hidden and so observers do not know that the message exists. The hidden message or data may be encrypted before it is hidden for an added layer of security. The reason why this is useful is that in some countries it is illegal to even possess encrypted material. By using steganography this material can be hidden.

One modern usage of steganography is in watermarking. Watermarks are identifiers inserted into a piece of data (whether it be text, audio, video or an image), which can either be used to verify the data as genuine, or even identify a particular copy of the piece of data. An example is the release of an audio file containing a new song to reviewers, with the condition that it is not released. The file is watermarked with the identity of the reviewer. If the song is then leaked online, it will be very simple for the record label to access one of the illegal copies and extract the watermark, identifying who leaked the song. This process is however vulnerable, as will be discussed in the next section.

Steganography is increasingly being found to be used by terrorists and criminals to hide data and exchange information. For example, a child pornography distributor could hide images in the photos on an legitimate ebay listing to distribute them to their customers [11]. There has also been evidence of al-Qaeda storing information contained in text files hidden in videos [8].

Steganography is not just used by criminals and organisations. There are a large number of freely available steganography programs which can be used by home users to store sensitive information more securely, for example bank account details could be hidden in an image so when they are required they can be retrieved, but if someone was to gain access to the computer they would not be able to identify them (as they would be able to recognise, and possibly break, an encrypted file).

There is evidence of governments using steganography for both legal and illegal communication. There has been court cases in the US where accused Russian spies were found to have been using steganographic communication channels (specifically images) to communicate with their handlers [15].

There has even been proposals of using steganography as a means for communication within a botnet. Nagaraja et al. [23] proposed Stegobot, a botnet which uses steganography as the basis for its command and control (C& C) network. It uses JPEG steganogrpahy to hide collected data (such as credit card details and passwords) in images that are uploaded to Facebook. Bots are connected to each other via users on the social network. Once the images are uploaded, they are visible to all users connected to the uploading user. Bots on infected machines intercept any images that a user on that machine views, and extracts any information. This bot then hides the data in an image upload by a user on its computer, where it will be visible to all of that user's connections. The data eventually reaches the bot master via restrictive flooding. The estimated bitrate is around 20mb/month, which while not sounding like much can represent a large amount of personal information.

One particularly interesting case id that of printer manufacturers secretly printing microscopic dots onto all pages they print. These dots are arranged in a pattern which can be