but forensic investigators found that it contained 141 separate text files detailing terrorist operations and plans. [8]

2.1.4 Issues

Text

The three different types of text steganography are vulnerable to different attacks. Structural based methods can be destroyed if the text is copied or reprinted. For example, if the data is hidden through whitespace, but the cover-text is hand copied onto paper from a computer screen, then there is a very high chance that the data is lost.
Linguistic based methods are vulnerable to the text being changed by a third party attacker. A popular example with this relates to the prisoner's problem.

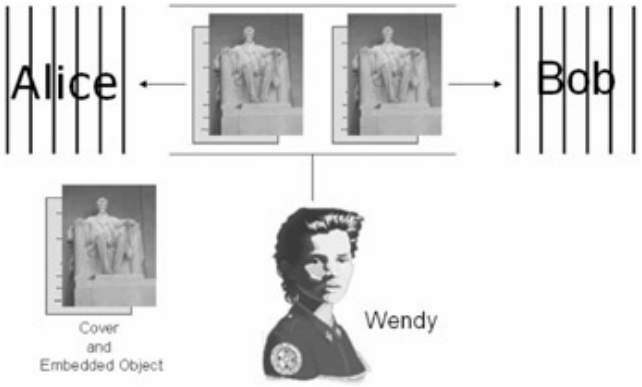

Figure 2.3: Representation of the prisoner's problem. [19]

In this scenario, the warden can intercept messages sent between prisoners and change words while still keeping the meaning of the text (as is done with synonym-based steganography methods). Doing this means that the correct data cannot be retrieved. An example of this, from the First World War is a cable-gram which read "Father is dead". The cable-gram was intercepted and the text changed to "Father is Deceased", which led to the response "Is Father dead or deceased?", which gave away that there was a hidden message. [16]

Images, Audio and Video

The primary vulnerability that these multimedia forms of steganography are susceptible to is compression. For example, in the case of an image, where data may be hidden in the least significant bit every k pixels, the image can be decompressed, distorted (for example by cropping) and then re-compressing [7]. Similar effects can affect audio and video. For example, in a audio file in the WAV format, data could be hidden in low volume or frequency sounds which humans cannot hear. If this file was compressed into the MP3 format, these