Published: 27 April 2018

New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check

Mustafa Cem kasapbaşi & Wisam Elmasry

Sādhanā 43, Article number: 68 (2018) | Cite this article

237 Accesses | 5 Citations | Metrics

Abstract

Steganography is the technique for hiding information within a carrier file so that it is imperceptible for unauthorized parties. In this study, it is intended to combine many techniques to gather a new method for colour image steganography to obtain enhanced efficiency, attain increased payload capacity, posses integrity check and security with cryptography at the same time. Proposed work supports many different formats as payload. In the proposed method, the codeword is firstly formed with secret data and its CRC-32 checksum, then the codeword is compressed by Gzip just before encrypting it by AES, and it is finally added to encrypted header information for further process and then embedded into the cover image. Embedding the encrypted data and header information process utilizes Fisher-Yates Shuffle algorithm for selecting next pixel location. To hide one byte, different LSB (least significant bits) of all colour channels of the selected pixel is exploited. In order to evaluate the proposed method, comparative performance tests are carried out against different spatial image steganographic techniques using some of the well-known image quality metrics. For security analysis, histogram, enhanced LSB and Chi-square analyses are carried out. The results indicate that with the proposed method has an improved payload capacity, security and

Non-LSB based Steganography through Matrix Encoding in Spatial domain of an Image

[1]K.Rosemary Euphrazia [2]M. Mary Shanthi Rani
[1]Dept. of Computer Science, Fatima College, Madurai, TamilNadu. India.
[2]Dept. of Comp. Sci. and Applications, Gandhigram Rural Institute, DeemedUniversityGandhigram, TamilNadu. India
[1]rosemph@yahoo.com[2]drmaryshanthi@gmail.com

ABSTRACT

Data security is the process of protecting the data from access, disclosure, modification, or destruction by an unauthorized person. Steganography is a process in which the secret information is embedded in a digital medium without inducing any visible distortions. Every secret message is carried within some other entity and thus the communication remains secret. The simplest approach to hide data within an image file is LSB substitution, where the least significant bits of the randomly selected or sequential pixels are replaced by the secret bits. Even though this method is simple and most commonly used method for hiding data, its embedding efficiency is less and is prone to statistical attacks. This paper focuses on developing a novel method for hiding secret bits through encoding technique rather than LSB substitution. The objective of this method is to increase the embedding efficiency through matrix encoding. A Non-LSB based embedding algorithm has been developed using matrix encoding method and is compared with the LSB technique. The developed algorithm is evaluated using the standard parameters such as PSNR (Peak Signal to Noise Ratio), BER (Bit Error Rate) and SD (Standard Deviation) of the pixel values and it shows better performance than existing methods.

Keywords: Embedding Efficiency, LSB Substitution, Matrix Encoding, Steganography

1. INTRODUCTION

Safety of the information transmitted across the internet is an imperative issue, as it is affected by many serious problems such as hacking, duplications and malicious usage of digital information. Some of the information transmitted online may be vital and sensitive, and in such cases the senders have to take information security issues into consideration. Being a type of secret sharing, steganography can be used in this regard. The goal of steganography is to conceal the very existence of the secret data embedded in a cover medium in such a way that it should be undetectable and robust. Any digital medium such as text, images, audio files, video files, network protocols etc. can