COMPUTERS & SECURITY 55 (2015) 21–45

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

# New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization

*Nameer N. El-Emam* *

*Department of Computer Science, Philadelphia University, Jordan*

ARTICLE INFO

*Article history:*
Received 12 November 2013
Received in revised form 20 April 2015
Accepted 28 June 2015
Available online 8 July 2015

*Keywords:*
Image segmentation
Steganography
High payload
Adaptive neural network
PSO
Finite elements

ABSTRACT

A new steganography algorithm based on five protection layers has been suggested in this paper for embedding a large amount of secret messaging in a color image, as represented in the spatial domain. The suggested hiding algorithm employs an impressive image segmentation algorithm that uses two levels of adaptive non-uniform segmentation (TLANUS) to embed data randomly instead of sequentially. For each byte and for each color in a cover image, a non-uniform number of bits to be replaced by secret bits is imposed, depending on the byte characteristic's assessment using a weighting factor (ω) that is created from a cipher key (ck) to damp the difference in the surrounding twelve high bytes for the current byte (b). A learning machine has been proposed to adjust a pixel's value; this machine is based on an adaptive neural network (ANN) with modified particle swarm optimization (MPSO). However, the PSO modification has been introduced using a second-order differential equation (SODE); this approach is applied to optimize the positions of the particles, where the adaptive finite-element method (AFEM) is used to find the approximate solution of the SODE. The experimental results have been discussed regarding different performance measures; these measures have demonstrated the effectiveness of the proposed steganography algorithm with the machine learning ANN_MPSO in terms of its embedding capacity and imperceptible level. Comparisons between the proposed approach and the wide spectrum of steganographic schemes have been implemented. The results confirm that the stego-image with high imperceptibility has been reached even if the stego-image holds a large amount of data that reaches twelve bits per pixels (12-bpp) at certain bytes. In addition, it is confirmed that the proposed algorithm can embed secret data efficiently with better visual quality and working under rich image models to confirm that the present approach is resistant to attacks.



## 1. Introduction

Steganography is the science of hiding data, and it is a type of disguise that enables hiding encrypted secret data in cover media (e.g., text, image, audio, and video) to produce stego-media. The secret data cannot be observed in the stego-media while it is transmitted on public communication channels in common types of computer networks. The intention of a steganography algorithm is not only to hide a large amount of secret data but also to communicate those data without triggering suspicion (Filler et al., 2011; Fridrich, 2009; Pevný et al., 2010).

* Tel.: + 0096265540195.
*E-mail address:* Nemam@philadelphia.edu.jo
http://dx.doi.org/10.1016/j.cose.2015.06.012
0167-4048/

A novel image steganographic technique based on the Voronoi diagram (dividing space into a number of regions) was proposed by Cui et al. (2012) to generate a Voronoi diagram of a graph transformed from a cover image (CI); those diagrams were generated from the Voronoi points that correspond to every two consecutive pixels within the cover image. Lee and Chen (2012) proposed a new scheme with reversible data hiding where the computational cost associated with the embedding and extracting was lower than that of most of the DE-based schemes, but the additional information of the location-map was needed to solve the underflow and overflow problems. Moreover, a reversible data-hiding method based on prediction-error expansion was proposed by Qin et al. (2012), where each pixel of the cover image, excluding the first row and first column, was predicted by its top and left neighboring pixels in the raster-scanning order. This prediction process produced a small prediction error and achieved a high embedding rate and good visual quality of the stego-image (SI) by the expansion of the prediction error. However, the information at the peak point was required in the procedure of extracting the embedded data and recovering the cover image. Efficient algorithms to hide a large amount of data were proposed by El-Emam (2007) and Saleh et al. (2010). Cetin and Ozcerit (2009) proposed two new steganographic algorithms to utilize similar and dissimilar histograms, where both algorithms had been based on two parameters, the perceptibility and capacity of a cover video using proper pixel selection.

Recently, a data-hiding method was modified by many researchers to increase the amount of hiding data without suspicion and to improve the quality. Liu et al. (2013) proposed an image hiding scheme based on the scrambling process composed of the rotation of a squared sub-image in the gyrator transform domains, where a squared sub-image was first selected from a secret image and was rotated along an axis, which was the center line or diagonal line of the sub-image. El-Emam and AL-Zubidy (2013) constructed a new steganography algorithm based on non-uniform adaptive image segmentation (NUAIS) and machine learning (ANN_ AGAUAR), to conceal successfully a large number of secret messages in a color image.

Chang et al. (2013) proposed a new index compression and reversible data-hiding scheme; this approach was based on side-match vector quantization (SMVQ) and search order coding (SOC). Hong et al. (2013) proposed a method that exploits the nearest neighboring pixels to predict the visited pixel value and to estimate the corresponding "just noticeable difference" (JND) of the current pixel, and they employed an embedding level selection mechanism to prevent near-saturated pixels from being over modified. An efficient reversible data-hiding algorithm based on a new gradient-based edge direction prediction scheme was proposed by Yang et al. (2013). This scheme can generate more accurate prediction results, and the prediction errors produce better quality in the marked images. Huang and Chang (2013) proposed a new method for reversible data hiding by employing hierarchical relationships of the original images using many parameters to access the performances of the reversible data-hiding algorithms; these parameters are the output image quality, the hiding capacity, and the overhead for decoding. The reversible data-hiding scheme for high-quality images was proposed by Guo and Tsai (2012) and Wang et al. (2013) in a spatial domain. This technique increased the embedding capacity and enhanced the image quality, and this scheme classifies all of the pixels as wall pixels and non-wall pixels. Chaumont et al. (2013) presented a method to protect the color information of images by providing free access to the corresponding gray-level images, and it is based on a color reordering algorithm after a quantization step. Chang et al. (2010) applied two novel techniques for an edge detector, where the first is to increase the robustness to guard against detectors while the second is to improve the payload and enhance the quality of the stego image. Luo et al. (2010) implemented LSB matching, revisiting image steganography and an edge adaptive scheme that can select the embedding regions according to the size of the secret message and the difference between two consecutive pixels in the cover image. Phadikar and Maity (2011) propose joint data-hiding and data modulation schemes to serve the purpose of quality access control of image(s) using quantization index modulation (QIM). Qu et al. (2010) proposed a novel quantum steganography protocol based on quantum secure direct communication using entanglement swapping of Bell's states; the protocol built up hidden channels within the improved ping-pong protocol to transmit secret messages. Qian and Zhang (2012) proposed a lossless data-hiding method to embed secret data into a JPEG bitstream by Huffman's code mapping. Sajedi and Jamzad (2010) introduced a boosted steganography scheme (BSS) that has a preprocessing stage before applying steganography methods. Wu et al. (2011) proposed a novel secret image-sharing scheme by applying an optimal pixel adjustment process to enhance the image quality under different payload capacities and various authentication bit conditions.

In the past few years, a number of researchers in the field of data-hiding applied intelligent computing algorithms based on Practical Swarm Optimizer (PSO) to obtain powerful, low cost, and optimal data-hiding algorithms. Li and Wang (2007) show a novel steganographic method that is based on JPEG and a Particle Swarm Optimization algorithm (PSO) to improve the quality of a stego image by means of an optimal substitution matrix for transforming the secret messages. A novel method to embed a secret message in the cover image was presented by Fazli and Kiamini (2008), for which the interceptors will not notice the existence of the hidden data in the least significant bit (LSB); to improve the quality of the stego image and increase the secret message capacity and protection level, the proposed scheme splits the cover image into n-blocks of $8 \times 8$ pixels and the secret message into n-partitions and then applies the Particle Swarm Optimization (PSO) algorithm to search approximate optimal solutions and find an optimal substitution matrix for transforming the secret message in each block. Rabevohitra and Sang (2012) presented a steganographic scheme for a JPEG compressed image with a high capacity and good quality. This approach quantizes a table of size $16 \times 16$ instead of the commonly used size $8 \times 8$ at the most JPEG compression to reach a high capacity, while PSO is applied to obtain good quality with an optimal substitution matrix to transform the secret data into the best fit in a cover image before the embedding process. A novel approach for image steganography that takes advantage of Particle Swarm Optimization (PSO) and the least bits (LSBs) replacement has been proposed by Nickfarjam and Azimifar (2012); this technique was based on hiding the most significant bits (MSBs) of the secret