Abstract

Even after rapid development of encryption and decryption algorithms, the communication channels still face acute threat of illegal intelligence gathering. The science of steganography has also simultaneously emerged as a means of covert communication. One major reason is spread of digital images as means for passing classified information include the easy distribution, easy coping and simple means of modification. This is so vital that the aspect of image content modification and protection has become a major security issue. Recently, fragile watermarking has been used as a technique to achieve image authentication and tampering localization. The main purpose of this work is to present an algorithm for generation of stego file based on alternative watermarking. In this paper, we present an implementation of a fragile image modification scheme for classified communication. This scheme is based on chaos theory wherein a labile signal that is sensitive to modifications is embedded in the image so as to detect the image (and thus textual) tampering inconsistency. This approach can be implemented for content authentication.

References
A Novel Approach of Message Encryption based on Steganography and Watermarking

- Ming-Shi Wang, Wei-Che Chen, A majority-voting based water-marking scheme for colour image tamper detection and recovery, Computer Standards & Interfaces, Vol. 29, Issue 5, July 2007, pp. 561-570

Index Terms

Computer Science Security

Keywords

Cipher text Cover image Decryption Encryption Encryption Algorithm Fragile watermarking

LSB

Plain text
Stego image.