# CALIFORNIA STATE SCIENCE FAIR
## 2012 PROJECT SUMMARY

**Name(s)**

Andrew S. Hong

**Project Number**

# S1411

**Project Title**

## The Art of Digital Steganography: A New Algorithm That Can Process Any Amount of Information in Various Formats Intact

**Abstract**

**Objectives/Goals**

The purpose of the project was to develop an algorithm that can conceal data of a variety of uncompressed files of different formats and recover the hidden data without loss of information.

**Methods/Materials**

The algorithm was implemented in Mathematica, a programming language. All materials used to test the algorithm belong to the student himself. There were four different cases to test the algorithm, and each case was tested numerous times to show that no information in the hidden and cover files was altered or lost. The first task was to conceal an image file inside another image file by using different numbers of LSBs (least significant bits) for concealing data to show the resulting image. The second task was to conceal a music file inside an image file. The third task was to conceal an image file inside a video file by splitting the data of the image, and the last task was to conceal a text file with over 40,000 words inside a video file.

**Results**

In all test cases, the implemented algorithm was successful in concealing and recovering vast amounts of information in various uncompressed digital formats without loss of information. Using fewer numbers of LSBs to conceal information resulted in better image quality, and there were no visible changes in the cover files when 1 bit was used to conceal information.

**Conclusions/Discussion**

The algorithm shows that there is a viable way of hiding a large amount of information without triggering suspicion and recovering information without any loss. The results also show that the algorithm works for files in a variety of uncompressed formats, including sound, image and text. Using one bit to hide information neither alters the hidden information nor creates noticeable differences in the cover file. Most importantly, if given multiple cover files, data to be hidden no longer has to be smaller than the data of the cover file because hidden information can be spread across multiple cover files.

This algorithm can be extended to a wide variety of applications, such as digital security and intelligence. Digital steganography can be used with encryption for watermarks and other security uses. Finally, reverse steganography can be used to crack the code and reveal information in the area of counter-terrorism.

**Summary Statement**

To improve current methods of digital steganography, I developed encoder and decoder algorithm to conceal data of a variety of uncompressed files of different formats.

**Help Received**