Encrypting Data Within the Color Values of Images for Messaging Purposes

Grant Spink, Computer Science AP

Introduction

Most digital images utilize a standard RGB color space to color its pixels. The human eye has been measured to only be able to distinguish 10 million colors, however the RGB 3 Byte Color Model can display over 16 million colors. Because only about 7 of the 8 bits that comprise each color byte create noticeable changes to the naked eye, data can be stored in the Least Significant Bits (LSB). The LSBs are located at places 0, 8, 16 in the 24 bit spectrum, and change each color's 256 possible values by 1. By contrast, the Most Significant Bits (MSB) are located at 7, 15, 23 in the 24 bit spectrum and change each color's 256 possible values by 128.

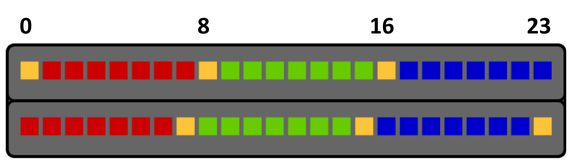

Figure 1. RGB model highlighting LSBs Top, MSBs Bottom.

Encrypted Messaging Platform

The low detectability of this data proves it to be ideal for hiding information such as messages. Encrypting the data and then inserting it within the LSB not only gives the illusion of randomness, but it also provides a secure platform to transmit secret messages.

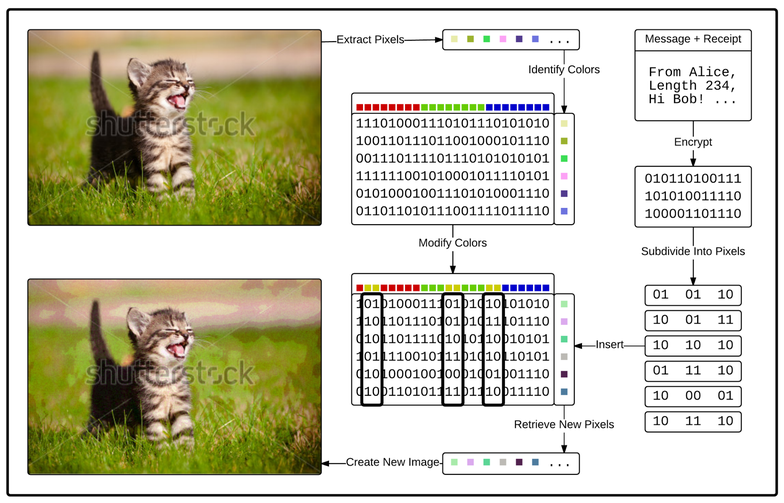

Figure 2. Encrypted data insertion method. Bits selected for modification: 1, 2, 11, 12, 16, 17.

Choosing Bits to Encrypt

Choosing only LSBs, which do not affect image quality may limit the amount of data that can be inserted. The user is given the option of choosing any number of bits within the spectrum, including the MSBs, to increase the amount of inserted data at the cost of image quality. It is possible to choose every bit, if one's intentions are to encrypt the most amount of data possible within an image (Figure 3).

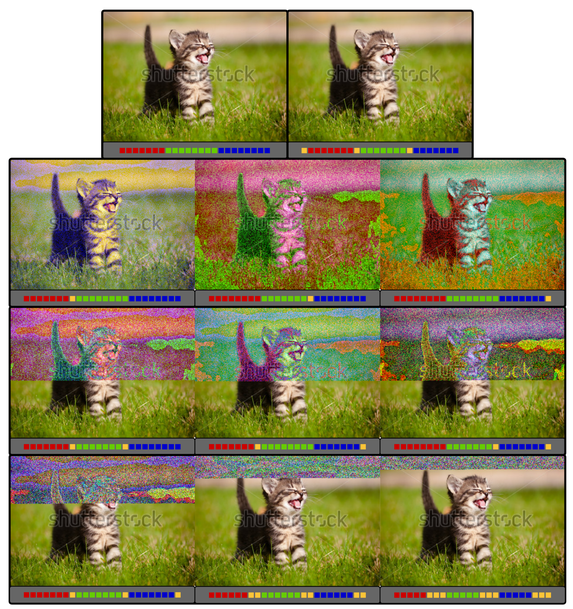

Figure 3. Data inserted into various bit places highlighted in yellow under each image.
Row 1: none, (RGB) LSBs.
Row 2: (R) MSB, (B) MSB, (G) MSB
Row 3: (RG) MSBs, (RB) MSBs, (GB) MSBs
Row 4: (RGB) MSBs, 2 (RGB) MSBs, 3 (RGB) MSBs

Encryption Process

The program uses a 2048-bit RSA cryptosystem to encrypt the message data for insertion into the images. This system takes advantage of public-key cryptography to provide the most secure transmission of data. Each user is given a public and private key. Keys are generated in pairs in such a way that if one key encrypts a message, the other key is needed to decrypt it.

The program also utilizes digital signing to verify sender authenticity. Each message is encrypted (signed) with the sender's private key, timestamped at intervals during the encryption, and then encrypted with the receiver's public key, so as to circumvent man-in-the-middle attacks.

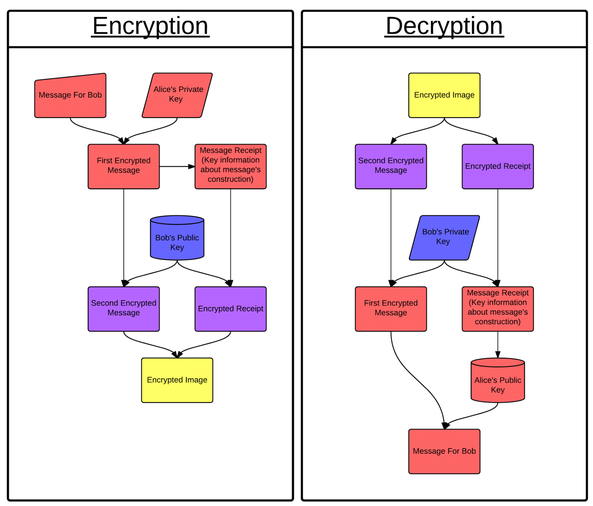

Figure 4. Message encryption and decryption. Alice encrypts a message for Bob, who then decrypts it.

Effectiveness at Storing Data

Because of the diversity of most images, it was found that the 3 LSBs in each of the red, green, and blue bytes can be used at the same time to hold data, with little to no alteration to the visual appearance of the image. This is a significant amount of usable space totalling 9/24 bits in each pixel or 37.5% of the total image. For example a 3000 x 1680 ~14MB wallpaper image would be able to store the entire 800,000 word King James Bible ~5MB, invisibly, with room to spare.

Figure 5. Left, 3000x1680 image unaltered. Right, 3000x1680 image encrypted with the 800,000 word King James Bible.

Effectiveness as a Messaging Platform

The robust security of the application proves it to be incredibly effective at hiding and transmitting data. However, because of the sheer amount of encryption that must be done, lengthy messages (upwards of 50,000 words) take several minutes to process. This leads to the conclusion that the program is viable as both an instant messaging service (small fast messages), and an email type service (slower larger messages).

Future Applications of the Software

Digital watermarking: Encoding copyright, date, geotag, and author would provide users with an anti image theft service.

Restricting visible parts of an image: Blurring out sensitive information such as a face, license plate, or logo, but wanting to keep the original image close by. As opposed to saving two images, the sensitive information is hidden within just one image, and can be retrieved later.

Image verification: Passport photographs or company IDs could be encoded so that when they are scanned, data is retrieved to verify the authenticity of the image.

Steganography: Images can be exchanged between two parties that appear to be inconspicuous, but upon decryption, actually reveal top secret information. This is a very safe and versatile form of communication as the images could even be posted on the internet without any suspicion.