Applied Soft Computing xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

A novel algorithm for colour image steganography using a new intelligent technique based on three phases

Nameer N. El-Emam [a,*], Mofleh Al-Diabat [b]

[a] Department of Computer Science, Philadelphia University, Amman, Jordan
[b] Department of Computer Science, Al al-Bayt University, Mafraq, Jordan

ARTICLE INFO

Article history:
Received 13 April 2014
Received in revised form 8 August 2015
Accepted 22 August 2015
Available online xxx

Keywords:
Data hiding
Steganography
Rich model
Steganalysis
Image segmentation
Neural networks
Genetic algorithm

ABSTRACT

A three-phase intelligent technique has been constructed to improve the data-hiding algorithm in colour images with imperceptibility. The first phase of the learning system (LS) has been applied in advance, whereas the other phases have been applied after the hiding process. The first phase has been constructed to estimate the number of bits to be hidden at each pixel (NBH); this phase is based on adaptive neural networks with an adaptive genetic algorithm using upwind adaptive relaxation ($LS_{ANN-AGAUpAR1}$). The LS of the second phase ($LS_{ANN-AGAUpAR2}$) has been introduced as a detector to check the performance of the proposed steganographic algorithm by creating a rich images model from available cover and stego images. The LS of the last phase ($LS_{CANN-AGAUpAR3}$) has been implemented through three steps, and it is based on a concurrent approach to improve the stego image and defend against attacks. The adaptive image filtering and adaptive image segmentation algorithms have been introduced to randomly hide a compressed and encrypted secret message into a cover image. The NBH for each pixel has been estimated cautiously using 32 principle situations (PS) with their 6 branch situations (BS). These situations have been worked through seven layers of security to augment protection from attacks. In this paper, hiding algorithms have been produced to fight three types of attacks: visual, structural, and statistical attacks. The simulation results have been discussed and compared with new literature using data hiding algorithms for colour images. The results of the proposed algorithm can efficiently embed a large quantity of data, up to 12 bpp (bits per pixel), with better image quality.

1. Introduction

The steganography algorithm, which uses spatial-based schemes to embed data into pixels within the cover image directly, is one of the most important strategies in the field of data security. This algorithm is a type of camouflage that can embed encrypted data into cover media (e.g., text, image, audio, video) to generate stego-media. The confidential data cannot be observed in the stego-media; while it is transmitted on the public communication channels in common computer networks. The goal of the steganography algorithm is to conceal a large amount of secret data and also to transmit these data with the minimum imperceptibility to fight steganalysis [1].

A simple and well-known traditional scheme is the least significant bit (LSB) replacement technique [2]. This technique can embed a secret message in a cover image without producing distortions in the stego-image. However, the maximum payload capacity of LSB is limited because one bit is a replacement for each byte.

Many existing LSB-based schemes have been used to improve the hiding capacity and/or to reduce the distortion of the stego-image. These schemes are based on difference expansion (DE), hybrid edge detector, and reversible data hiding (RDH) algorithms, and adaptive pixel adjustment using soft computing and computational intelligence.

High capacity data hiding has been proposed by many researchers, but they did not present the effect of the security level against new attackers if the payload capacity has been increased. Al-Qershi and Khoo [3] presented a scheme based on difference expansion (DE) to increase the hiding capacity for medical images. Hiding high payload by employing the LSB substitution technique as a fundamental stage and taking advantage of the edge detection technique was proposed by Chen et al. [4]. Ioannidou et al. [5] applied image steganography by taking advantage of sharp areas in images to hide a large amount of data; this approach is based on a hybrid edge detector. Qu et al. [6] proposed a quantum

* Corresponding author. Tel.: +962 65540195; fax: +962 65695567.
E-mail addresses: Nemam@philadelphia.edu.jo (N.N. El-Emam), moflehd@aabu.edu.jo (M. Al-Diabat).

http://dx.doi.org/10.1016/j.asoc.2015.08.057
1568-4946/

steganography protocol with a large payload based on quantum secure direct communication using entanglement swapping and building up a hidden channel within the improved ping-pong protocol to transmit secret messages.

The reversible image steganographic scheme provides the ability to embed secret data into a host image and later recover the host image without losing any information when the secret data are extracted. However, the reversible techniques do not generate a high-quality stego image, and the values of the statistical and visual measures are average. Lee et al. [7] presented an adaptive, reversible data scheme based on the prediction of difference expansion. Yang et al. [8] constructed a reversible data hiding (RDH) algorithm based on a gradient-based edge direction prediction (GEDP) scheme. Chang et al. [9] presented an index compression and reversible data hiding scheme based on side-match vector quantization (SMVQ) and search order coding (SOC). A framework in lossless and reversible data hiding research based on the histogram difference shift was proposed by Feng and Fan [10]. Lin et al. [11] introduced reversible data hiding to fully recover the original host image after extracting the secret message. A reversible image steganographic scheme based on predictive coding was proposed by Wu et al. [12] to embed secret data into compression codes during the lossless image compression to provide a lossless hiding mechanism in the compression domain. Zeng et al. [13] presented a lossless data hiding scheme; the proposed scheme was based on pixel difference histogram shifting to spare space for data hiding. Pixel differences are generated between a reference pixel and its neighbours in a pre-assigned block. A reversible data hiding method for natural images created by constructing a multilevel histogram based on differences between pairs of adjacent pixels was presented by Zhaoa et al. [14]. Lee and Chen [15] applied an adaptive reversible data scheme based on the prediction of difference expansion.

In the literature concerning data camouflage methods, there is research to raise the amount of data hiding in the stego image while maintaining the quality of the stego image; nevertheless, the quality of the stego image has been restricted due to the conventional tools that have been used to develop stego images. Eslami and Ahmadabadi [16] proposed a polynomial-based secret image sharing scheme with two achievements, the first was the proposal of embedding according to the size of the hidden data, and the second was the introduction of an authentication chaining method. An embedding scheme with minimal distortion was proposed by Lin [17], for which the message to be embedded was divided into sub-messages, each of which was embedded into a pixel vector with three pixels instead of one pixel. Sajedi and Jamzad [18] introduced a boosted steganography scheme (BSS) that uses a pre-processing stage before applying the steganography methods, where the goal of the BSS is increasing the undetectability of stego images. Liu et al. [19] proposed an image hiding scheme based on the scrambling process composed of the rotation of the squared sub-image in the gyrator transform domains. Yu et al. [20] constructed a distortion-free data hiding algorithm that can embed secret messages into high dynamic range (HDR) images to satisfy three significant benefits. First, the algorithm can convey secret messages to produce a stego image. Second, adaptive message embedding is used to conceal different amounts of secret messages based on their homogeneous representations, and third, efficient time required for message embedding or extraction is efficient.

The rest of the paper is structured as follows: in Section 2, a brief review of related works is presented. In Section 3, the proposed steganography with seven layers of security is discussed. The steps of the proposed steganography algorithm are provided in Section 4. In Section 5, the learning system based on three phases using adaptive neural networks and an adaptive genetic algorithm with upwind adaptive relaxation is discussed. In Section 6, the implementation images are introduced to demonstrate data hiding for colour images. A discussion of the results is presented in Section 7. Finally, Section 8 summarizes the primary conclusions of the proposed algorithm.

2. Related works

A rapid growth in steganalysis techniques using a support vector machine (SVM) to detect steganography has become a large challenge in recent years [1]. Therefore, intelligent techniques have been developed by many researchers within the field of data hiding to fight steganalysis. These techniques are based on soft computing using neural networks, ant colony optimization (ACO), practical swarm optimization (PSO), genetic algorithm (GA), and adaptive immune system (AIS). However, the number of studies using meta-heuristics on an image steganography algorithm is limited. These algorithms do not cover a wide range of attacks (visual, structural, and statistical).

Zhang et al. [21] applied a method of information-hiding capacity using a traditional neural network on attractors and attraction basins. This method had been applied on grey images, and the quality of the stego images was not typical. Embedding secret data into the compression codes of colour images using a genetic algorithm was proposed by Chang et al. [22], for which the scheme GA-AMBTC was based on a conventional genetic algorithm. A data embedding scheme using hybrid adaptive neural networks with an adaptive genetic algorithm and uniform adaptive relaxation ANN_AGAUAR was proposed by El-Emam and AL-Zubidy [23]; this approach focused on hiding a large amount of data in colour images. This approach reduced the effect of statistical and visual attacks. In addition, the quality of the stego image produced by this algorithm was not commensurate with the complexity of the steganography algorithm. The particle swarm optimization algorithm (PSO) was introduced by Li and Wang [24] to improve the quality of the stego images by deriving a substitution matrix to transform the secret messages using the PSO algorithm, where the scanning of the pixels is not random but is based on a zigzag scanning order. Furthermore, this approach was applied on grey images, but the quality of stego image was not typical.

Najafi [25] trained a neural network to determine the perceptual masking model of the human vision system, for which the neural network identifies pixels whose most significant alteration is least perceptible to the human eye. This method is only effective against visual attacks. Two schemes were suggested by Lin and Chang [26]. These schemes are the compact covering scheme (CCS) and the intelligent compact covering scheme (ICCS), which directly compress and conceal the repeated bit-blocks of secret data bits into covering images to exploit the embedding capacity and to increase the embedding efficiency. This approach uses zigzag scanning on uniform blocks with of size 6×6 on grey images to conceal/extract secret data. The two intelligent schemes for the embedding process did not prove that the proposed approach was successful for protecting against attacks.

In this paper, we propose a new data hiding algorithm based on three phases of intelligent techniques; these phases have been employed effectively in a rich model to confirm the ability to fight three types of attacks (visual, structural and statistical attacks). The proposed intelligent approaches are based on adaptive neural networks with adaptive genetic algorithms based on upwind adaptive relaxation ANN_AGAUpAR. Furthermore, the hiding algorithm has been created using seven security layers to hide a large amount of secret messages in a colour image with high imperceptibility and high protection of the secret message.

The differences between the proposed and other intelligent techniques are discussed in Section 7, and the results confirmed

Please cite this article in press as: N.N. El-Emam, M. Al-Diabat, A novel algorithm for colour image steganography using a new intelligent technique based on three phases, Appl. Soft Comput. J. (2015), http://dx.doi.org/10.1016/j.asoc.2015.08.057