memory " (where "dress" replaces "jog"). These are two bad replacements, hence the low score.
Finally, the two sentences from the piece of fiction (1,1 and 2,1) provided some interesting results. The first sentence, 1,1, received a very low score despite the only word difference from the original being "door" replaced by "brink". The general consensus among the subjects that the sentence did not make sense. This may be due to the lack of context. If the subjects had access to the surrounding text the sentence would make more sense, but taken by itself it does not. The second sentence, however, received a much better score, as the only replacement was the word "top" with "point". This still made sense to the subjects, although two of them did comment that the word "point" may contain data. One thing that was found during these tests is that the non-native English speakers had more trouble identifying suspicious words than the native speakers. This means that the algorithm will be more effective if used on English text in non-English speaking countries. This is a similar result as described by Shirali-Shahreza et al. [32] with their American-British English substitutions.
It was also interesting that the scores were generally better once the subjects know about the algorithm and how it operated. Although the sentences may not be quite as complex as some of the sentences in the first section, it is possible that knowing what to look for made the users more tolerant to bad words, at least on a subconscious level.
What this test has proven is that the quality of the original text can have a large impact on the human analyser, even simple punctuation mistakes (all punctuation is kept by the algorithm) caused them to lower their scores in some places. Words which the users did not know, such as "dupes", or uncommon usages of words threw off the subjects, which will cause human analysis to throw up false positives.

5.8 Robustness to Steganalysis

5.8.1 Automatic

As has been shown with the results from the statistical analysis above, if the output was to be analysed by a method which used frequency analysis to detect hidden data then it should not be detected. It could, however, be susceptible to more advanced steganalysis techniques, such as the use of a grammar or more advanced semantic testing. There is a good possibility, however, that the algorithm will pass the simple frequency analysis and not be suspicious enough to warrant the more advanced methods, which will have a much higher cost.
There is also the fact that with this form of steganography, there is no easy way to know if the text actually contains data or not. If the deobfuscation algorithm is applied to unprocessed text, then there is a good chance that it will come out with data anyway, as the