

The output can be printed, copied, retyped, sent in emails but the data will never be lost (save for spelling mistakes while copying). The output cannot be compressed, so it is not vulnerable to compression algorithms which is one of the major flaws in many image, audio and video steganography algorithms.

The desired capacity for hiding data was around one bit for every ten words. The actual capacity, found through the statistical evaluation, is around 0.9 bits for every 10 words, so this has very almost been achieved.

The output of the algorithm is robust against at least frequency analysis based methods of steganalysis, and in many cases would be robust against more advanced methods involving grammars. Through human evaluation, the algorithm has also been moderately successful in avoiding human detection. There is still work that needs to be done, as described in the future work section above, but for a prototype the algorithm is very successful. Through the development of the test application, StegChat, the algorithm has proven that it can work in a real life situation and with further development the StegChat application could become a very useful tool.