This chapter discusses the preparatory work done before beginning the project’s implementation. §\ref{sec:preliminaries} introduces the relevant concepts, terminologies, and notations from cryptography, graphics, and unsupervised machine learning fundamental to the project, §\ref{sec:projectStrategy} discusses the methodologies used when approaching the design of the project’s implementation, and §\ref{sec:startingPoint} provides an overview of the project’s foundations.

# Homomorphic Encryption

## Introduction

There are two broad categories of cryptographic encryption schemes: private-key (symmetric) and public-key (asymmetric). While both can be applied to HE, this dissertation will address public-key encryption because it is the technique adopted by all HE schemes used in the project.

A public-key encryption scheme is defined by a triple of functions $\Pi = (\texttt{KeyGen}, \texttt{Enc}, \texttt{Dec})$. \texttt{KeyGen} is a function used to generate a \textit{public key} (\texttt{PK}) and \textit{private key}\footnote{The \textit{private key} is referred to as a \textit{secret key} by some literature. While these terms are equivalent, general convention is to use \textit{secret key} in relation to symmetric encryption, and \textit{private key} when discussing asymmetric.} (\texttt{SK}) such that $(\texttt{PK}, \texttt{SK}) \leftarrow \texttt{KeyGen}(1^l)$, where the security parameter, $l$, measures how hard it is for an adversary to break the scheme\footnote{An $l$-bit security parameter would require an expected $2^l$ attempts to guess the keys.}. Denoting the space of all possible plaintext messages as $\mathcal{M}$ and ciphertext messages as $\mathcal{C}$, a message $m \in \mathcal{M}$ is encrypted into its corresponding ciphertext $c \in \mathcal{C}$ by $c \leftarrow \texttt{Enc}\_\texttt{PK}(m)$. Similarly $c$ is decrypted back into $m$ by $m \leftarrow \texttt{Dec}\_\texttt{SK}(c)$.

In order to extend $\Pi$ into a HE scheme, a fourth function $\texttt{Eval}(f, c\_1, \ldots, c\_n)$ must be introduced. The evaluation function, $\texttt{Eval}$ applies a Boolean circuit, $f$, to the ciphertext arguments, $c1, \ldots, c\_n$ such that, for all arguments, it holds that

Equation

where $m\_1, \ldots, m\_n$ are the plaintext equivalents of $c\_1, \ldots, c\_n$. This is, perhaps, better illustrated by Figure \ref{fig:homomorphicEncryption} below.

Theoretically, a \textit{fully} homomorphic scheme\footnote{The prefix \textit{fully} derives from the existence of \textit{partially} homomorphic schemes. A partially homomorphic scheme will only allow certain operations on the ciphertext – usually multiplication and division – and have existed for many years. Some examples of partially homomorphic schemes include RSA, ElGamal, and Paillier encryption [PARTIALSCHEMES].} allows the evaluation of Boolean circuits indefinitely. However, in practice, the time complexity of operations means many schemes are \textit{levelled} homomorphic schemes. This means they only support operations up to a \textit{bounded depth} – that is, only a predefined number of circuits can be applied to a ciphertext before the plaintext becomes irrecoverable. The maximum depth is a critical factor when applying HE to practical problems because it significantly limits the scope of supported algorithms.

## Ring Learning with Errors

For an encryption scheme to be \textit{perfectly secure}, a ciphertext must provide no additional information about its plaintext (see Equation \ref{eq:def1}). In other words, the probability of generating a given ciphertext from a particular plaintext is independent of the plaintext (see Equation \ref{eq:def2}). The two equations below can be shown to be equivalent using Bayes’ rule.

Equations

While it is possible to create perfectly secure encryption schemes\footnote{For example, the One-Time Pad[OTP]}, they are impractical in real applications. Therefore, \textit{computational security} is considered sufficient. Relying on the hardness of certain mathematical problems, computational security means that an encryption scheme is \textit{practically unbreakable}: the most efficient known algorithm for breaking a cipher would require more computational steps than an attacker with unlimited hardware could perform. For example, the RSA encryption scheme relies on the fact that there exists no known, efficient algorithm for computing the prime factors of a large number on a classical computer – the integer factorisation problem. In complexity theory, this problem falls into the set of $\mathcal{NP}$.

Similarly, the HE schemes used in this project rely on computational security. They utilise the hardness of the \textit{ring learning with errors} (henceforth RLWE) problem introduced by Lyubashevsky et al.\ [RLWE]. A polynomial-time reduction from the \textit{shortest vector problem} to RLWE can be derived. Therefore, since the shortest vector problem is $\mathcal{NP}$-hard under the correct choice of parameters, it is safe to rely on RLWE for computational security.

To understand the RLWE problem, knowledge of group theory is required. The relevant definitions are introduced in Appendix \ref{app:groups}. The RLWE problem requires the ring formed by the set of polynomials modulo $\Phi (X)$ that also have coefficients in $\mathbb{Z}\_q$\footnote{$\mathbb{Z}\_q$ is the set of integers modulo $q$. For example, $\mathbb{Z}\_7 = \{0, 1, 2, 3, 4, 5, 6\}$.}. Known as a \textit{quotient ring}, this can be denoted by $\mathcal{R}\_q = \mathbb{Z}[X] / (\Phi(X))$, where $\Phi(X)$ is an \textit{irreducible polynomial} – a polynomial which cannot be factored into two non-constant polynomials.

Informally, RLWE describes the problem of finding an unknown $s \in \mathcal{R}\_q$ given a polynomial vector computed using $s$ and some sampled errors. An encryption scheme can be created such that, after encoding a plaintext vector, $\vec{v}$, as a list of polynomials and it to a polynomial using a secret polynomial, it is infeasible to recover $\vec{v}$ in polynomial time.

The HE schemes discussed in this dissertation rely on the RLWE problem to assert \textit{indistinguishable encryptions under a chosen-plaintext attack} (IND-CPA) security. Fundamentally, any encryption scheme is IND-CPA secure if, when attacked by a probabilistic, polynomial-time adversary, the chances of correctly deciding which of two plaintexts a particular ciphertext corresponds to is even. Therefore, in practice, even if an adversary has access to an encryption \textit{oracle}, the adversary’s chances of calculating the correct plaintext when given a ciphertext should be no better than if they were randomly guessing.

Practically, HE schemes choose a \textit{cyclotonic polynomial} for $\Phi(X)$, where the $n$-th cyclotonic polynomial, $\Phi\_n(X)$, is defined as

Equation

In order to speed up computation, $n$ is selected to be an even power of two. Consequently, $\Phi\_n(X) = X^\frac{n}{2} + 1$. This allows the \textit{number theoretic transform} (NTT)\footnote{A specialisation of the discrete Fourier transform, the NTT is a generalisation of the Fast Fourier transform in the case of finite fields [NTT].}. The advantage of this is that it can be easily accelerated using hardware [HARDWARE].

The sampled errors used when deriving ciphertexts imply almost exponential error growth in the number of multiplications applied. The limited depth property of levelled HE schemes directly results from this. However, the relative growth size can be reduced by increasing the modulus $q$. Although, if a polynomial degree of size $n/2$ is used, efficient attacks exist against the RLWE problem for a small value of $q$ [HEStandard]. Therefore, a fundamental trade-off is introduced between the supported depth of multiplication and the security level.

# Moving Object Detection

## Introduction

\textit{Image segmentation} is a well-established problem in the fields of digital image processing and computer vision research. The problem describes the process of partitioning a digital image into multiple regions, represented as sets of pixels. The goal is to simplify an image representation so that it is easier to, for example, locate objects or boundaries, allowing further analysis. More precisely, image segmentation describes labelling each pixel of an image such that all pixels sharing a particular characteristic are assigned the same label [SHAPIRO].

There are two broad categories of segmentation techniques: \textit{semantic} [SEMANTIC] and \textit{instance} [INSTANCE]. This dissertation will focus on semantic segmentation through moving object detection because videos will be segmented into two categories: foreground and background, rather than labelling individual instances of objects.

To perform \textit{foreground extraction}, also known as \textit{background subtraction}, the background of an image must be modelled so that changes in the scene can be detected. This is an unsolved problem. Image data can be very diverse, with variable lighting and repetitive movements (like leaves and shadows) making robust models hard to develop.

Once a background model has been developed, it can be used to detect moving objects in videos by comparing each frame to a reference frame and extracting the differences. There are several methods for achieving this. Below are five algorithms investigated for this dissertation.

## Frame Differencing

\textit{Frame differencing} is the most straightforward background subtraction algorithm [FRAMEDIFFERENCING]. First, a reference frame is established. There are several options for this, including selecting the first frame, or continually updating to the frame previously received. Challenges include ensuring the model can adapt to permanent changes, like a fence being added to a property, and accounting for random noise. Updating the reference too frequently can cause issues with slow-moving objects becoming occluded.

Once the reference frame, $B$, has been selected, the foreground can be extracted. Denoting each frame at time $t$ as $f\_t$, the value of each pixel in $B$, $P(B)$, can be subtracted from the corresponding pixel in $f\_t$, $P(f\_t)$. The mathematical definition is given by Equation\ref{eq:frameDifferencing}.

Equation

where $F$ represents the frames in the resultant video.

## Mean Filter

A \textit{mean filter} approach to moving object detection attempts to overcome the weaknesses of frame differencing in selecting a reference frame [MEANFILTER]. Instead of taking a frame directly from the video, the value of $B$ at time $t$ is calculated using Equation \ref{eq:meanFilter}.

Equation

where $N$ is the number of preceding images included in the average, and $f\_t$ is the frame in the video at time $t$. $N$ would depend on the video speed and the amount of motion expected in the video.

After $B$ has been calculated at time $t$, the value of the resultant video $F\_t$ can be calculated using the same method as frame differencing, given by Equation \ref{eq:frameDifferencing}.

## Median Filter

The \textit{median filter} algorithm is similar to performing mean filter extraction. Instead of using the mean to calculate the reference frame, the median of the preceding $N$ frames is used [MEANFILTER]. Then, the moving objects are extracted by subtracting the reference frame from each frame in the video, according to Equation \ref{eq:frameDifferencing}.

## Gaussian Average

Wren et al.\ originally proposed fitting a Gaussian probabilistic density function to the most recent $N$ frames [WREN]. Rather than storing an image as the reference frame, this method stores a mean and variance for each pixel. When a new frame is received, the likelihood of each pixel is calculated. Assuming that the background is the most common value for a pixel, the foreground can be segmented by grouping the pixels with a sufficiently low likelihood.

Rather than recalculating the mean every time a frame is received – giving an $O(n^2)$ time complexity – the algorithm can be implemented using cumulative functions for the mean and variance to achieve a linear time complexity. The functions are defined by Equation \ref{eq:mean} and Equation \ref{eq:variance} respectively.

Equation

Equation

where $\alpha$ determines the size of the \textit{temporal window} used to fit the Gaussian model\footnote{$\alpha$ weights frames according to age. Eventually, an old frame will be weighted so insignificantly that its impact is negligible. Therefore, it determines how far into the past the model uses to predict future pixels.}, $d = |f\_t - \mu\_t|$ gives the Euclidean distance from the pixel to the mean, and $c$ is some constant defined by the model creator.

From these models, the foreground can be extracted according to Equation \ref{eq:meanThreshold}

Equation

where $k$ is a constant that the model creator can tune to achieve optimal results.

A variant of this algorithm might only update the model if a pixel is believed to be in the background. This prevents the model from becoming skewed if there is lots of movement. However, it requires the entire frame to be initially background and struggles to cope with constant changes.

## Gaussian Mixture Models

Stauffer and Grimson proposed \textit{Gaussian mixture models} (henceforth GMMs) for moving object detection in 1999 [STAUFFER]. GMMs are probabilistic models that represent the presence of normally distributed subpopulations within an overall population. They are particularly useful because they don’t require the subpopulation of a data point to be identified. Instead, subpopulations are labelled automatically, constituting \textit{unsupervised machine learning}.

There are two types of parameters necessary for GMMs, the \textit{component weights}, and the component \textit{means} and \textit{variances}. For a GMM with $N$ components, the $i^\text{th}$ component has $\mu\_i$ and variance $\sigma\_i$ in the \textit{univariate case}, and mean $\vec{\mu}\_i$ and a covariance matrix $\Sigma\_i$ in the \textit{multivariate case}. The component weights, $\phi\_k$ for component $k$, are constrained by the equation $\sum^K\_{i=1} \phi\_i = 1$. If the component weights aren’t learned, they are known as an \textit{a-priori}\footnote{A probability derived purely through deductive reasoning.} distribution over components such that $\probP(x \text{ generated by component k}) = \phi\_k$. If the component weights are learned, they are known as \textit{a-posteriori}\footnote{From Bayesian statistics, referring to conditional probability $\probP(A | B)$.} estimates of the component probabilities given the data.

When fitting a GMM, the Gaussian distributions are tuned to match the distributions observed in the data. A common method for this is to use \textit{expectation maximisation} (EM), if the number of components is known. If all of the data is available, it can be incorporated into this stage to achieve the most accurate fitting. However, only a subset of the data will likely be available in practice, so the GMM will extrapolate to more values. This technique can also be taken advantage of if there is limited time to perform fitting.

Once a GMM has been fitted, it can be used for inference. This dissertation will focus on inference for \textit{clustering} because it is most useful for moving object detection. The posterior component assignment probabilities can be estimated using Bayes’ theorem over the GMM parameters. Knowing the component that a data point most likely belongs to provides a way to group the points into clusters. In the scenario of moving object detection, this would be two clusters: the foreground and the background.