Abstract

Digital Crime is the latest terrorist who can intrude into any domain by breaking any type of firewall or secret code without frittering even a single drop of blood. To fight this terror, a cryptic army was evolved but not good enough to succeed. As a consequence, an effective commando namely steganography has been evolved who can combat any type of destructive intrusion. In this paper, Space Filling Curve (SFC) and RBG colour compound stego action against the threat of digital crime has been proposed. The proposed stego system scans the colour image pixel by pixel along a complex path, not row by row, and hides the variable k bit of the secret data in each pixel visited in the order defined by a Space-Filling Curve (SFC) such as the Hilbert curve and the Moore curve traversing paths. Such curves visit each pixel in the color image which is split into Red, Green and Blue components. The effectiveness of the proposed stego system has been estimated by computing bit error rate (BER), Mean square error(MSE), Peak Signal to Noise Ratio (PSNR) and Mean Structural Similarity index(MSSIM). This paper also illustrates how security has been enhanced using this algorithm.

Reference

[1]. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35
[5]. [Chin-Chen Chang, Chih-Yang Lin, Yi-Hsuan Fan, Lossless data hiding for color images based on block truncation coding, Pattern Recognition 41 (7) 2008 2347-2357.
Constructive Role of SFC & RGB Fusion versus Destructive Intrusion

Index Terms

Computer Science

Security

Key words

LSB steganography

Information hiding

space filling curves steganography