New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm

Nameer N. El-Emam a,⁎, Rasheed Abdul Shaheed Al-Zubidy b

a Department of Computer Science, Philadelphia University, Jordan
b Department of Computer Information System, Philadelphia University, Jordan

1. Introduction

Steganography algorithm is kind of camouflage that allows to embed the encrypted data into cover media (e.g. Text, image, audio, video, etc.) to generate stego-media. The secret message (Smsg) cannot be seen in the stego-media while it is transmitted on public communication channels in the common types of computer networks. The goal of steganography algorithm is not only to conceal a large amount of secret messages but also to transmit these imperceptible messages; this is done by different techniques and used by many researchers (Filler et al., 2011; Fridrich, 2009; Pevný et al., 2010).

Wang and Moulin (2008) constructed perfectly secure steganographic by embedding the message into the cover-text. The resulting Stego-image (I₁) has exactly the same probability distribution as the cover-text. El-Emam (2007) proposed an efficient algorithm to hide a large amount of data into the color bitmap image and to work against statistical and visual attacks. Munuera (2007) shown some relations between steganographic algorithms and error-correcting codes, these relations are used to construct good steganographic protocols and deduces their properties from those of the corresponding codes. Sajedi and Jamzad (2010) introduced boosted steganography scheme (BSS) that has a preprocessing stage before applying steganography methods. The goal of BSS is increasing the undetectable of I₁. Qian and Zhang (2012) proposed lossless data hiding method to embedding secret data into JPEG bitstream by Huffman’s code mapping. 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 builds up hidden channel within the improved ping-pong protocol to transmit secret messages. Lee and Chen (2010) proposed a novel data hiding scheme that uses a simple modulus function to address four performance criterion (the embedding capacity, the visual quality of the I₁, the security, and the complexity of the data-embedding algorithm). Lee et al. (2010) presents an adaptive reversible data scheme based on the prediction of difference expansion; this scheme gains from embedding capacity by taking full advantage of the large quantities of smaller

⁎ Controversy corner. It is the intention of the Journal of Systems and Software to publish, from time to time, articles cut from a different cloth. This is one such article. The goal of CONTROVERSY CORNER is both to present information and to stimulate thought and discussion. Topics chosen for this coverage are not just traditional formal discussions of research work; they also contain ideas at the fringes of the field’s “conventional wisdom”. These articles will succeed only to the extent that they stimulate not just thought, but action. If you have a strong reaction to the article that follows, either positive or negative, send it along to your editor, at card@software.org. We will publish the best of the responses as CONTROVERSY REVISITED.

⁎⁎ Corresponding author. Tel.: +962 7 77489308; fax: +962 2 6374444.
E-mail address: nemam@philadelphia.edu.jo (N.N. El-Emam).