Computers have improved almost every aspect of modern life. Recently, home security has become a target of the technology revolution. Companies like Ring [RING] and Eufy [EUFY] offer IoT devices like doorbells and cameras to allow their customers to continuously monitor their property. On top of traditional surveillance, these companies also provide software solutions to analyse footage. For example, a doorbell may recognise a visitor or alert to the presence of a stranger. However, the computational intensity of inference means footage must be transferred to more powerful servers.

To provide security, video is encrypted before transmission to the server. However, the footage must be decrypted when inference is being performed. This poses significant privacy concerns. Decrypting footage on the server exposes the opportunity for employees of these companies to access video content. Consequently, malicious actors could use this information to monitor peoples’ location, appraise their belongings, extort subjects, and more. Similar risks exist if the company is hacked and raw video data is exfiltrated. Homomorphic Encryption (henceforth HE) may provide a solution to this.

In cryptography, HE describes encryption schemes that allow mathematical operations to be performed directly on encrypted data, or \textit{ciphertext}, rather than on raw data, or \textit{plaintext}. For example, consider the calculation $3 \times 5$. In a traditional encryption scheme, the plain values $3$ and $5$ would be multiplied and then encrypted. Using a homomorphic scheme, $3$ and $5$ can be encrypted, and the ciphertexts multiplied, resulting in a ciphertext that produces $15$ when decrypted. However, HE is a developing research area, so has limitations. HE ciphertexts are much larger than unencrypted data, so operations' time and space complexity significantly increased. Similarly, not all operations are available in the HE domain, and those that are varies between schemes, so the choice of scheme is critical to success. An open question is, can this technique be scaled to more complex algorithms, like those required for surveillance?

More specifically, this project aims to investigate if it is possible to extract moving objects from HE video data. Moving object detection is fundamental to surveillance. Detecting when, for example, somebody enters a property allows security systems to alert their owners, possibly pre-empting a break-in. However, more than just motion must be sensed. Objects must be extracted and analysed to prevent users from being notified of unimportant events like, for example, leaves blowing onto a property. Gradual changes and random noise in an environment make modelling a background for object detection a significant challenge to overcome.