There have been many attempts to improve video inference privacy using malleable encryption, 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, removing utility 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. While this work can be used to establish a foundation for GMM implementation in the HE domain, audio and video analysis details differ, so its relevance is bounded. 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 the limited applicability of HE to real-time applications due to high computational complexity. However, a consequence of this is that the usefulness of HE in video inference is not well documented. Moreover, as computing capability and hardware acceleration advance, the relative difficulty of HE operations will reduce. Therefore, more insight into the applicability will become increasingly valuable, as suggested by the growing popularity of HE research. This project attempts to offer some understanding of this field by investigating HE for surveillance through techniques to optimise network transmission and modification of standard inference algorithms to support HE data, overcoming the inherent computational challenges.