Abstract

Image Steganography is to hide messages or information within other information in such a way as to not be detectable. This makes use of the fact that there is a large amount of data being transferred every second, making it impossible to scan all the information for hidden messages. Typical cryptographic methods obscure the information, but it is still very obvious that a message is being sent. Steganography attempts to correct this flaw so an observer is unable to know if a message is being sent or not. This can be used in addition to traditional cryptographic methods, so the security will only be enhanced, assuming that the traditional methods are being used with the same rigor as before.

Steganography in images is each pixel is encoded as a series of numbers which represent the red green and blue values which make up the color for that pixel. Since a
slight change in this color scheme is not detectable by the human eye, it can be used to hide information. This is usually accomplished by changing the least significant bit, or LSB, for each pixel to correspond to the bits of the hidden message.

Reference

- Ping Wah Wong; Memon, N., “Secret and public key image watermarking schemes for image authentication and ownership verification”, Image Processing, IEEE Transactions on, Volume 10, Issue 10, Page(s):2-8
- Dekun Zou, Chai Wah Wu, Guorong Xuan, Yun Q. Shi, “A content-based image authentication system with lossless data hiding”, Multimedia and Expo, International Conference on, Volume: 2, Page(s):1-3
- Debnath Bhattacharyya1, Poulami Das1, Samir Kumar Bandypadhyay, and Tai-hoon Kim “Text Steganography: A Novel Approach” (2009)

Index Terms

Computer Science Security
Key words
cryptography
digital signature
Image Steganography
watermarking