manipulating the syntactic or semantic properties of the existing text. These are discussed in detail in section 2.1.5.

Images

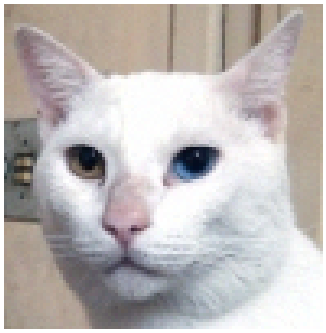

Figure 2.2: Example of image steganography. Image contains the text "Boss said that we should blow up the bridge at midnight." [39]

Image steganography can either be in the image or transform domain. Steganography in the image domain usually involves hiding data in the least significant bits at certain intervals in the image, for example one bit in each of the red, green blue values. In the transform domain, a transformation is applied on the cover image (such as the lossy part of a compression algorithm) and then the data is hidden. In JPEG compression this involves taking advantage of the discrete cosine transform. This means that the data is less susceptible to further compression algorithms. [22]

Audio

As with image steganography, data can be hidden using the least significant bit in the audio. Most commonly, the data is hidden in such a way that the data is inaudible to the human ear. For example, humans cannot hear a tone that immediately follows a louder tone, so this is often used to hide data as using the most significant bit can be used to help overcome audio compression, without the original file sounding any different to humans. Another possibility is to introduce a minute echo to sounds to hide data, the delay dictating the data being hidden [5].

Video

Video can be used to hide data in much of the same ways as with images by hiding data in each individual frame. A famous example of this is a video found on a laptop owned by an suspected al-Qaeda member. The video, at first glance, appeared to be pornography