Meeting Time:19/09/24 11.00 am

Location: Online

**Attendees:**

- Gnaneshwar Reddy Bana 23832048

- Kanishk Kanishk 23959947

- Pedro Wang 23870387

- Sarath Pathari 22941307

- Yuxin Gu 23743373

- Yuanfu Cao 23633858

- Client Matthew

**Demonstration of Current Features and Integration Plan:** The team showcased the current CLI model prototype, which can analyze uploaded images, and plans to integrate it into the graphical user interface (GUI) in the next iteration. The client hopes that the future GUI will support user-friendly operations, including image uploads and various distortion controls, to enable more intuitive image processing and analysis.

**Batch Processing and CSV File Support:** Users discussed the need for batch processing and CSV file export functionality. The client specified that the CSV file should include fields such as model name, distortion intensity, file name, prompt information, and the language model's analysis output. They also hope to support generating and downloading CSV files directly within the GUI in the future. Additionally, the client requested support for batch processing multiple images and automatically generating structured analysis reports.

**Image Distortion Effects and Future Features:** The team plans to develop the GUI in the next Sprint and implement various image distortion effects such as blur, brightness, contrast, sharpness, color, rain effect, and water effect. The client is satisfied with this and hopes to add more creative distortion effects in the future, such as dynamic water ripples and flames, to test how the language model responds to these complex visual inputs.

**Language Model Security and Prompt Injection Attacks:** Users expressed concerns about potential security issues when using language models to control robots, especially the risk of prompt injection attacks. The client suggested adding stronger system instruction support to the system and developing multiple predefined prompts to handle different scenarios and prevent malicious actors from injecting unsafe commands to alter the robot's behavior.

**Real-Time Inference and Dynamic Scenario Decision-Making Research:** The client showed great interest in real-time inference and evaluation capabilities, although it is challenging to achieve currently. They hope to simulate the robot's decision-making process in dynamic environments by gradually displaying images in the future. Moreover, they wish to further explore how the robot can make reasonable decisions and ensure safety in real-world environments, such as when encountering pedestrians or kangaroos with dynamic changes.