Applied Soft Computing 67 (2018) 505–518

Contents lists available at ScienceDirect

Applied Soft Computing

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

Robust steganographic method based on unconventional approach of neural networks

Robert Jarusek, Eva Volna, Martin Kotyrba *

University of Ostrava, Department of Informatics and Computers, 30. dubna 22, 70103, Ostrava, Czech Republic

ARTICLE INFO

Article history:
Received 7 September 2017
Received in revised form 14 March 2018
Accepted 18 March 2018
Available online 26 March 2018

Keywords:
Steganography
Robustness
Watermark
Neural network
Discrete cosine transform – DCT

ABSTRACT

The article deals with the issue of using an apparatus of neural networks in the area of steganography. A new method called STEGONN was proposed. The proposed method is robust enough to an attack and the hidden message hard to be falsified. The core of our work lies in a design and implementation of a method for the use of neural networks as a native coder and decoder of a secret message (digital watermark) with an emphasis on the minimum necessary level of image data modification – covermedium. A covermedium is not perceived as a passive cover of a secret message, but we make active use of cover medium data, primarily its data markers (image markers) to insert a secret message. The advantage over other steganographic methods is the fact that the method implicitly offer the possibility to detect corrupted parts of the stegomedium and inform the user about possible manipulation with the image. The characteristics of the proposed method have been experimentally verified and compared with commercially available steganographic applications.

1. Introduction

The aim of steganography is to hide a message (information, data) in a place where no one expects it while its presence is not detectable. Authors [11] mention three aspects of assessing systems for hiding information:

- capacity
- security
- robustness

Capacity is understood as the amount of information which can be hidden in the medium, *security* represents impossibility of an intruder to reveal the secret message, and *robustness* expresses the capability of the medium to hold hidden data even after its possible modification. The steganographic process is depicted in Fig. 1

The issue of hiding information in graphical data is complicated primarily due to its demands on sufficient robustness and capacity to insert a secret message into image data, where the data should be modified the least possible. An ideal state is when a secret information is inserted into image data so that the image data itself (covermedium) is not modified in any way, i.e. covermedium = stegomedium.

2. Current steganographic methods

Currently, there are four basic steganographic methods, namely: End Of File (EOF) [3], Least significant bit (LSB) [9], and methods based on the use of Discrete Cosine Transform (DCT) [1] or Discrete Wavelet Transform (DWT) [4]. Models to effectively calculate the degree of digital image's trustworthiness are mentioned in [14]. Table 1 provides a comparison of selected Steganographic approaches. The levels where individual algorithms meet the requirements are defined as none, low, medium, and high. The comparative criteria are as follows:

- Visibility: subjective visibility of a secret message in a stegomedium
- PSNR (*peak signal-to-noise ratio*) expresses the ratio between the maximum possible energy of signal and the energy of noise defined by the relation (1)

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX}{\sqrt{MSE}}\right) \quad (1)$$

where *MAX* is the maximum possible value of a pixel in an image (i.e. 255 for 8 bits per channel).

* Corresponding author.
E-mail addresses: robert.jarusek@osu.cz (R. Jarusek), eva.volna@osu.cz (E. Volna), martin.kotyrba@osu.cz (M. Kotyrba).

https://doi.org/10.1016/j.asoc.2018.03.023
1568-4946/

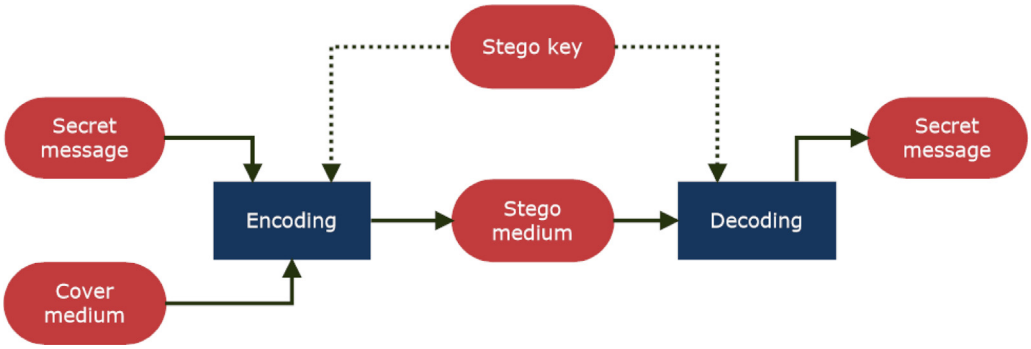

Fig. 1. Steganographic process – message coding and decoding.

Table 1
Comparison of selected steganographic methods.

	EOF	LSB	DCT	DWT	Ideal method
Visibility	none	low	high	medium	none
PSNR	none	low	medium	medium	none
Capacity of medium	high	high	low	low	high
Robustness	none	low	high	medium	high
Security	none	low	medium	medium	high
Computational complexity	low	low	high	medium	low

MSE (*mean squared error*) for two black-and-white images *I* and *K* of dimensions M × N is defined by the relation (2):

$$MSE = \frac{1}{M \cdot N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} (I_{m,n} - K_{m,n})^2 \quad (2)$$

- *Capacity of the medium:* amount of information which can be hidden in the medium
- *Robustness:* ability of the stegomedium to hide a secret message even after its possible modification
- *Security:* resistance of the stegomedium against counterfeiting of a secret message
- *Computational complexity*: amount of time required to insert a secret message into a covermedium

In the following part, we will consider only neural network approaches. The neural network has an admirable ability to simulate any nonlinear correlation. Therefore, neural networks are used in steganography primarily as classifiers [12], where a feed-forward neural network with backpropagation learning process is utilized as the categorizer. Authors proposed a steganalysis system that has pointed out a promising way towards blind and practically powerful steganalysis. In [17], the authors presented a steganalysis technique based on a statistical analysis on the texture of an image for the detection of wavelet domain information hiding techniques. They applied backpropagation neural network approach as a separator to differentiate non stegoimages and stegoimages. Experimental results have proved that the proposed algorithm is more effective compared with previously existing techniques. In [19], the authors presented a method based on backpropagation neural network to get statistical features of images to identify the underlying hidden data. Then the estimation ability of the neural network for demonstrating either an image is non stego or stego image was utilized. Experiment results show that the method is valid in steganalysis and can be used for network security, watermarking, etc. In [18], a steganalysis technique is proposed for a pixel-value differencing method. This steganographic method, which is immune against conventional attacks, performs the embedding in the difference of the values of pixel pairs. Therefore, the histogram of the differences of an embedded image is different as compared with a cover image. The authors presented five different n-level perceptron neural network approaches trained to discover diverse layers of implanting. Every image is served to all systems and selecting scheme classifies the image as either cover images or stego images. Implementation of the estimator showed an average accuracy of 88.3% in the estimation of the amount of embedding. In [5], the authors proposed a blind steganalysis method which depends on a universal neural network approach and matches it to Stegdetect – a kind of a tool that uses a linear classification device. In [8], the authors presented an overview of neural-network-based methods that are acceptable to distinguish its efficiency for steganalysis. In [13], Hopfield neural networks are used as envelopes for chaotic representation of processed data. An overview of techniques based on neural networks is listed in [6]. Other steganographic techniques from the area of softcomputing based on a hybrid optimization of PSO and genetic algorithm, which allows us to find an optimal secret key, are mentioned in [15].

Since there are various ways of implementation of steganography techniques, it is obvious that the basic foundation stone of most steganographic approaches is inserting a no matter how compressed or ciphered secret message into the least significant and noticeable parts of the covermedium (LSB, high coefficients in discrete transformations DFT, DCT, DWT). The main approach is the idea that a covermedium as the holder of a secret message is only a passive receiver of useful steganographic information and data representation of the covermedium as such, primarily its data entropy, is unimportant for implementation of the secret message. Thus, the proposed method STEGONN is focused on active and targeted use of data representation of a covermedium for intelligent inserting of a secret message, whose inserting, the way of inserting, and subsequent extraction are directly conditioned and led by the structure of the covermedium.

3. Method STEGONN

The proposed method STEGONN [7] contains an apparatus of neural networks for intelligent inserting of a secret message into image markers of a covermedium while those markers represent the configuration of the used neural networks. A secret message is not inserted into the covermedium directly, but the covermedium contains only information how to extract the message. This approach significantly increases robustness and security of the described steganographic method. The approach introduces the core of the proposed method STEGONN and according to the performed research, nothing similar has been published so far.

3.1. Encoding of a message

The following flowchart (Fig. 2) represents a process of encoding a secret message.