decoded into the date and time the page was printed, along with the printers serial number [30]. It is claimed that this data is used by governments in criminal counterfeit investigations. This is an example of steganography where the data has been used to generate a pattern, and then this pattern has been printed at a microscopic level, following a similar (but much smaller) principle to microdots. There are a number of pieces of software that can be used to perform steganography. OpenStego [26] is an open source program for performing image steganography. It can hide any type of file within the image, and files are encrypted before they are hidden. OpenPuff [25] is a piece of freeware that can perform steganography on multiple file types, including audio and video (but not text), and can even split the steganography over multiple files so there are theoretically no data limits.

2.1.3 Types of Steganography

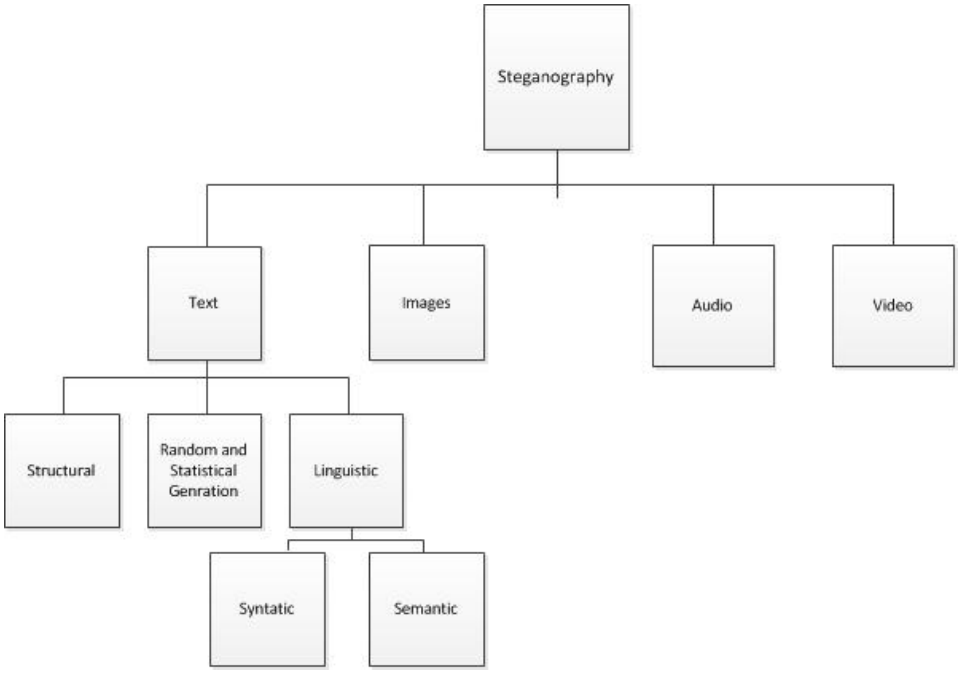

Figure 2.1: The different forms of steganography

Text

There are three mains forms of text steganography: structural, random and statistical generation and linguistic. Structural text steganography involves changing the physical structure of the text, for example by adding whitespace or increasing the line spacing. Random and statistical generation involves generating the cover-text either randomly, or according to some function on an input. Linguistic steganography, the focus of this project, involves