A message can be communicated to other people using a combination of pictures, sounds, and actions. Ensuring that the message is understood as intended often depends on the presentation of these forms of multimedia. In today’s digital world, traditional multimedia artefacts such as paintings, photographs, audiotapes and videocassettes, although still used, are gradually being replaced with a digital equivalent. It is normally easy to duplicate these digital multimedia files, and they are often available within public repositories. Although this has its advantages, security may be a concern, especially for sensitive multimedia data. Information security services such as identification and authentication, authorisation, and confidentiality can be implemented to secure the data at the file level, ensuring that only authorised entities gain access to the entire multimedia file.

It may not always be the case however that a message must be conveyed in the same way for every entity (user or program) that makes a request for the multimedia data. Although access control measures can be ensured for the multimedia at *the file level*, very little work has been done to ensure access control for multimedia at *the content level*. A number of models will be presented in this dissertation that should ensure logical access control at the content level for the three main types of multimedia, namely images, audio, and video. In all of these models, the multimedia data is securely stored in a repository, while the associated security information is stored in a database. The objects that contain the authorisation information are created through an interface that securely communicates with the database. Requests are made through another secure interface, where only the authorised multimedia data will be assembled according to the requesting entity’s security classification. Certain important side issues concerning the secure multimedia models will also be discussed. This includes security issues surrounding the model components and suspicion i.e. reducing the probability that a requesting entity would come to the conclusion that changes were made to the original multimedia data.