Abstract

Steganography consist of concealing secret information in a cover object to be sent over a public communication channel. It allows two parties to share hidden information in a way that no intruder can detect the presence of hidden information. This paper presents a novel steganography approach based on pixel location matching of the same cover image. Here the information is not directly embedded within the cover image but a sequence of 4 bits of secret data is compared to the 4 most significant bits (4MSB) of the cover image pixels. The locations of the matching pixels are taken to substitute the 2 least significant bits (2LSB) of the cover image pixels. Since the data are not directly hidden in cover image, the proposed approach is more secure and difficult to break. Intruders cannot intercept it by using common LSB techniques.


Index Terms

Computer Science

Security

Keywords

Steganography, 4MSB, 2LSB, Matching Pixel Locations.