the recipient. For example, the word "hello" hidden with spammimic gives the result:
" Dear Decision maker , We know you are interested in receiving amazing intelligence . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1625 ; Title 4 ; Section 302 . THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich as few as 55 DAYS . Have you ever noticed most everyone has a cellphone and more people than ever are surfing the web . Well, now is your chance to capitalize on this ! WE will help YOU decrease perceived waiting time by 200your business into an E-BUSINESS ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Mr Ames of Massachusetts tried us and says "My only problem now is where to park all my cars" ! We are licensed to operate in all states ! We beseech you - act now . Sign up a friend and your friend will be rich too ! Thank-you for your serious consideration of our offer ! "
This is much more realistic than the Stego! example, as it appears almost exactly like a poorly written spam message. This approach takes advantage of the fact that 80 % of all email traffic is spam [9], and so discovering this email and extracting the bits among all of the other spam messages will incur a very high cost.

Linguistic

Linguistic steganography comes in two forms: syntactic and semantic. Syntactic text steganography involves altering the structure of the text without significantly altering the meaning or tone. Examples methods could be to alter the punctuation in a sentence. One proposed solution by Judge [14] uses spelling errors to hide data, for example spelling "is" as "iz". A correctly spelled word indicated a zero, a incorrectly spelled word a 1. This major flaw with this method is that it can be affected by unintentional spelling mistakes.
Semantic based steganography is the focus of this paper. This method involves replacing words with their synonyms in order to hide data. This will be explored more fully in the "Current Research" section below.

2.2 Steganalysis

Steganalysis is to steganography what cryptanalysis is to cryptography. The primary difference is that while with cryptanalysis the aim is to extract the original data from the encrypted message, the goal of steganalysis is primarily to detect if the object contains hidden data. It can be used to extract the message in some cases, although this is not always important and the steganography is considered to be broken if just the existence of hidden data is proven.