Abstract

LSB-based steganographic methods embed secret messages into the cover image by directly manipulating the least-significant-bit (LSB) plane. Although it is not the best steganographic method, LSB replacement is worth studying because of its large embedding capacity and simplicity. In LSB replacement, the LSB plane is simply replaced with the secret message so that the LSB values carry the hidden message directly. As more and more techniques of hiding information (Steganography) are developed, the methods of detecting the use of steganography (Steganalysis), also advance. Most steganography techniques change the properties of the cover source which increases the probability of detecting the changes. The DCT-M3 algorithm reduces significantly the number of changes in the cover image; the embedding capacity has been improved by 16.7% approximately while maintaining minimum detectability against blind steganalysis schemes. The effectiveness of steganography is measured using three parameters. First, the steganographic technique must provide the maximum information. Second, the embedded data must not be traceable to the viewer. Third, the hidden information should be successfully retrieved at the receiver. It is difficult to recognize the existence of a
hidden data in the cover image using the existing methods. This is because embedding is randomly performed in the frequency domain.

References


Index Terms

Computer Science
Security

Keywords

LSB image, steganography, secret message, image cover, LSB plane, hidden information.