Nigerian Research Journal of Engineering and Environmental Sciences 6(2) 2021 pp. 476-482
p ISSN: 2635-3342; e ISSN: 2635-3350

Nigerian Research Journal of Engineering and Environmental Sciences
Journal homepage: www.rjees.com

Original Research Article

Using Artificial Neural Network to Analyze Stego Images

[1]Nkuna, M.C., *[1,2]Esenogho, E. and [1]Heymann, R.

[1]Centre for Collaborative Digital Networks, Department of Electrical and Electronic Engineering Science, Faculty of Engineering and Built-Environment, University of Johannesburg, P.O Box 524, Auckland Park, 2006, South Africa.
[2]Department of Computer Engineering, Faculty of Engineering, University of Benin, PMB 1154, Benin City, Edo State, Nigeria.
*ebenezer.esenogho@uniben.edu

http://doi.org/10.5281/zenodo.5805077

ARTICLE INFORMATION

Article history:
Received 11 Aug, 2021
Revised 27 Sep, 2021
Accepted 01 Oct, 2021
Available online 30 Dec, 2021

Keywords:
Least significant bits
Stego-image
Artificial neural network
Artificial intelligence
Steganography
Discrete cosine transform

ABSTRACT

This paper proposed a discrete cosine transform least significant Bit-2 steganography encryption method for embedding the secret data in the cover image. The method overcomes physical signs of pixel modifications while achieving a high data payload. This technique enables data to be hidden in a cover image, while the image recognition artificial neural network checks the presence of any visible alterations on the stego-image. The traditional least significant bit (LSB) and the proposed discrete cosine transform least significant bit-2 (DCT LSB-2) methods were tested for embedding efficiency. The stego-images obtained from the embedding process using the traditional LSB and the proposed DCT LSB-2 encoding algorithms were analyzed using a neural network. Results obtained from the proposed DCT LSB-2 method achieved high data payload and simultaneously minimized visible alterations, and maintained the efficiency of the neural network compared with the traditional LSB. The proposed method has shown an improved stego-system compared to traditional LSB techniques.

1. INTRODUCTION

The strategy of steganography has been widely studied to covertly transmit data between people. Nowadays, the internet, online shopping, online reservations, and online payments, etc., are the main source of information exchange. With this advancement, there is a need to protect information to evade detection from unauthorized interceptors. Steganography becomes more significant as more people join the cyberspace revolution. Due to the developments in information communication technology (ICT), most of the

information is saved electronically. Thus, the security of information has become an important issue. Besides cryptography, steganography can be used to hide and protect information (Singh *et al*., 2018).

Studies have in the past implemented image steganography in a traditional way, whereby the secret information hidden in the cover media was purposefully embedded with a focus such that the human visual system would not detect that there is information hidden in the cover image (Gayathri *et al*., 2017). The focus of this paper is that there is an existing image recognition artificial neural network system that is already in place. However, there is a need to implement the image steganography technique such that it does not break the existing artificial neural network (avoid the image recognition ANN from misclassifying stego images).

The discrete transform method inserts the secret data in the cover image by altering the coefficient in a transform domain. This transform domain can be a discrete Fourier transform (DFT) or a discrete wavelet transform (DWT). The transform techniques are more complex to implement, and they apply alterations of the discrete cosine transform (DCT) (Patel *et al*., 2014; Nath *et al*., 2017). The DCT is the commonly used transform technique. The cover image is converted from the spatial to the frequency domain. The higher-order DCT coefficients correspond to fine features and low-order DCT coefficients correspond to a large feature of pixels. High-order coefficients are used for implanting the secret data. The inserting process is achieved by solely altering the DCT coefficients (Pannu, 2015). DCT technique allows the effects of spreading the location of the pixels over the entire image. Hence, the method is limited for small-scale secret data and the secret information is more secured against hackers and unauthorized detection (Krishna *et al*., 2018). The DCT is used by joint photographic experts group (JPEG) compression algorithms and it transforms consecutive 8x8 pixel blocks of the cover image into 64 DCT coefficients each.

In Nkuna et al. (2020), the author integrated a smartphone network architecture and data security techniques to mitigate sharp practices in non-profit organizations (NPOs). The author explored how image steganography models can be implemented in a mobile smartphone to come up with an app that can be used to counteract the mismanagement of resources in non-profit organizations. The author proposed a variable size least significant bit algorithm to embed a time and date stamp on an image captured whenever there are events in the NPO. However, the amount of data that can be successfully hidden in the image without showing any visible properties of image manipulation was not investigated. This compromised the robustness of the system since Steganalysis can be detected on the resulting images with hidden information. This setback will however be taken into consideration in this current work. A similar technique was used in Esenogho *et al*. (2017a,b) using an artificial neural network technique for improving the prediction of credit card default employing a stacked sparse autoencoder approach for classification.

The key contribution of this paper is to propose a new steganography encoding technique (referred to as the DCT LSB-2 method) that is used in conjunction with an image recognition artificial neural network to achieve an improved data payload in a steganography system. The proposed method is compared to an existing LSB technique (Mathivanan *et al*., 2020).

2. METHODOLOGY

2.1. Proposed Encoding Scheme

The encoding scheme proposed for this study is illustrated in Figure 1. The algorithm uses a red green blue (RGB) cover image and a set of secret data bits of variable size depending on the size of the data that needs to be embedded. Both the cover image and secret data bits are fed into a DCT algorithm which maps the cover image's color gradient coefficient to a highly suitable coefficient of the secret data bits to ensure that there are no mismatches that may cause visible pixel alterations. Furthermore, the bits of the secret data are embedded (two at a time) on the bits of the cover image through the use of an LSB-2 substitution algorithm.

Then finally, the algorithm outputs a stego-image that consists of the embedded secret data bits and saves it as an RGB stego-image.

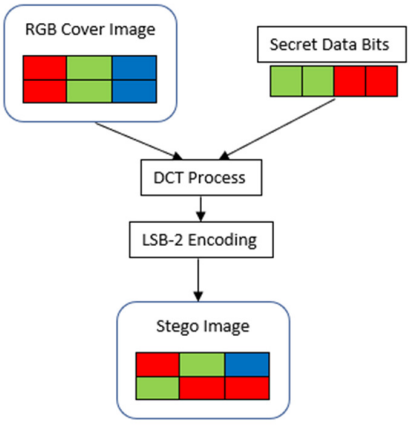

Figure 1: Proposed encoding scheme

2.2. Proposed Artificial Neural Network Architecture

Figure 2 presents the model of the proposed artificial neural network. The model was trained using 1000 images of different Coke cans. The model used 75% of the images (750 images) for training and 25% (250 images) for testing and validation. The blocks indicate the different processes for the model training and evaluation. The data image paths were fed into the neural network algorithm where the images were resized and flattened to ensure that they are all in the same dimension size. The images were further partitioned into 75% training and 25% validation. As indicated from Figure 2, the model was trained and evaluated (validated) using the stated partition weights, and the model was finally saved for testing prediction confidence in the stego-images that resulted from the traditional LSB and the proposed DCT LSB-2 techniques.

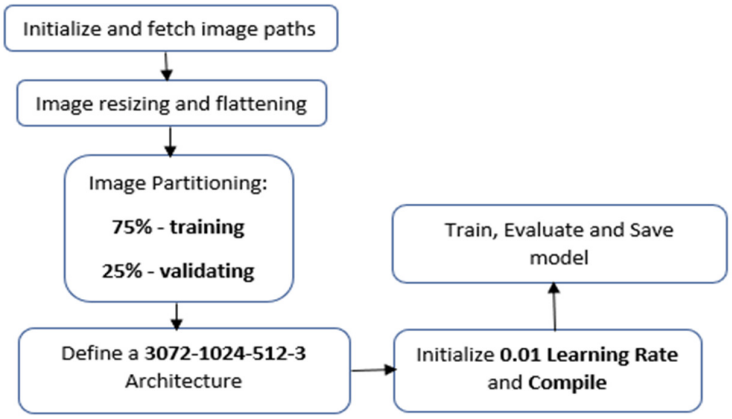

Figure 2: Proposed ANN model (Ebiaredoh-Mienye et al., 2021)

2.3. System Model

This proposed model takes as input the cover image and secret data. Then it feeds the input to the stego-system encoder implemented in JavaScript. The proposed DCT LSB-2 and traditional LSB encoding

algorithms were implemented (one at a time) to encode the secret data into the cover image and saves the resulting stego-image. An image recognition artificial neural network was used to classify the stego-image.

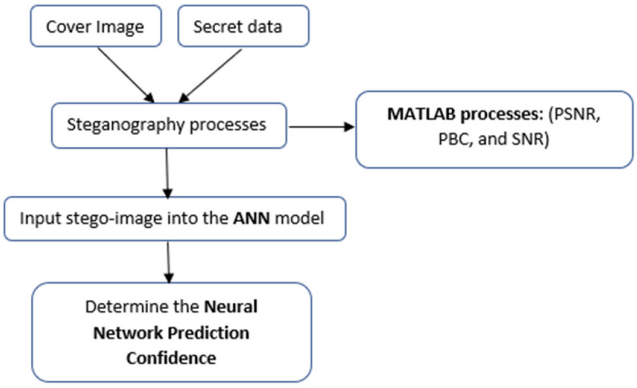

Figure 3: Functional model

The neural network was trained to recognize the nature of the stego-image before any secret data is embedded into the cover image and it classifies the image with certain prediction confidence in percentage. The stego-image was fed through a stego-system decoder and the DCT LSB-2 and LSB decoding algorithms were individually implemented to recover the hidden secret data. MATLAB was used to do the image processing functions and determines the performance parameters [Peak signal-to-noise ratio (PSNR), percentage of bytes changed (PBC), signal-to-noise ratio (SNR), and the mean square error (MSE)] of the stego-image. The size of the secret data is then increased slightly, while the same cover image is used to encode the secret data, and the previously explained steps are repeated until the neural network fails to recognize the resulting stego-image, then breaks. The size of the secret data embedded at the instant where the neural network breaks (misclassifies the stego-image) is the maximum secret data payload that can be hidden. The generic schematic diagram of the high-end design is shown in Figure 3.

2.4. Evaluation of the Proposed Method

The performance of the proposed method was evaluated by using the image parameters listed below and compared to the existing LSB technique. All the mathematical operations were implemented in MATLAB (Suresh *et al*., 2018).

2.4.1. Mean square error (MSE)

The MSE characterizes the collective squared error between the stego image and the original cover image and was calculated using Equation 1.

$$MSE = \frac{\sum_{P,Q}[I_1(p,q) - I_2(p,q)]^2}{P * Q} \quad (1)$$

Where I_1 and I_2 represent the cover image and the stego-image respectively. P and Q are the numbers of rows and columns of the cover and stego images respectively.

2.4.2. Peak-signal-to-noise ratio (PSNR)

The PSNR denotes a quantity of the highest error and was calculated using Equation 2.

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

Where R=255.

2.4.3. Percentage bytes changed (PBC)

The PBC was used to size the quality of the stego-image and was calculated using Equation 3.

$$PBC = \left(\frac{Number\ of\ Bytes\ Changed}{Total\ number\ of\ Bytes}\right) \times 100 \quad (3)$$

3. RESULTS AND DISCUSSION

3.1. PBC vs. NN Prediction Confidence Analysis for Existing LSB and Proposed DCT LSB-2 Methods

As observed from Figure 4, the LSB technique resulted in a decreased neural network efficiency for values of the percentage of bytes changed (PBC) greater than 35%, while the proposed DCT LSB-2 method constantly maintained the efficiency of the neural network throughout all the regions of the PBC. This means that as more than 35% of the image pixels are altered with the secret data, the LSB technique starts to decrease the neural network efficiency. Hence, it can be stated from Figure 4 that the proposed DCT LSB-2 method achieves the objective of maximizing the neural network efficiency and results in improved performance.

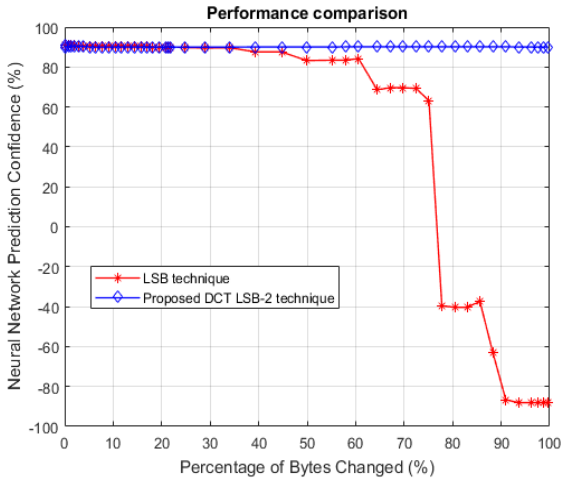

Figure 4: Performance comparison of LSB and the proposed DCT-2 techniques

3.2. Analysis of PBC vs. PSNR for LSB and Proposed DCT LSB-2 Methods

From Figure 5, it is clear that the proposed DCT LSB-2 method achieved a constant PSNR behavior (of greater than 40dB) throughout all the values of the PBC shown. This is in line with theory, which states that to achieve a stable steganography system, the values of the PSNR should be greater than 30dB to minimize visible pixel modification properties and thus achieves a robust system (Mathivanan et al., 2020). Hence the proposed method achieves improved performance.

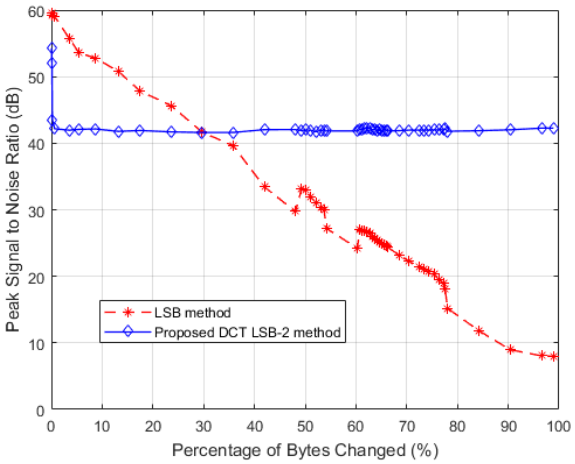

Figure 5: LSB vs. Proposed DCT LSB-2

4. CONCLUSION

This paper proposed an improved steganography encoding scheme that utilizes an existing image recognition ANN for validation. The proposed DCT LSB-2 method has resulted in improved performance compared to the LSB method. Furthermore, the proposed scheme achieves an improved data payload for the steganography system compared to other methods tested in previous studies.

5. ACKNOWLEDGMENT

This work was supported by the Centre of Collaborative Digital Networks, University of Johannesburg, South Africa. This research received no external funding however, and the APC will be paid from the research center's funds.

6. CONFLICT OF INTEREST

There is no conflict of interest associated with this work.

REFERENCES

Ebiaredoh-Mienye, S.A., Esenogho, E. and Swart, T. G. (2021). Artificial neural network technique for improving prediction of credit card default: A stacked sparse autoencoder approach. *International Journal of Electrical and Computer Engineering,* 11(5), pp. 4392-4402.

Esenogho, E. and Srivastava, V. M. (2017a). Channel Assembling Strategy in Cognitive Radio Networks: A Queuing-Based Approach. *International Journal on Communications Antennas and Propagation*, 7(1), pp. 31-47.

Esenogho, E. and Srivastava, V. M. (2017b). Two Heterogeneous Channel Assembling Strategies in Cognitive Radio Networks: A Performance Analysis. *International Journal of Engineering and Technology Innovation,* 7(2), pp. 98-116.

Gayathri, M. and Shaimaa M. H. (2017). Image Steganography Method using Zero Order Hold Zooming and Reversible Data Hiding. *International Research Journal of Engineering and Technology,* 4(8), pp. 198-206.

Krishna, M. M., Neelima, M., Harshali, M. and Rao, M. V. G. (2018). Image Classification using Deep Learning. *International Journal of Engineering and Technology,* 7(2), pp. 614-617.

Mathivanan, P. and Balaji-Ganesh, A. (2020). ECG steganography based on tunable Q-factor wavelet transform and singular value decomposition. *International Journal of Imaging Systems and Technology*, 31, pp. 270-287.

Nath, A., Roy, S., Gopalika, C. and Mitra, D. (2017). Image Steganography using Encrypted Message. *International Journal of Advanced Research in Computer Science and Management Studies,* 5(4), pp. 7-11.

Nkuna, M. C., Esenogho, E. and Heymann, R. (2020). Integrating Smartphone Network Architecture and Data Security Techniques to Mitigate Sharp Practices in Non-Profit Organisations. *Journal of Communication*, 15(10), pp. 755-767.

Nabofa-Ebiaredoh S. A., E. Esenogho and Swart, T. G. (2020). Integrating Enhanced Sparse Autoencoder Based Artificial Neural Network Technique and SoftMax Regression for Medical Diagnosis. *Mdpi Electronics Journal*, 9(11), pp.1963-1976.

Pannu, A. (2015). Artificial Intelligence and its Application in Different Areas. *International Journal of Engineering and Innovative Technology,* 4(10), pp. 79-84.

Patel, P. R. and Patel, Y. (2014). Survey on Different Methods of Image Steganography. *International Journal of Innovative Research in Computer and Communication Engineering,* 2(12), pp. 7614-7618.

Singh, W. G., Shikhar, M., Kunwar, S. and Kapil, S. (2018). Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map. *International Journal for Light and Electron Optics,* 170(10), pp.106-124

Suresh, K., Babu, A. R. V. and Venkatesh, P. M. (2018). Experimental investigations on grid integrated wind energy storage system using neuro fuzzy controller, Modelling, Measurement, and Control A. *International Information and Engineering Technology Association,* 91(3), pp. 123-130.