There have been many attempts at solving video inference in the encrypted domain, but none are without flaws. In 2013, Chu et al. [CHU] proposed an encryption scheme that supports real-time moving object detection. However, this was quickly shown to suffer from information leakage, leaving it vulnerable to chosen-plaintext attacks \footnote{A \textit{chosen-plaintext attack} is a scenario in which an adversary can freely encrypt plaintexts of their choosing and analyse the resulting ciphertexts.} Similarly, in 2017, Lin et al. [LIN] proposed an encryption scheme to achieve the same goal by only encrypting some of the bits in each pixel, but this is unprotected against steganographic \footnote{\textit{Steganography} describes the technique of securing messages through information hiding. Unlike cryptography, where the existence of a message is known, but its contents are not, steganography attempts to hide the message’s existence.} attacks. Therefore, while research has solved the weaknesses in privacy, it is yet to offer a solution that also preserves security, making them useless to real-world applications.

Likewise, researchers have been investigating inference using HE for many years. In 2012, Graepel et al. [GRAEPEL] introduced machine learning in the HE domain. Dowlin et al. [DOWLIN] built upon this when they developed the CryptoNets model for deep learning with HE in 2016. However, deep learning neural networks are considered overly complex for moving-object detection. Instead, Gaussian Mixture Models (GMMs) are the most common technique for background modelling. There is much less HE research into this area of unsupervised learning. The best example comes from 2013 when Pathak and Raj [PATHAK] proposed a HE implementation of a GMM for audio inference. But there do not seem to be any investigations linking HE and GMMs to video analysis.

The most prevailing explanation for this lack of research is HE’s inapplicability to real-time applications due to its high computational complexity. While this may be true now, it is important to acknowledge that advances in computing capability will reduce the relative difficulty of HE operations. Consequently, more insight into its applicability will become increasingly valuable, as suggested by the trend in the growing popularity of HE research. This dissertation attempts to offer some beginnings to this insight by investigating the limitations of current HE implementations concerning surveillance.