment. The default lighting setups and camera poses were used for this RQ.

Table 2 presents the performance of seven VLA models on these tasks and scenes. Overall, we find that current VLA models do not perform well in the four studied robotic manipulation tasks. The average success rates across the seven VLA models for the four tasks are 12.4%, 6.0%, 1.2%, and 0.5%, respectively. In Task 1, the best-performing VLA model, RT-1-400k, succeeded in only 34.4% of the test scenes. We also observed significant performance drops in Task 2, Task 3, and Task 4 compared to Task 1. The best-performing VLA model in Task 2, OpenVLA-7b, completed only 12.7% of the test scenes. In Task 3 and Task 4, the best-performing VLA models (RT-1-X and Octo-small) achieved success rates of just 2.2% and 2.1%, respectively. One possible reason is that these three tasks are more complex than Task 1, as they require multiple steps of reasoning (i.e., identifying the source and target objects and their positions before generating the corresponding control signals). Among the seven VLA models studied, we did not find any model that performed significantly better than the others across different tasks.

Finding 1

All VLA models exhibit ***subpar performance*** *in the four studied robotic manipulation tasks, particularly in those that require identifying multiple target objects (i.e., Task 2, Task 3, and Task 4). These results suggest that the development of VLA models is still in its early stages, as they are far from being ready for deployment in real-world scenarios.*

To understand the rationale behind the subpar performance of these VLA models, we broke down each testing scene according to the different steps required to complete a task successfully. Specifically, we measured the success rates of each step in a testing scene for the four tasks, as

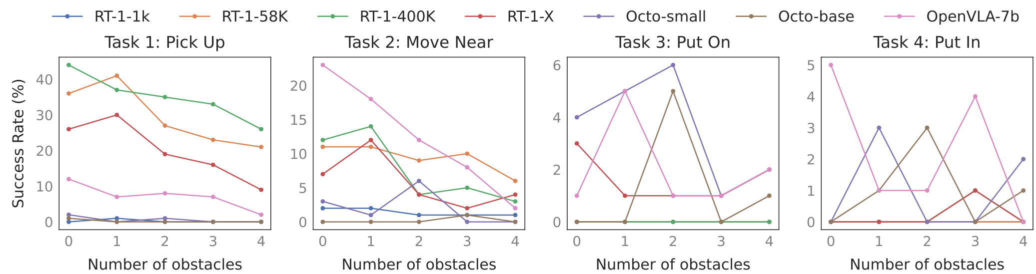


Fig. 3. (**RQ2**) VLA performance vs. the number of obstacles.

presented in Table 2. For instance, Task 1 requires the robot to (1) grasp the target object (the column *Grasp* in Table 2), (2) lift the object significantly (the column *Lift* in Table 2), and (3) continue lifting for five consecutive frames (the column *Success* in Table 2). In all four tasks, we found that the success rates dropped significantly between steps. For example, in Task 1, the average success rate of correctly grasping the target object is 23.3%. The success rates for lifting and maintaining the lift then drop to 15.7% and 12.4%, respectively. These results indicate that the current VLA models struggle to interpret natural language instructions that require the robot to perform multiple sequential actions.

In Task 2, Task 3, and Task 4, VLA models successfully picked up source objects in 16% to 25% of scenes. However, they then failed to identify the target objects, with only 0.6% to 13.7% of objects being correctly moved and 0.5% to 6.0% of objects being correctly placed. To improve, one could consider the idea of *chain-of-thought* prompting in LLMs. Specifically, the complex task instructions could be decoupled into individual action steps, allowing the VLA model to be prompted step-by-step.

Finding 2

Current VLA models cannot successfully execute designated task instructions that require multiple steps of action, highlighting the urgent need to improve their capabilities in accurately interpreting natural language prompts.

5.2 RQ2: How Does the Number of Obstacles Affect a VLA Model's Performance?

To investigate RQ2, we used VLATest to generate 100 scenes for each task with a fixed number of n obstacles, where n was set to 0, 1, 2, 3, and 4, resulting in a total of 500 scenes per task. We used the default lighting conditions and camera poses when investigating this research question.

The results are depicted in Fig. 3. In the first two tasks (i.e., Task 1 and Task 2), we observed that the VLA model's success rate decreased as the number of obstacles increased. The average success rates across different VLA models and scenes dropped from 17.3% to 8.3% and from 8.3% to 1.1% when increasing the number of obstacles from 0 to 4 in Task 1 and Task 2, respectively. However, in Task 3 and Task 4, we did not find a similar pattern. This may be because all VLA models performed poorly even without any obstacles ($n = 0$). The average success rates across different VLA models and scenes were 1.2% and 0.7% when $n = 0$ and 1.1% and 0.4% when $n = 4$ for Task 3 and Task 4, respectively.

Finding 3

The number of obstacles affects the VLA model's performance, indicating that VLA models become unreliable in more complex environments. When there were four obstacles presented in the scene, the VLA models only passed 8.2%, 2.3%, 1.0%, and 0.4% of the test scenes in Task 1, Task 2, Task 3, and Task 4, respectively.

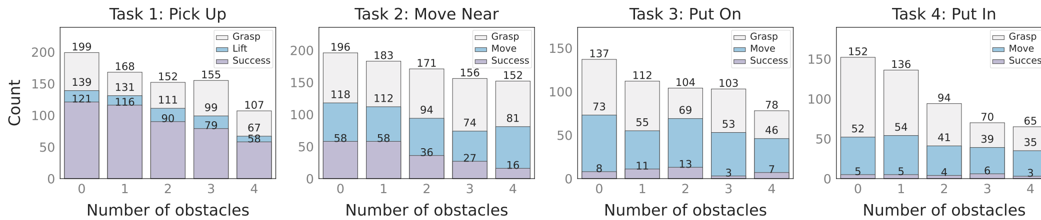


Fig. 4. (**RQ2**) The number of successful testing scenes at different steps vs. the number of obstacles.

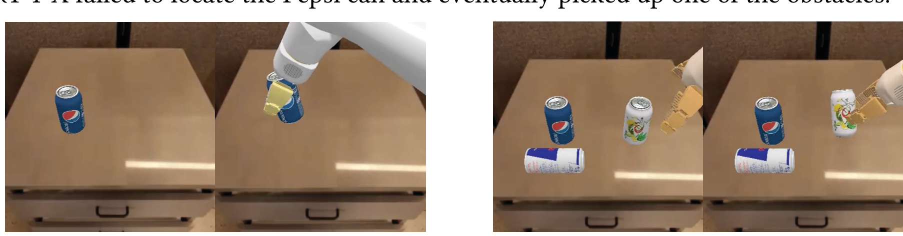
Similar to RQ1, we also analyzed each testing scene and its success at each individual step. We counted the number of testing scenes that succeeded at each step and presented the results in Fig. 4. We found that the major challenge faced by the current VLA models lies in their inability to identify the correct object to manipulate.

In all four tasks, we found that the success rates for grasping the target object decreased as the number of obstacles increased. These results indicate that when there are multiple obstacles, the VLA models struggle to locate the correct object to manipulate. Specifically, without any obstacles, the VLA models successfully located the object to manipulate in 199, 196, 137, and 152 out of 700 cases for Task 1, Task 2, Task 3, and Task 4, respectively. However, with four obstacles, the VLA models successfully located the correct object in only 107, 152, 78, and 65 out of 700 cases for the four tasks, respectively. The average success rates of grasping across VLA models dropped to 53.7%, 77.6%, 47.4%, and 42.8% for four tasks, respectively.

Finding 4

With multiple obstacles in the scene, the VLA models' ability to accurately locate the correct object to manipulate can be significantly affected.

Fig. 5 shows two different testing scenes of Task 1. In both scenes, the VLA model, RT-1-X, was asked to pick up the *Pepsi can*. When there was no obstacle (Fig. 5a), RT-1-X was able to successfully grasp and lift the coke can. However, when there were two other obstacles (i.e., *7up can* and *Redbull can*), RT-1-X failed to locate the Pepsi can and eventually picked up one of the obstacles.



(a) No obstacles (b) Two obstacles

Fig. 5. RT-1-X perform Task 1 with different number of obstacles.

5.3 RQ3: Does the Change in Lighting Conditions Affect a VLA Model's Performance?

To answer this research question, we first collected all the successfully executed scenes for each VLA model in RQ1, resulting in a total of 1,434 passed test cases. We then re-executed these test cases three times after randomly increasing or decreasing the lighting intensities ($N = 4,302$). Specifically, we randomly sampled a factor $\alpha \in (1, 20]$ for increasing or $\alpha \in [1/20, 1)$ for decreasing the lighting intensity. This factor was then multiplied by the default lighting intensity used in RQ1. We manually checked the cases when α was set to 20 and 1/20 and confirmed that the images captured under such lighting conditions were still recognizable by the humans.

We present the experiment results in Table 3. Overall, we found that randomly perturbing the lighting conditions significantly affected the performance of the VLA models. Out of 1,434 passed

Table 3. (**RQ3**) Performance of subject VLA models under default (**Def.**) and mutated (**Mut.**) lighting conditions. Each cell represents the number of successfully passed test scenes by different VLA models in different tasks. The top-1, top-2 and top-3 robust VLA models are highlighted, respectively.

VLA Models	**Task 1 Pick Up**		**Task 2 Move Near**		**Task 3 Put On**		**Task 4 Put In**		**Overall**		
	Def.	Mut.†	Def.	Mut.†	Def.	Mut.†	Def.	Mut.†	Def.	Mut.†	Mut./Def. (%)
RT-1-1k	7	0.7	14	14.0	0	—	0	—	21	14.7	70.0%
RT-1-58k	282	142.0	109	109.0	0	—	0	—	491	251.0	51.1%
RT-1-400k	344	163.0	94	92.0	5	5.0	1	1.0	444	261.0	58.8%
RT-1-X	195	77.3	58	57.0	22	20.7	4	3.0	279	158.0	56.6%
Octo-small	8	0.0	15	2.3	21	6.0	10	1.0	54	9.3	17.2%
Octo-base	0	—	6	1.7	11	3.0	11	0.7	28	5.4	19.3%
OpenVLA-7b	59	21.0	127	127.0	20	20.0	11	11.0	217	169.0	77.9%
Tot.	895	404.0	423	403.0	79	54.7	37	16.7	1434	878.4	61.3%

† Averaged results over three mutations.

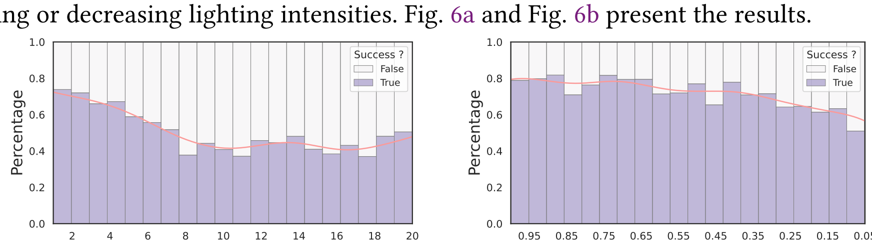
test cases with default lighting conditions, only 878.4 test cases (average results over three mutations for each test case) could still be successfully executed with perturbed lighting conditions. The perturbed lighting conditions had a significant impact on Task 1, Task 3, and Task 4, where only about half of the test cases could still be passed after the perturbation. In Task 2, however, five out of seven VLA models exhibited robust performance despite changes in lighting conditions.

Among the seven VLA models, we found that OpenVLA-7b was the most robust, with 77.9% of the test cases still being passed under mutated lighting conditions. A plausible explanation is that OpenVLA-7b leverages two vision models (i.e., SigLIP [88] and DinoV2 [55]) pre-trained on a diverse set of images and fine-tuned on the LLaVA 1.5 data mixture (1 million images and texts). As a result, OpenVLA-7b can effectively interpret images captured under varying lighting conditions. In contrast, Octo-small and Octo-base were trained solely on images captured from robot demonstrations, making them less robust when faced with lighting conditions different from the default ones. Only 17.2% and 19.3% of the test cases could still be successfully executed after changing the lighting conditions, respectively.

Finding 5

Overall, the VLA models are not sufficiently robust against changes in lighting conditions. Only 61.3% of the test cases could still be successfully executed under mutated lighting conditions. Among the seven VLA models, OpenVLA-7b demonstrated the highest robustness to changes in lighting conditions.

We further investigated the extent to which the VLA models' performance could be affected by increasing or decreasing lighting intensities. Fig. 6a and Fig. 6b present the results.



(a) Increasing the lighting intensity (b) Decreasing the lighting intensity

Fig. 6. VLA performance vs. different lighting intensities.

Increasing the lighting intensity ($\alpha > 1$). Even when the lighting intensity is increased by less than 2.5 times (i.e., $\alpha < 2.5$) of the default value, the success rate of the VLA models immediately drops to around 0.7. These results indicate that even a small increase in lighting intensity can

Table 4. (**RQ4**) Performance of subject VLA models with default (**Def.**) and mutated (**Mut.**) camera poses. Each cell represents the number of successfully passed test scenes by different VLA models in different tasks. The top-1, top-2 and top-3 robust VLA models are highlighted, respectively.

VLA Models	**Task 1 Pick Up**		**Task 2 Move Near**		**Task 3 Put On**		**Task 4 Put In**		**Overall**		
	Def.	Mut.†	Def.	Mut.†	Def.	Mut.†	Def.	Mut.†	Def.	Mut.†	Mut./Def. (%)
RT-1-1k	7	0.7	14	4.3	0	—	0	—	21	5.0	23.8%
RT-1-58k	282	121.3	109	27.0	0	—	0	—	491	39.3	30.2%
RT-1-400k	344	180.3	94	21.3	5	0.0	1	0.7	444	202.3	45.6%
RT-1-X	195	43.0	58	13.3	22	0.7	4	0.0	279	57.0	20.4%
Octo-small	8	0.3	15	3.3	21	1.0	10	0.3	54	4.9	9.1%
Octo-base	0	—	6	0.7	11	1.7	11	0.3	28	2.7	9.6%
OpenVLA-7b	59	20.7	127	44	20	3.0	11	0.3	217	68.0	31.3%
Tot.	895	366.3	423	113.9	79	6.4	37	1.6	1434	488.2	34.0%

† Averaged results over three mutations.

significantly degrade the performance of the VLA models. As the factor α increases, the success rate of the VLA models continues to decrease. In extreme cases (e.g., $\alpha > 7.5$), the VLA models succeed in less than half of the scenes.

Finding 6

The performance of the VLA models degrades with increasing lighting intensity. When the lighting intensity exceeds 8 times of the default value, the VLA models succeed in only about 40% of the testing scenes that could be passed under default lighting conditions.

Decreasing the lighting intensity **(**$\alpha < 1$**).** Similar to increasing the lighting intensity, the VLA models' performance is also affected by even a small perturbation (e.g., $\alpha > 0.9$) when decreasing the intensity. The VLA models' performance degrades with decreasing α. However, compared to increasing the lighting intensity, decreasing it has less significant effects on the models' performance. When $\alpha < 0.2$, the VLA models can still pass around 60% of the testing scenes.

Finding 7

The effect of decreasing the lighting intensity is less significant than increasing it on the VLA models' performance. Even when the lighting intensity is reduced to 0.15 of its default value, the VLA models can still pass 60% of the test cases.

5.4 RQ4: Does the Change of Camera Pose Affect a VLA Model's Performance?

Similar to RQ3, we re-executed the 1,434 passed test cases collected from RQ1 three times after randomly moving and rotating the camera from its default position ($N = 4,302$). Specifically, we rotated the camera around each axis by an angle randomly sampled between $-5°$ and $5°$. Additionally, we randomly moved the camera away from its center by a distance randomly sampled between 0 and 5 cm. We manually checked the corner cases where the camera was rotated by $5°$ and moved by 5 cm and confirmed that the images captured with these camera angles still included the entire scene and objects. We report our experiment results in Table 4

Overall, we found that the VLA model's performance was greatly affected by the mutated camera poses. With mutated camera poses, the subject VLA models only passed 34.0% of the test cases that could be passed with default camera poses. These results indicate that the current VLA models are very sensitive to the camera's extrinsic calibration results. When deploying VLA models, to achieve compatible performance, the developers need to carefully set up the camera poses, as in the robot demonstration data used for training. However, these may limit the generalizability of the

Table 5. (**RQ5**) Performance of subject VLA models with seen/unseen objects. Each cell in the column *Seen* and *Unseen* represents the success rate of different VLA models in different tasks. Darker the color, larger the negative differences between the performance on seen and unseen objects.

VLA Models	**Task 1: Pick Up**			**Task 2: Move Near**			**Task 3: Put On**			**Task 4: Put In**		
	Seen	Unseen	Diff.†	Seen	Unseen	Diff.†	Seen	Unseen	Diff.†	Seen	Unseen	Diff.†
RT-1-1k	0.7%	1.4%	+100.0%	1.4%	0.9%	-35.7%	0.0%	0.0%	—	0.0%	0.0%	—
RT-1-58k	28.2%	5.0%	-82.3%	10.9%	3.9%	-64.2%	0.0%	0.0%	—	0.0%	0.0%	—
RT-1-400k	34.4%	10.3%	-70.1%	9.4%	2.9%	-69.2%	0.5%	0.4%	-20.0%	0.1%	0.1%	—
RT-1-X	19.5%	3.0%	-84.6%	5.8%	1.3%	-77.6%	2.3%	0.6%	-73.9%	0.4%	0.7%	+75.0%
Octo-small	0.8%	0.1%	-88.9%	0.8%	1.5%	+87.5%	2.2%	0.9%	-59.1%	1.1%	0.8%	-27.3%
Octo-base	0.0%	0.0%	—	0.6%	0.4%	-33.3%	1.2%	0.2%	-83.3%	1.1%	0.5%	-54.5%
OpenVLA-7b	5.9%	3.5%	-40.7%	12.7%	2.8%	-78.0%	2.1%	0.9%	-57.1%	1.1%	1.0%	-0.9%
Avg.	12.8%	3.3%	-74.2%	6.0%	2.0%	-66.7%	1.2%	0.4%	-66.7%	0.5%	0.4%	-20.0%

† Diff. = (Unseen - Seen) / Seen

VLA models. Future work may consider data augmentation to improve the VLA model's robustness under different camera settings to enhance generalizability.

Finding 8

Current VLA models are not robust against mutated camera poses, resulting in degraded performance when the visual input is captured from an angle varied from the default one. When rotating the camera for a maximum angle of 5° and moving it for a maximum distance of 5cm, the performance dropped to 34.0% of the performance on average with default camera poses.

Among seven subject VLA models, the most robust one, RT-1-400k, succeeded in 45.6% of the test cases with the mutated camera poses that were passed with the default camera poses. OpenVLA-7b also passed 31.3% of the test cases. We noticed a significant performance gap between two Octo models and other VLA models, where both two Octo models only passed less than 10% of the test cases while the other five models all passed more than 20% of the test cases. These results may have been largely attributed to the fact that Octo models used the smaller training dataset (~ 65K robot demonstrations) compared with the other ones (130K ~ 160K robot demonstrations). As a result, the Octo model's generalizability to visual inputs captured from different camera angles is significantly affected.

Finding 9

Among seven subject VLA models, RT-1-400k was the most robust one against the perturbation of camera poses. Octo-series models performed significantly less robustly than the other models. This may be largely attributed to the fact that Octo models were trained with only half of the robot demonstration data compared with the other subject models.

5.5 RQ5: How Robust Do VLA Models Perform Against Unseen Objects?

To investigate this research question, we used an external object dataset, YCB [9]. YCB contains 56 objects that are not included in the Open-Embodiment-X dataset (the training/fine-tuning dataset of our seven subject VLA models). Similar to RQ1, we leveraged VLATest to generate 1,000 testing scenes for each of the four subject robotic manipulation tasks while sampling the target object and the obstacles from the YCB dataset. We compared the performance of these subject VLA models with objects from YCB dataset to the results in RQ1.

Table 5 shows the performance of seven subject VLA models when manipulating seen and unseen objects. Overall, when manipulating with unseen objects, the performance of subject VLA models

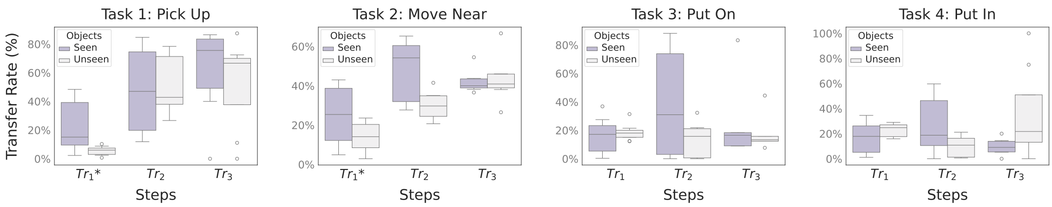


Fig. 7. (**RQ5**) Transfer rate (Tr) of each task when manipulating with seen/unseen objects. Entries with * mean that their mean differences are statistically significant ($p < 0.05$).

dropped significantly compared with manipulating with seen objects. The average performance across different VLA models dropped by 74.2%, 66.7%, 66.7%, and 20.0% in Task 1, Task 2, Task 3, and Task 4, respectively. Notably, we also found that none of these VLA models completely failed when manipulating unseen objects (except those that also failed with seen objects). These results suggest that, while all VLA models exhibit certain possibilities of generalizing themselves to unseen objects, the performance is by far unreliable.

Finding 10

Current VLA models, though exhibit potential for generalization, are still unreliable for handling manipulation tasks with unseen objects. Our subject VLA models saw a performance drop ranging from 20.0% to 74.2% across four tasks when manipulating unseen objects compared with the seen objects.

We also examined each testing scene and the success of the VLA model at every individual step, similar to the investigation of RQ1 and RQ2, to understand how unseen objects might have impacted its performance. Specifically, since the model must succeed at each step sequentially to complete the testing scene, we define a metric called the **transfer rate** (Tr), which calculates the model's ability to transfer success from one step to the next, as follows.

$$Tr_n = \frac{Success\_rate_n}{Success\_rate_{n-1}}, \tag{1}$$

where $Success\_rate_n$ denotes the success rate of a task at step n. We define $Success\_rate_0 = 1000$.

We present the results in Fig. 7. We also performed a paired t-test to examine the statistical differences between Tr of seen and unseen objects. Overall, though Tr_1, Tr_2, and Tr_3 all decreased when manipulating with unseen objects instead of the seen ones, we only saw significant statistical differences on Tr_1 in Task 1 and Task 2 ($p = 0.011$ and $p = 0.007$, Cohen's d effect sizes are 1.34 and 0.891, respectively). These results reveal that the biggest challenge for current VLA models when dealing with unseen objects remains to accurately locate the correct object to manipulate, suggesting that the VLA models may not be able to recognize unseen objects in many cases. We did not observe significant statistical differences on Tr_1 in Task 3 and Task 4. A plausible explanation is due to the small number of passed test cases (~ 20 out of 1000) in both tasks.

Finding 11

Current VLA models struggled to recognize unseen objects, which was the primary cause of failure in most test scenes.

6 Discussion

Our study reveals several key implications that can lead to the development of better and more reliable VLA models for robotic manipulation. In this section, we discuss these implications and explore future research opportunities.

VLA models for robotic manipulation—too good to be true for now. While VLA models have the potential to revolutionize AI-enabled robotic manipulation, our experiment results in RQ1 and RQ2 reveal that the current models are still **unreliable** for common robotic manipulation tasks at the time of this study. As a result, deploying VLA models in high-stakes and safety-critical applications remains impractical.

Our detailed analysis suggests that the deficiency mainly comes from the lack of capabilities in precisely interpreting complex task requirements and accurately localizing the correct target objects to manipulate. We believe there is a huge space for improvement in addressing these issues. One potential solution is to scale up the model size. Currently, even the largest model in our study, OpenVLA-7b, has only 7 billion parameters, which is significantly smaller than state-of-the-art (SOTA) models in other domains. For instance, one of the largest open-source LLMs, Llama 3.1, has 405 billion parameters. The closed-source LLMs such as GPT-4 and Claude-3.5 typically have even much higher numbers of model parameters. By scaling up the model, we may also observe *emergent capabilities* for VLA models [8].

In addition to scaling up the size of VLA models, exploring more effective prompting strategies could be another promising direction. Previous studies have demonstrated that improved prompting can significantly enhance the performance of LLMs across various tasks, such as solving mathematical problems [79, 84] and code generation [11, 89]. Our Finding 2 suggests that current VLA models struggle to decompose complex task instructions into multiple steps of action. To fix this, one may consider prompting the VLA model step by step. This also aligns with one of the popular prompting strategies in the field of LLMs – *chain-of-thought* prompting. While our study has only explored the most basic prompts, future research should explore more advanced prompting techniques to evaluate their impact on VLA model performance. Furthermore, one can also introduce multi-agent systems to split the robotic manipulation tasks among multiple VLA agents, which is a strategy widely used in other domains [80, 83, 90].

Addressing the robustness challenges. Our study results from RQ3 and RQ4 reveal that current VLA models lack robustness against several external factors, such as lighting conditions and camera poses. We also found that models with large-scale pre-training or those trained with larger datasets of robot demonstration data exhibit greater robustness compared to others. This highlights a promising research direction: enriching the robot demonstration data. Since manually collecting real-world robot demonstration data requires significant labeling efforts, researchers may consider leveraging data augmentation techniques [2, 5] or employing *sim2real* translation [32, 92] to scale up training data by utilizing simulation environments.

Moreover, our Finding 6, Finding 7, and Finding 8 show that when external factors like lighting and camera angles deviate significantly from default settings, VLA model performance drops accordingly. This suggests that existing robot demonstration datasets may lack diversity, especially regarding variations in external conditions. In future work, when collecting datasets for training/fine-tuning factors, practitioners should take these environmental factors into account, which may potentially lead to the training of more robust VLA models.

Assessing the capabilities of VLA models. Our Finding 10 and Finding 11 (RQ5) suggest that current VLA models struggled to perform tasks with unseen objects. In practice, it is unrealistic to expect VLA models to successfully perform manipulation for every possible task scenario. Thus, in parallel to the development of more powerful and robust VLA models, it is also important to design novel techniques to comprehensively assess the capabilities of VLA models and derive proper guidelines about the use of VLA models. To address these, potential solutions include throughout offline benchmarking and online risk assessment.

In terms of offline benchmarking, our 18,604 generated test scenes across four tasks can serve as one of the early benchmarks for VLA models. In future work, practitioners may focus on expanding this benchmark to include a broader range of robotic manipulation tasks and diverse robot settings, covering various object types, environmental factors, and task complexities. In terms of online risk assessment, one may consider adopting SOTA techniques for risk assessment in other domains, such as uncertainty estimation [37, 53] and safety monitoring [82]. While general techniques may be directly used in the context of robotic manipulation with VLA models, it is unclear to what extent they can help with assessing the quality and reliability of decisions made by VLA models.

Towards efficient testing for VLA models. Although our proposed VLATest successfully identified numerous failed test scenes across our subject VLA models, it also incurred significant time overheads. Specifically, we relied on a *random sampler* for sampling target objects and obstacles in the testing scenes, which may not have been the most efficient approach. Future research could focus on optimizing the $pose_s ampler$ in Algorithm 1 to strategically assign critical positions and orientations for objects and obstacles. For instance, one can consider metamorphic-based methods [24, 78, 86] or search-based methods [13, 93] to efficiently generate test scenes for VLA models. Meanwhile, researchers may also work on test prioritization [14, 22, 46] or test selection [1, 23, 34, 36] towards efficient testing for VLA models.

Nevertheless, as VLA models continue to evolve, we argue that testing strategies must also evolve in parallel. The complexity and capabilities of these models are likely to increase, requiring more sophisticated and adaptive testing frameworks that can keep pace with advancements.

7 Related Work

7.1 Foundation Models for Robotics

A large body of research has been done on the use of foundation models for robotics. Based on the data modality, recent work can be roughly categorized into two groups: (1) those that use large language models (LLMs) for robotics, and (2) those that use multi-modality foundation models (e.g., vision language models) for robotics. One of the early attempts in using LLMs for robotics is to leverage LLMs as a reward designer for Deep Reinforcement Learning-based robotic manipulation [65]. This work proposes a self-refined framework to let the LLM automatically and interactively generate and refine reward functions used to train DRL policies for robotic control. Alternatively, Zhou et al. [94] adopts LLMs, first, as a translator to convert natural language input into a Planning Domain Definition Language (PDDL) formulation and then outputs action plan sequences for hong-horizon tasks.

Different from the use of LLMs, multi-modality foundation models such as vision language models (VLMs) enable the possibility of advancing AI-enabled robotics in several novel tasks, e.g., for robotic manipulation [7, 8, 72], visual question answering with robots [19], and visual state representations [54]. Our work is most closely related to those using vision-language-action models, a specialized category of VLMs, for robotic manipulation [7, 8, 39, 44, 45, 68, 72]. One of the pioneer works in VLA models for robotic manipulation is RT-1 [7], which uses a combination of a FiLM EfficientNet and a transformer to learn control policies from 130k real-world robot demonstrations. Since the publish of Open X-Embodiment dataset [57], a series of VLA models have been proposed by either training or fine-tuning on Open X-Embodiment [8, 39, 45, 72]. Our work is parallel to these works. We propose a general testing framework to test VLA models and present an empirical study to comprehensively assess the performance of VLA models.

7.2 Testing Cyber-Physical Systems

Quality assurance of traditional cyber-physical systems (CPS) and AI-driven CPS is a vital topic in the realm of software engineering, which assures the safety and trustworthiness of such complex systems in safety-critical domains. Substantial efforts have been made by researchers and industrial practitioners to safeguard the quality of CPS from various perspectives, such as testing [3, 12, 42, 52, 91], analysis [6, 67, 85] and repairing [28, 64, 77]. Considering robotic manipulation as a widely deployed representative CPS, our work is most related to the testing of CPS.

In particular, Lee et al. [42] propose MOTIF, a gray-box fuzzing-based approach to generate test data for software deployed in CPS. This method monitors the coverage achieved by the vanilla and the mutated functions, thereby exploring the behaviour space of the software under test. Differing from the existing testing solutions, MOTIF specifically targets the testing challenges of C and C++ languages that are widely used in CPS contexts. In terms of the black-box approach, Menghi et al. [52] introduces ARIsTEO, a searched-based testing method with a loop of approximation and refinement to identify requirement violations of CPS models, and Chen et al. [12] propose an active fuzzing approach to find test suits for packet-level CPS network attacks. Moving forward with CPS with AI module embedded, Zhang et al. [91] design a series of time-aware coverage criteria for DNN controllers in CPS and develop a falsification framework FalsifAI, to find system defects by leveraging the coverage information from the proposed criteria. It is worth noting that the aforementioned works are not well applicable to VLA models, which is attributable to the multimodality characteristic, autoregressive generation mechanism, and large-scale model size. In contrast, our study initiates a testing framework tailored for VLA models in the context of different robotic manipulation tasks. VLATest encompasses four multimodality-aware testing operators to comprehensively assess the VLA models from different perspectives.

7.3 Benchmarking and Testing Foundation Models

After the remarkable success of foundation models, an important research direction is to explore and understand the boundaries of their capabilities, which can provide a basis for further safeguarding and enhancement. Based on this motivation, numerous studies have focused on evaluating large language models in the text domain across various properties, such as correctness [48], factuality [21, 49], robustness [76, 95], fairness [69], and privacy [29]. These studies offer a wealth of resources for the general performance assessment of LLMs. On the other hand, researchers have also made significant efforts to evaluate specific capabilities of LLMs, such as code-related abilities. These efforts include validating the correctness of generated code [10, 51, 87], examining whether LLMs can address real-world GitHub issues [38], and analyzing error patterns in LLM-driven code translations [58].

While the aforementioned studies provide valuable insights, most of them focus on performing analysis on static benchmarks. Orthogonal to these related works, there are also several attempts at dynamically generating test cases to evaluate one or more key properties of models. For example, existing studies use rule-based methods to generate test cases that measure bias [75] or linguistic capabilities [41], employ metamorphic testing for evaluating language translation [31, 70], and utilize mutation-based frameworks to assess robustness [81]. Our work differs from these previous approaches in two main ways: (1) our framework centers on VLA, a novel architecture that integrates multi-modal inputs and generates complex control commands, distinguishing it from language-focused foundation models; (2) our framework generates test cases that account for complex interactions in robotic manipulation within a 3D environment, presenting a new challenge compared to prior text-only testing frameworks.

8 Threats to Validity

We discuss the threats to the validity of our empirical study results, as well as the mitigating factors.

Internal Validity. One potential threat comes from the randomness in our experiments. To mitigate this, we generated 18,604 testing scenes in our empirical study. Overall, our empirical study took over 400 GPU hours to finish. While we only executed each testing scene once per VLA model, we believe this has limited impact on our findings as our goal is to evaluate the VLA model's overall performance on each task instead of the success of one specific testing scene.

Another potential threat to internal validity is the choice of prompt templates. To mitigate this, we followed the previous works [7, 8, 39, 72] to use the standard prompt template when evaluating VLA models for robotic manipulation. We also discuss the impact of prompts and the potential of improving VLA models with better prompting in Sec. 6.

External Validity. Threats to external validity include whether our study results can generalize to different experimental settings, such as different robotic manipulation tasks and different VLA models. To mitigate these threats, we select the four most popular robotic manipulation tasks according to Open X-Embodiment dataset [57]. In terms of the VLA models, we included the SOTA publicly available VLA models by the time we conducted this study. Given that the VLA model for robotic manipulation is a fast-developing research area, we also plan to extend our evaluation to other SOTA VLA models, e.g., RT-2 [8], once they are made available.

Finally, we have only implemented VLATest and evaluated the VLA models within one simulation environment, Maniskill2 [26]. To reduce the impact of distribution shifts between simulation and real robot execution, we chose a improved version of Maniskill2 [43], which provides *visual matching* to render realistic images as the visual input for VLA models.

Construct Validity. When designing our testing framework, VLATest, we have only considered a limited number of testing operators. To combat the threat, we included testing operators covering different aspects, e.g., task difficulties (i.e., number of obstacles) and environmental factors (i.e., the lighting intensity and camera poses). In future work, one may continue to improve VLATest by adding more testing operators, such as the number of lighting sources, the intrinsic parameters of cameras, and the resolution of cameras, for more comprehensive evaluation of VLA models.

9 Conclusion

In this paper, we propose VLATest, one of the early testing frameworks for testing VLA models for robotic manipulation. VLATest is a generation-based fuzzing framework based on ten operators covering different perspectives in the test scene of robotic manipulation. Upon implementing VLATest with Maniskill2 simulation environments, we further conducted a large-scale empirical study to assess the performance and robustness of seven popular VLA models across four robotic manipulation tasks. We generated 18,604 testing scenes, conducted more than 400 GPU hours of simulation and performed a detailed analysis of the challenges and limitations faced by the current VLA models. At the end of the paper, we discuss the implications of our study, shedding light on several future research directions to improve the quality and reliability of VLA models for robotic manipulation.

10 Data Availability

Our artifacts, including the replication packages and the generated testing scenes, are available on an anonymous Git repository: https://anonymous.4open.science/r/VLATest-5642.

References

[1] Zohreh Aghababaeyan, Manel Abdellatif, Mahboubeh Dadkhah, and Lionel Briand. 2024. Deepgd: A multi-objective black-box test selection approach for deep neural networks. *ACM Transactions on Software Engineering and Methodology* 33, 6 (2024), 1–29.

[2] Khaled Alomar, Halil Ibrahim Aysel, and Xiaohao Cai. 2023. Data augmentation in classification and segmentation: A survey and new strategies. *Journal of Imaging* 9, 2 (2023), 46.

[3] Jon Ayerdi, Valerio Terragni, Aitor Arrieta, Paolo Tonella, Goiuria Sagardui, and Maite Arratibel. 2021. Generating metamorphic relations for cyber-physical systems with genetic programming: an industrial case study. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 1264–1274.

[4] Yuntao Bai, Andy Jones, Kamal Ndousse, et al. 2022. Training a helpful and harmless assistant with reinforcement learning from human feedback. *arXiv preprint arXiv:2204.05862* (2022).

[5] Homanga Bharadhwaj, Jay Vakil, Mohit Sharma, Abhinav Gupta, Shubham Tulsiani, and Vikash Kumar. 2024. Roboagent: Generalization and efficiency in robot manipulation via semantic augmentations and action chunking. In *2024 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 4788–4795.

[6] Matteo Biagiola and Paolo Tonella. 2024. Testing of deep reinforcement learning agents with surrogate models. *ACM Transactions on Software Engineering and Methodology* 33, 3 (2024), 1–33.

[7] Anthony Brohan, Noah Brown, Justice Carbajal, et al. 2022. Rt-1: Robotics transformer for real-world control at scale. *arXiv preprint arXiv:2212.06817* (2022).

[8] Anthony Brohan, Noah Brown, Justice Carbajal, et al. 2023. Rt-2: Vision-language-action models transfer web knowledge to robotic control. *arXiv preprint arXiv:2307.15818* (2023).

[9] Berk Calli, Arjun Singh, Aaron Walsman, Siddhartha Srinivasa, Pieter Abbeel, and Aaron M Dollar. 2015. The ycb object and model set: Towards common benchmarks for manipulation research. In *2015 international conference on advanced robotics (ICAR)*. IEEE, 510–517.

[10] Federico Cassano, John Gouwar, Daniel Nguyen, et al. 2023. MultiPL-E: a scalable and polyglot approach to benchmarking neural code generation. *IEEE Transactions on Software Engineering* 49, 7 (2023), 3675–3691.

[11] Xinyun Chen, Maxwell Lin, Nathanael Schärli, and Denny Zhou. 2023. Teaching large language models to self-debug. *arXiv preprint arXiv:2304.05128* (2023).

[12] Yuqi Chen, Bohan Xuan, Christopher M Poskitt, Jun Sun, and Fan Zhang. 2020. Active fuzzing for testing and securing cyber-physical systems. In *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*. 14–26.

[13] Mingfei Cheng, Yuan Zhou, and Xiaofei Xie. 2023. Behavexplor: Behavior diversity guided testing for autonomous driving systems. In *Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis*. 488–500.

[14] Xueqi Dang, Yinghua Li, Mike Papadakis, Jacques Klein, Tegawendé F Bissyandé, and Yves Le Traon. 2024. Test input prioritization for machine learning classifiers. *IEEE Transactions on Software Engineering* (2024).

[15] Amandeep Dhaliwal. 2020. The rise of automation and robotics in warehouse management. In *Transforming Management Using Artificial Intelligence Techniques*. CRC Press, 63–72.

[16] Yan Ding, Xiaohan Zhang, Chris Paxton, and Shiqi Zhang. 2023. Task and motion planning with large language models for object rearrangement. In *2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2086–2092.

[17] Alexey Dosovitskiy, Lucas Beyer, Alexander Kolesnikov, Dirk Weissenborn, Xiaohua Zhai, Thomas Unterthiner, Mostafa Dehghani, Matthias Minderer, Georg Heigold, Sylvain Gelly, et al. 2020. An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. In *International Conference on Learning Representations*.

[18] Danny Driess, Fei Xia, Mehdi SM Sajjadi, et al. 2023. Palm-e: An embodied multimodal language model. *arXiv preprint arXiv:2303.03378* (2023).

[19] Yuqing Du, Ksenia Konyushkova, Misha Denil, Akhil Raju, Jessica Landon, Felix Hill, Nando de Freitas, and Serkan Cabi. 2023. Vision-language models as success detectors. *arXiv preprint arXiv:2303.07280* (2023).

[20] Andrius Dzedzickis, Jurga Subačiūtė-Žemaitienė, Ernestas Šutinys, Urtė Samukaitė-Bubnienė, and Vytautas Bučinskas. 2021. Advanced applications of industrial robotics: New trends and possibilities. *Applied Sciences* 12, 1 (2021), 135.

[21] Nouha Dziri, Ehsan Kamalloo, Sivan Milton, Osmar Zaiane, Mo Yu, Edoardo M Ponti, and Siva Reddy. 2022. Faithdial: A faithful benchmark for information-seeking dialogue. *Transactions of the Association for Computational Linguistics* 10 (2022), 1473–1490.

[22] Yang Feng, Qingkai Shi, Xinyu Gao, Jun Wan, Chunrong Fang, and Zhenyu Chen. 2020. Deepgini: prioritizing massive tests to enhance the robustness of deep neural networks. In *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*. 177–188.

[23] Xinyu Gao, Yang Feng, Yining Yin, Zixi Liu, Zhenyu Chen, and Baowen Xu. 2022. Adaptive test selection for deep neural networks. In *Proceedings of the 44th International Conference on Software Engineering*. 73–85.

[24] Xinyu Gao, Zhijie Wang, Yang Feng, Lei Ma, Zhenyu Chen, and Baowen Xu. 2024. MultiTest: Physical-Aware Object Insertion for Testing Multi-sensor Fusion Perception Systems. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. 1–13.

[25] Ruchi Goel and Pooja Gupta. 2020. Robotics and industry 4.0. *A Roadmap to Industry 4.0: Smart Production, Sharp Business and Sustainable Development* (2020), 157–169.

[26] Jiayuan Gu, Fanbo Xiang, Xuanlin Li, et al. 2023. Maniskill2: A unified benchmark for generalizable manipulation skills. *arXiv preprint arXiv:2302.04659* (2023).

[27] Huihui Guo, Fan Wu, Yunchuan Qin, Ruihui Li, Keqin Li, and Kenli Li. 2023. Recent trends in task and motion planning for robotics: A survey. *Comput. Surveys* 55, 13s (2023), 1–36.

[28] Zhengang Guo, Yingfeng Zhang, Xibin Zhao, and Xiaoyu Song. 2020. CPS-based self-adaptive collaborative control for smart production-logistics systems. *IEEE transactions on cybernetics* 51, 1 (2020), 188–198.

[29] Aamir Hamid, Hemanth Reddy Samidi, Tim Finin, Primal Pappachan, and Roberto Yus. 2023. GenAIPABench: A benchmark for generative AI-based privacy assistants. *arXiv preprint arXiv:2309.05138* (2023).

[30] Dong Han, Beni Mulyana, Vladimir Stankovic, and Samuel Cheng. 2023. A survey on deep reinforcement learning algorithms for robotic manipulation. *Sensors* 23, 7 (2023), 3762.

[31] Pinjia He, Clara Meister, and Zhendong Su. 2020. Structure-invariant testing for machine translation. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering*. 961–973.

[32] Sebastian Höfer, Kostas Bekris, Ankur Handa, et al. 2021. Sim2real in robotics and automation: Applications and challenges. *IEEE transactions on automation science and engineering* 18, 2 (2021), 398–400.

[33] Jane Holland, Liz Kingston, Conor McCarthy, Eddie Armstrong, Peter O'Dwyer, Fionn Merz, and Mark McConnell. 2021. Service robots in the healthcare sector. *Robotics* 10, 1 (2021), 47.

[34] Qiang Hu, Yuejun Guo, Xiaofei Xie, Maxime Cordy, Mike Papadakis, Lei Ma, and Yves Le Traon. 2023. Aries: Efficient testing of deep neural networks via labeling-free accuracy estimation. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*. IEEE, 1776–1787.

[35] Siyuan Huang, Zhengkai Jiang, Hao Dong, Yu Qiao, Peng Gao, and Hongsheng Li. 2023. Instruct2act: Mapping multi-modality instructions to robotic actions with large language model. *arXiv preprint arXiv:2305.11176* (2023).

[36] Yuheng Huang, Jiayang Song, Qiang Hu, Felix Juefei-Xu, and Lei Ma. 2024. Active Testing of Large Language Model via Multi-Stage Sampling. *arXiv preprint arXiv:2408.03573* (2024).

[37] Yuheng Huang, Jiayang Song, Zhijie Wang, Shengming Zhao, Huaming Chen, Felix Juefei-Xu, and Lei Ma. 2023. Look before you leap: An exploratory study of uncertainty measurement for large language models. *arXiv preprint arXiv:2307.10236* (2023).

[38] Carlos E Jimenez, John Yang, Alexander Wettig, Shunyu Yao, Kexin Pei, Ofir Press, and Karthik Narasimhan. 2023. Swe-bench: Can language models resolve real-world github issues? *arXiv preprint arXiv:2310.06770* (2023).

[39] Moo Jin Kim, Karl Pertsch, Siddharth Karamcheti, et al. 2024. OpenVLA: An Open-Source Vision-Language-Action Model. *arXiv preprint arXiv:2406.09246* (2024).

[40] Maria Kyrarini, Fotios Lygerakis, Akilesh Rajavenkatanarayanan, Christos Sevastopoulos, Harish Ram Nambiappan, Kodur Krishna Chaitanya, Ashwin Ramesh Babu, Joanne Mathew, and Fillia Makedon. 2021. A survey of robots in healthcare. *Technologies* 9, 1 (2021), 8.

[41] Jaeseong Lee, Simin Chen, Austin Mordahl, Cong Liu, Wei Yang, and Shiyi Wei. 2024. Automated Testing Linguistic Capabilities of NLP Models. *ACM Transactions on Software Engineering and Methodology* (2024).

[42] Jaekwon Lee, Enrico Viganò, Oscar Cornejo, Fabrizio Pastore, and Lionel Briand. 2023. Fuzzing for CPS Mutation Testing. In *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE, 1377–1389.

[43] Xuanlin Li, Kyle Hsu, Jiayuan Gu, et al. 2024. Evaluating Real-World Robot Manipulation Policies in Simulation. *arXiv preprint arXiv:2405.05941* (2024).

[44] Xinghang Li, Minghuan Liu, Hanbo Zhang, et al. 2023. Vision-language foundation models as effective robot imitators. *arXiv preprint arXiv:2311.01378* (2023).

[45] Xiang Li, Cristina Mata, Jongwoo Park, et al. 2024. LLaRA: Supercharging Robot Learning Data for Vision-Language Policy. *arXiv preprint arXiv:2406.20095* (2024).

[46] Yinghua Li, Xueqi Dang, Lei Ma, Jacques Klein, and Tegawendé F Bissyandé. 2024. Prioritizing test cases for deep learning-based video classifiers. *Empirical Software Engineering* 29, 5 (2024), 111.

[47] Jacky Liang, Wenlong Huang, Fei Xia, Peng Xu, Karol Hausman, Brian Ichter, Pete Florence, and Andy Zeng. 2023. Code as policies: Language model programs for embodied control. In *2023 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 9493–9500.

[48] Percy Liang, Rishi Bommasani, Tony Lee, et al. 2023. Holistic Evaluation of Language Models. *Transactions on Machine Learning Research* (2023). https://openreview.net/forum?id=iO4LZibEqW Featured Certification, Expert Certification.

[49] Stephanie Lin, Jacob Hilton, and Owain Evans. 2022. TruthfulQA: Measuring How Models Mimic Human Falsehoods. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics*. 3214–3252.

[50] Haotian Liu, Chunyuan Li, Qingyang Wu, and Yong Jae Lee. 2024. Visual instruction tuning. *Advances in neural information processing systems* 36 (2024).

[51] Jiawei Liu, Chunqiu Steven Xia, Yuyao Wang, and Lingming Zhang. 2024. Is your code generated by chatgpt really correct? rigorous evaluation of large language models for code generation. *Advances in Neural Information Processing Systems* 36 (2024).

[52] Claudio Menghi, Shiva Nejati, Lionel Briand, and Yago Isasi Parache. 2020. Approximation-refinement testing of compute-intensive cyber-physical models: An approach based on system identification. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering*. 372–384.

[53] Subhabrata Mukherjee and Ahmed Awadallah. 2020. Uncertainty-aware self-training for few-shot text classification. *Advances in Neural Information Processing Systems* 33 (2020), 21199–21212.

[54] Suraj Nair, Aravind Rajeswaran, Vikash Kumar, Chelsea Finn, and Abhinav Gupta. 2022. R3m: A universal visual representation for robot manipulation. *arXiv preprint arXiv:2203.12601* (2022).

[55] Maxime Oquab, Timothée Darcet, Théo Moutakanni, et al. 2023. DINOv2: Learning Robust Visual Features without Supervision. *Transactions on Machine Learning Research* (2023).

[56] James Orr and Ayan Dutta. 2023. Multi-agent deep reinforcement learning for multi-robot applications: A survey. *Sensors* 23, 7 (2023), 3625.

[57] Abhishek Padalkar, Acorn Pooley, Ajinkya Jain, et al. 2023. Open x-embodiment: Robotic learning datasets and rt-x models. *arXiv preprint arXiv:2310.08864* (2023).

[58] Rangeet Pan, Ali Reza Ibrahimzada, et al. 2024. Lost in translation: A study of bugs introduced by large language models while translating code. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. 1–13.

[59] Ethan Perez, Florian Strub, Harm De Vries, Vincent Dumoulin, and Aaron Courville. 2018. Film: Visual reasoning with a general conditioning layer. In *Proceedings of the AAAI conference on artificial intelligence*, Vol. 32.

[60] Abu Rayhan. 2023. Artificial intelligence in robotics: From automation to autonomous systems.

[61] Olga Russakovsky, Jia Deng, Hao Su, et al. 2015. Imagenet large scale visual recognition challenge. *International journal of computer vision* 115 (2015), 211–252.

[62] Mohamed Shamout, Rabeb Ben-Abdallah, Muhammad Alshurideh, Haitham Alzoubi, B al Kurdi, and Samer Hamadneh. 2022. A conceptual model for the adoption of autonomous robots in supply chain and logistics industry. *Uncertain Supply Chain Management* 10, 2 (2022), 577–592.

[63] Ishika Singh, Valts Blukis, Arsalan Mousavian, Ankit Goyal, Danfei Xu, Jonathan Tremblay, Dieter Fox, Jesse Thomason, and Animesh Garg. 2023. Progprompt: Generating situated robot task plans using large language models. In *2023 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 11523–11530.

[64] Jiayang Song, Xuan Xie, and Lei Ma. 2023. SIEGE: A Semantics-Guided Safety Enhancement Framework for AI-Enabled Cyber-Physical Systems. *IEEE Transactions on Software Engineering* 49, 8 (2023), 4058–4080.

[65] Jiayang Song, Zhehua Zhou, Jiawei Liu, Chunrong Fang, Zhan Shu, and Lei Ma. 2023. Self-refined large language model as automated reward function designer for deep reinforcement learning in robotics. *arXiv preprint arXiv:2309.06687* (2023).

[66] Mohsen Soori, Behrooz Arezoo, and Roza Dastres. 2023. Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics* 3 (2023), 54–70.

[67] Andrea Stocco and Paolo Tonella. 2022. Confidence-driven weighted retraining for predicting safety-critical failures in autonomous driving systems. *Journal of Software: Evolution and Process* 34, 10 (2022), e2386.

[68] Austin Stone, Ted Xiao, Yao Lu, et al. 2023. Open-world object manipulation using pre-trained vision-language models. *arXiv preprint arXiv:2303.00905* (2023).

[69] Lichao Sun, Yue Huang, Haoran Wang, et al. 2024. Trustllm: Trustworthiness in large language models. *arXiv preprint arXiv:2401.05561* (2024).

[70] Zeyu Sun, Jie M Zhang, Mark Harman, Mike Papadakis, and Lu Zhang. 2020. Automatic testing and improvement of machine translation. In *Proceedings of the ACM/IEEE 42nd international conference on software engineering*. 974–985.

[71] Mingxing Tan and Quoc Le. 2019. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In *Proceedings of the 36th International Conference on Machine Learning (Proceedings of Machine Learning Research, Vol. 97)*, Kamalika Chaudhuri and Ruslan Salakhutdinov (Eds.). PMLR, 6105–6114.

[72] Octo Model Team, Dibya Ghosh, Homer Walke, Karl Pertsch, Kevin Black, Oier Mees, Sudeep Dasari, Joey Hejna, Tobias Kreiman, Charles Xu, et al. 2024. Octo: An open-source generalist robot policy. *arXiv preprint arXiv:2405.12213* (2024).

[73] Hugo Touvron, Louis Martin, Kevin Stone, et al. 2023. Llama 2: Open foundation and fine-tuned chat models. *arXiv preprint arXiv:2307.09288* (2023).

[74] Manas Wakchaure, BK Patle, and AK Mahindrakar. 2023. Application of AI techniques and robotics in agriculture: A review. *Artificial Intelligence in the Life Sciences* 3 (2023), 100057.
[75] Yuxuan Wan, Wenxuan Wang, Pinjia He, Jiazhen Gu, Haonan Bai, and Michael R Lyu. 2023. Biasasker: Measuring the bias in conversational ai system. In *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 515–527.
[76] Boxin Wang, Weixin Chen, Hengzhi Pei, et al. 2023. DecodingTrust: A Comprehensive Assessment of Trustworthiness in GPT Models. In *Thirty-seventh Conference on Neural Information Processing Systems Datasets and Benchmarks Track*. https://openreview.net/forum?id=kaHpo8OZw2
[77] Renzhi Wang, Zhehua Zhou, Jiayang Song, Xuan Xie, Xiaofei Xie, and Lei Ma. 2024. MORTAR: A Model-based Runtime Action Repair Framework for AI-enabled Cyber-Physical Systems. *arXiv preprint arXiv:2408.03892* (2024).
[78] Shuai Wang and Zhendong Su. 2020. Metamorphic object insertion for testing object detection systems. In *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*. 1053–1065.
[79] Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten Bosma, Fei Xia, Ed Chi, Quoc V Le, Denny Zhou, et al. 2022. Chain-of-thought prompting elicits reasoning in large language models. *Advances in neural information processing systems* 35 (2022), 24824–24837.
[80] Chunqiu Steven Xia, Yinlin Deng, Soren Dunn, and Lingming Zhang. 2024. Agentless: Demystifying llm-based software engineering agents. *arXiv preprint arXiv:2407.01489* (2024).
[81] Mingxuan Xiao, Yan Xiao, Hai Dong, Shunhui Ji, and Pengcheng Zhang. 2023. LEAP: Efficient and Automated Test Method for NLP Software. In *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE, 1136–1148.
[82] Xuan Xie, Jiayang Song, Zhehua Zhou, Yuheng Huang, Da Song, and Lei Ma. 2024. Online Safety Analysis for LLMs: a Benchmark, an Assessment, and a Path Forward. *arXiv preprint arXiv:2404.08517* (2024).
[83] John Yang, Carlos E Jimenez, Alexander Wettig, Kilian Lieret, Shunyu Yao, Karthik Narasimhan, and Ofir Press. 2024. Swe-agent: Agent-computer interfaces enable automated software engineering. *arXiv preprint arXiv:2405.15793* (2024).
[84] Shunyu Yao, Dian Yu, Jeffrey Zhao, Izhak Shafran, Tom Griffiths, Yuan Cao, and Karthik Narasimhan. 2024. Tree of thoughts: Deliberate problem solving with large language models. *Advances in Neural Information Processing Systems* 36 (2024).
[85] Rajaa Vikhram Yohanandhan, Rajvikram Madurai Elavarasan, Premkumar Manoharan, and Lucian Mihet-Popa. 2020. Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access* 8 (2020), 151019–151064.
[86] Boxi Yu, Zhiqing Zhong, Xinran Qin, Jiayi Yao, Yuancheng Wang, and Pinjia He. 2022. Automated testing of image captioning systems. In *Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis*. 467–479.
[87] Hao Yu, Bo Shen, Dezhi Ran, Jiaxin Zhang, Qi Zhang, Yuchi Ma, Guangtai Liang, Ying Li, Qianxiang Wang, and Tao Xie. 2024. Codereval: A benchmark of pragmatic code generation with generative pre-trained models. In *Proceedings of the 46th IEEE/ACM International Conference on Software Engineering*. 1–12.
[88] Xiaohua Zhai, Basil Mustafa, Alexander Kolesnikov, and Lucas Beyer. 2023. Sigmoid loss for language image pre-training. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 11975–11986.
[89] Kechi Zhang, Zhuo Li, Jia Li, Ge Li, and Zhi Jin. 2023. Self-edit: Fault-aware code editor for code generation. *arXiv preprint arXiv:2305.04087* (2023).
[90] Yuntong Zhang, Haifeng Ruan, Zhiyu Fan, and Abhik Roychoudhury. 2024. Autocoderover: Autonomous program improvement. *arXiv preprint arXiv:2404.05427* (2024).
[91] Zhenya Zhang, Deyun Lyu, Paolo Arcaini, Lei Ma, Ichiro Hasuo, and Jianjun Zhao. 2022. FalsifAI: Falsification of AI-enabled hybrid control systems guided by time-aware coverage criteria. *IEEE Transactions on Software Engineering* 49, 4 (2022), 1842–1859.
[92] Wenshuai Zhao, Jorge Peña Queralta, and Tomi Westerlund. 2020. Sim-to-real transfer in deep reinforcement learning for robotics: a survey. In *2020 IEEE symposium series on computational intelligence (SSCI)*. IEEE, 737–744.
[93] Yuan Zhou, Yang Sun, Yun Tang, Yuqi Chen, Jun Sun, Christopher M Poskitt, Yang Liu, and Zijiang Yang. 2023. Specification-based autonomous driving system testing. *IEEE Transactions on Software Engineering* 49, 6 (2023), 3391–3410.
[94] Zhehua Zhou, Jiayang Song, Kunpeng Yao, Zhan Shu, and Lei Ma. 2024. Isr-llm: Iterative self-refined large language model for long-horizon sequential task planning. In *2024 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2081–2088.
[95] Kaijie Zhu, Jindong Wang, Jiaheng Zhou, Zichen Wang, Hao Chen, Yidong Wang, Linyi Yang, Wei Ye, Neil Zhenqiang Gong, Yue Zhang, et al. 2023. Promptbench: Towards evaluating the robustness of large language models on adversarial prompts. *arXiv preprint arXiv:2306.04528* (2023).