Adapting moving object detection algorithms for the HE domain proved to be the project's biggest challenge. The limited number of operations available, combined with the limited number of applications supported by ciphertexts, means some aspects of inference cannot be recreated. Particular challenges came when trying to implement the median filter and a GMM.

However, frame differencing, the mean filter, and the Gaussian average methods of background subtraction were successfully implemented using the techniques described in §\ref{sec:adaptations}. A sample of the results from each of these algorithms running on the Moving-MNIST dataset is provided in Figure \ref{fig:inferenceResults}, and an example of what can be achieved on a more realistic dataset – the LASIESTA dataset – is provided in Figure \ref{fig:lasiestaResults}.

# Online Mixture Model

In the \textit{online mixture model} algorithm detailed in §\ref{sec:OMM}, Equation \ref{eq:gmmInequality} describes how a fitted model can be used to segment an image. However, inequality comparison operators are not provided by the standard CKKS implementation. To solve this, Cheon et al.\ proposed the algorithm in Figure \ref{fig:comparison} [COMPARISON]. Unfortunately, this introduces security concerns. If the ability to compare two HE ciphertexts is added to the system, an attacker\footnote{such as Mallory in §\ref{sec:threatModel}.} could use it to exfiltrate information about the image. For example, with enough comparison operations, they would be able to determine the exact value of each pixel in a frame. Consequently, this algorithm was abandoned to preserve the security of the system.

For the same reason, the median filter could not be implemented. The pixel values could not be ordered without a comparison operator, so a median could not be calculated.

# Expectation-Maximisation

The difficulty in implementing this algorithm came from the number of operations that need to be performed across the fitting and predicting stages. Calculating means and covariances repeatedly requires many successive multiplications, requiring many coefficient levels in ciphertexts. Also, like the online mixture model, not all operations are supported by the CKKS scheme. In particular, the algorithm requires several divisions to be performed when updating the Gaussian distributions. Currently, the best solution for this seems to be provided by Cheon et al.\ [COMPARISON]. However, the algorithm, given in Figure \ref{fig:division}, has a minimal domain requiring input values to be between zero and two. Normalising pixel values might provide a method for incorporating this, but the noise induced by HE means inference becomes infeasibly inaccurate.