This chapter evaluates the project’s implementation using three main criteria: the extent to which it meets the success criteria detailed in §\ref{sec:requirements}, the applicability of HE to inference algorithms, and its practicality regarding current, real-world surveillance technology. Consequently, the chapter is divided into three sections to tackle each criterion distinctly. Both quantitative and qualitative analysis is used throughout the chapter to analyse the implementation's performance and make predictions about the scope to which the investigation may be extended in future. Unless otherwise specified, the data presented was generated using $64 \times 64$ pixel images from the Moving-MNIST dataset.

|  |  |  |
| --- | --- | --- |
| Requirement | Achieved | Justification |
| A1 | ✔️ | The project contains a client-server application that allows videos to be homomorphically encrypted and transmitted across a network, with implementation techniques detailed in §\ref{sec:networking}. |
| A2 | ✔️ | The project contains several algorithms that are able to extract moving objects from homomorphically encrypted videos, with implementation techniques detailed in §\ref{sec:inference}. |
| A3 | ✔️ | The accuracy of HE inference algorithms are evaluated to investigate their efficacy and applicability in §\ref{sec:idk}. |
| B1 | ✔️ | The MeKKS scheme, detailed in §\ref{sec:mekks}, provides a complete implementation of the fundamental principles of the CKKS HE scheme. |
| B2 | x | Due to time constraints, an independent investigation into the security of HE schemes could not be completed. However, only well-established, trusted schemes were considered; hence CKKS was selected and reimplemented over less secure schemes. |
| B3 | x | The implementation of moving object detection algorithms proved to be more open than expected. Consequently, more time was dedicated to further understanding this area rather than expanding into other inference paradigms. |

The success criteria in §\ref{sec:requirements} were split into two categories: \textit{core} and \textit{extensions}. As detailed in Table \ref{tab:requirements}, All three of the core criteria were implemented, and one of the three extensions has also been completed. The open-ended nature of this project means that defining a \textit{completed} state for some criterium was not trivial. For example, for criterium \texttt{A2}, while some algorithms have been implemented in their entirety, others require further investigation. However, it was important to have a goal for each criterium to properly plan the project and consider all aspects equally. Therefore, a justification for the state of each criterium has been included.