Implementation of Integration Blowfish Cryptography Methods with Blend Steganography to Improve Security Text Messages

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 132
Number 7

Year of Publication: 2015

Authors:
Rahmad Zainul Abidin, Yudi Prayudi, Imam Riadi

10.5120/ijca2015907493
{bibtex}2015907493.bib{/bibtex}

Abstract

Various techniques to ward off evil that uses information technology have been made, such as the delivery of messages by combining techniques Blowfish cryptography with steganography DCS (Dynamic Cell Spreading). However, DCS has a weakness when compared to steganography Blend. The disadvantage is the DCS insert text data in all the colors RGB. This will result in more pixels change and easily detected image embed text (stego image), while Blend is fewer the pixel changes. Based on DCS weakness, this research proposes the incorporation of steganographic techniques Blend as data embed technique and the Blowfish cryptography as data encryption technique.

This research testing process to MSE and PNSR analysis, to determine the rate of change of the original image (cover image) with stego image. Then Blend MSE PNSR results compared to the DCS.

The comparison showed that PSNR Blend value is higher than the value of DCS and MSE
Blend value is lower than the value of DCS. Obtained conclusions that the method of integration Blowfish cryptography with Blend steganography is better than the DCS steganography.

References


Index Terms

Computer Science  Security
Keywords

Cryptography, Blowfish, steganography, Blend.