Using Artificial Neural Network to Test Image Covert Communication Effect

Caswell Nkuna1, Ebenezer Esenogho1,2,*, Reolyn Heymann1, and Edwin Matlotse2

1 Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg, South Africa; E-mail: 201598913@student.ac.za (C.N.), rheymann@uj.ac.za (R.H.)
2 Department of Electrical Engineering, University of Botswana, Gaborone; Email: matlotsee@ub.ac.bw (E.M.)
*Correspondence: ebenezere@uj.ac.za, Esenoghoe@ub.ac.bw (E.E.)

Abstract—Hacking social or personal information is rising, and data security is given serious attention in any organization. There are several data security strategies depending on what areas it is applied to, for instance, voice, image, or video. Image is the main focus of this paper; hence, this paper proposed and implemented an image steganography (covert communication) technique that does not break existing image recognition neural network systems. This technique enables data to be hidden in a cover image while the image recognition Artificial Neural Network (ANN) checks the presence of any visible alterations on the stego-image. Two different image steganography methods were tested: Least Significant Bit (LSB) and proposed Discrete Cosine Transform (DCT) LSB-2. The resulting stego-images were analyzed using a neural network implemented in the Keras TensorFlow soft tool. The results showed that the proposed DCT LSB-2 encoding method allows a high data payload and minimizes visible alterations, keeping the neural network’s efficiency at a maximum. An optimum ratio for encoding data in an image was determined to maintain the high robustness of the steganography system. This proposed method has shown improved stego-system performance compared to the previous techniques.

Keywords—Least Significant Bit (LSB), stego-image, Artificial Neural Network (ANN), steganography, TensorFlow

I. INTRODUCTION

The strategy of steganography has been widely studied to transmit data covertly between people. Nowadays, the internet, online shopping, online reservations, and online payments are the primary information exchange source. 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 information is saved electronically. Thus, the security of data has become an important issue. Besides cryptography, steganography can hide and protect information [1–3].

Techniques such as steganography in connection with artificial neural networks may be set up to help strengthen data security in these times of digital communication. This integration is essential because it works in real time and exists in the day-to-day application of secure information transmission. Secret information is hidden in digital cover media, and only the intended recipient has knowledge and access to the confidential information. While a lot of systems use neural networks nowadays, the focus area in this paper is based on investigating if image steganography can be applied without it interfering with existing neural networks [3].

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 pick up that there is information hidden in the cover image [4]. The focus of this paper is that there is an existing image recognition artificial neural network system already in place. However, the requirement is to implement the image steganography technique such that it does not interfere with the current image recognition artificial neural network. Ensure it can still recognize the stego-images, although with introduced additive noise in the image pixels due to lossy pixel compression. Fig. 1 illustrates the general process of steganography.

Figure 1. Steganography process.

To be precise, this study investigates the implementation of image steganography while simultaneously keeping the efficiency of an existing neural
network at the maximum. This investigation uses different digital cover images to embed secret data. Performance parameters of digital image processing will be used to investigate the appropriate thresholds and maximum data sizes that can be embedded while not destroying the visible properties of the digital cover image. The artificial neural network is used only to test the resulting stego-images and validate whether the two image steganography methods can be applied without breaking the neural network. The key contributions of this paper are as follows.

- Propose and implement an image steganography technique (proposed Discrete Cosine Transform Least Significant Bit-2 (DCT LSB-2)) that does not break existing image recognition neural network systems.
- Develop a TensorFlow platform in Keras to implement a simple image recognition artificial neural network to test if the data hiding system does not interfere with the neural network.
- Compare the LSB and the proposed DCT LSB-2 methods to determine the best algorithm to insert data in an image steganography system.
- Determine the maximum data payload of an image before the image is unrecognizable by an existing neural network using the two methods mentioned above.
- Ascertain the suitable steganography hiding algorithm (between the LSB and DCT LSB-2) that results in a higher data payload while not breaking the Artificial Neural Network (ANN).
- Establish the optimum rate for embedding information using the LSB and DCT LSB-2 methods.

The rest of the paper is organized as follows: Section II presents some previous related works utilizing different methods. A proposed methodology is presented in Section III. Section IV captures the proposed scheme, while the system model and assumptions are presented in Section V. The results obtained are presented and discussed in Section VI. Finally, the paper is concluded in Section VII.

II. RELATED WORKS

Umamaheshwari [5] proposed and analyzed several steganographic algorithms for secured data hiding. These include the LSB-1, LSB-2, LSB-3, and masking techniques in image steganography. This work did not investigate if these steganography methods do not interfere with existing neural networks. Hence, the work becomes unreliable and vulnerable in neural network detection. So, a need to investigate the implementation of image steganography that will not interfere with existing image recognition artificial neural networks arises.

Mathivanan and Ganesh [6] present a novel Electrocardiogram (ECG) steganography scheme based on the Tunable Q-factor Wavelet Transformation (TQWT) and Singular Value Decomposition (SVD) methods that ensure improved safety and confidentiality of patient information. The paper uses parameters such as Q, r, and J to decompose the cover signal into individual frequency sub-bands with the tunable Q-factor wavelet transformation. The SVD method decomposes high-frequency sub-band coefficients into single values. The techniques proposed by the authors are a profound advancement in the study of improved steganography techniques. The delimitation of this study is that it does not address the integration of neural network concepts into its work and only focuses on patient data confidentiality. This current paper proposes a technique that can be implemented in various fields of steganography application according to a particular requirement. It also integrates the aspects of Artificial Neural Network (ANN) use, gradually rising daily. Hence, this study becomes significant in its field and advances existing techniques.

Nath [7] did a study to investigate the advanced steganography algorithm using encrypted secret messages. Before the confidential data is embedded in cover media, the encryption algorithm requires a stego-key to encrypt the data before it is embedded in the cover media. This advancement is an improvisation of the security of confidential data. This research focused on hiding data so the human eye would not pick up the hidden data in the cover media. However, the limitation of this approach is that most systems nowadays use neural networks with very high recognition and detection properties. So, although this approach is robust for the human visual system, it becomes compromised in the evolving digital communications with neural network systems.

Krishna and Neelima et al. [8] studies the image classification technique using deep learning. The author investigated various algorithms for image recognition using artificial neural networks and convolutional neural networks. The author, in his study, applied different algorithms for implementing the classification of images by using additional trained artificial and convolutional neural network models. This study did not include any aspect of image steganography or any other data-hiding technique. This work relates to the current research presented in this article because an image recognition ANN is adopted for testing purposes after the implementation of image steganography in different cover images.

Nkuna and Esenogho et al. [9] integrates 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 develop 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 system’s robustness since steganalysis can be detected on the resulting photos with confidential information. However, this setback will be considered in this current work; hence, this work is an improvement of the work...
presented in [9]. A similar technique was used in [10] using an Artificial neural network technique for improving the prediction of credit card default employing a stacked sparse autoencoder approach for classification.

III. PROPOSED METHODOLOGY

In this section, the proposed model’s generic overview functional flow diagram is presented in Fig. 2. In contrast, the generic functional flow diagram of the image recognition ANN training model is shown in Fig. 3.

![Figure 2. Generic functional flow diagram of the proposed method.](image)

![Figure 3. Generic functional flow of the neural network training model.](image)

The model is trained using 1000 images of different coke cans. The photos were gathered from online sources, while some were captured using a mobile camera. When teaching the model, the photos were resized to a fixed size of $32 \times 32$ pixels before inputting them into the ANN. The $32 \times 32$ pixel size was chosen to ensure that the pictures do not take up a lot of computer memory space. Some resizing alternatives are $64 \times 64$ pixels, $128 \times 128$ pixels, etc.; however, these were not chosen due to the limitations of the computer space that was utilized for training the ANN model.

Furthermore, higher image pixels for resizing would result in a larger ANN and more extended time complexity during the training process considering the significance of the number of images used (1000 images). Hence, the $32 \times 32$ pixels fixed size was chosen for this work’s purposes and scope. The model uses 75% of the images for training and 25% for testing and validation. The rationale for choosing the 75/25 split was obtained from earlier studies, which found that the best results are obtained when 20–30% of the data is used for testing and the remaining 70–80% for training [8]. Hence, the 75/25 split was selected for this implementation. A Stochastic Gradient Descend (SGD) optimizer was used for the ANN training. The SGD optimizer used gradient fall along with momentum and was imported from the Keras library. After training, the model is saved so it can be used for the classification of the coke cans stego-images.

Image analysis is done using Eq. (1) [1–8]:

$$MSE = \frac{\sum_{p,q}[I_1(p,q)-I_2(p,q)]^2}{p \times q}$$  \hspace{1cm} (1)

The Mean Square Error (MSE) characterizes the collective squared error between the stego-image and the original cover image.

$$PSNR = 10 \log_{10} \left( \frac{R^2}{MSE} \right)$$  \hspace{1cm} (2)

The Peak-Signal-to-Noise-Ratio (PSNR) denotes the quantity of the highest error.

$$PBC = \left( \frac{Number\ of\ Bytes\ Changed}{Total\ number\ of\ Bytes} \right) \times 100$$  \hspace{1cm} (3)

Percentage Bytes Changed (PBC) is used to size the quality of the stego-image.

IV. PROPOSED SCHEME

To minimize the risk of detecting the hidden secret information, a DCT LSB-2 embedding scheme is proposed. The problem of sequence mapping due to the DCT LSB-2 method is resolved by randomly embedding the data in random pixels of the cover image. As a result, the secret message is in arbitrary pixels distributed over the cover image [11, 12].

![Figure 4. Variable size LSB-2 method.](image)
embedded in the cover image by modulating the coefficient in the transform domain [3, 9]. A graphical illustration of the technique is presented in Fig. 4.

This method inserts the confidential 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) [4, 12].

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 prominent part of pixels. High-order coefficients are used for implanting the confidential data. The inserting process is done by altering the DCT coefficients [13].

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 confidential information is more secure against hackers and unauthorized detection [12]. JPEG compression algorithms use the DCT, transforming consecutive 8 × 8 pixel blocks of the cover image into 64 DCT coefficients. The calculation of the DCT coefficient of a single 8 × 8 block of an image pixel is given in Eqs. (4) and (5) [5–7, 14–17].

\[ F_{p,q}(i,j) = \frac{1}{4} C(p) C(q) \sum_{i=0}^{7} \sum_{j=0}^{7} f(i,j) e^{-j \pi (i+0.5)p/8} e^{-j \pi (j+0.5)q/8} \]

\[ C(i) = \begin{cases} \frac{1}{\sqrt{2}}, & i = 0 \\ 1, & \text{otherwise} \end{cases} \quad \text{(5)} \]

A quantization operation is performed as in Eq. (6) [4].

\[ F_{q}(i,j) = \frac{F(i,j)}{Q(i,j)} \quad \text{(6)} \]

where \( F_{q}(i,j) \) is the quantized coefficient, \( F(i,j) \) is the original coefficient, and \( Q(i,j) \) is the quantization step size.

V. SYSTEM MODEL AND ASSUMPTIONS

The proposed model takes as input the cover image and confidential data. Then it feeds the information into the stego-system encoder implemented in JavaScript. The proposed DCT LSB-2 and LSB encoding algorithms are implemented (one at a time) to encode the secret data into the cover image and save the resulting stego-image. An image recognition artificial neural network is used to classify the stego-image.

The neural network is trained to recognize the nature of the stego-image before any confidential data is embedded into the cover image. It classifies the image with a certain prediction confidence in percentage.

This work assumes that the confidential data decoding process is not in the scope of this work. The secret data recovery is only reflected in the system flow model (Fig. 5) for information purposes since any data encoding process requires a decoding element. Hence, in this case, there is no focus on decoding the secret data as indicated by the red cross.

The stego-image is fed into MATLAB, which is used to do image processing functions and determines the performance parameters (PSNR, PBC, SNR, and the MSE) of the stego-image. The size of the secret data bits is increased, the same cover image is used to encrypt the confidential data, and the previously explained steps are repeated until the neural network fails to recognize the resulting stego-image, then breaks. The incremental size of the private data is not constant for the same encoding scheme but increases in the size of the same bits for different encoding techniques. The size of the private data embedded at the instant where the neural network breaks (misclassifies the stego-image) is the maximum secret data payload that can be hidden without destroying all the visible properties of the cover image.

When the stego-image starts showing observable alterations due to the additive noise caused by the secret data encryption, the corresponding neural network prediction confidence and the PBC of the stego-image are recorded. These values are regarded as the optimum prediction confidence and data payload. The schematic diagram of the high-end model design is shown in Fig. 5.

The cover images are not shuffled during the encoding process; instead, they are fed into the stegosystem encoder by a user as a png image file type. Whereby an algorithm (i.e., proposed DCT LSB-2) encodes a set of secret data bits into a specific pixel bit’s location of the cover image. The mapping of the pixel locations where the confidential data encoding process occurs is determined using the DCT coefficient calculation Eqs. (4) and (5). The proposed method does not use a random pixel modification procedure but uses a predefined pixel location calculated and mapped by the DCT calculation.

The complexity of the model has been capped with some assumptions to avoid being overly complicated. Only two encoding algorithms are tested in this work: the traditional LSB method and a proposed DCT LSB-2 algorithm. The proceeding LSB-3 & 4 algorithms were not tested due to complexity and computing resources limitation. Furthermore, the information decoding element is not in the scope of the work since the objective is to use a simple artificial neural network to test steganography encoding algorithms effectively. This model is implemented manually, so it is time-consuming now; however, automation can be implemented on the data size incremental and encoding processes.
VI. RESULTS AND DISCUSSIONS

The results obtained are illustrated and discussed in the sub-sections that follow.

A. Analysis of PBC vs. MSE for the LSB and Proposed DCT LSB-2 Techniques

Figs. 6 and 7 represent the relationship between the PBC and the MSE for different cover images using the LSB and the proposed DCT LSB-2 methods, respectively. It can be observed that when using the LSB technique, the MSE grows very steeply as compared to Fig. 7, which means that the image fidelity degrades much quicker when using the LSB method. Fig. 7 shows a more stable MSE in the entire PBC range. This improves performance by the proposed DCT LSB-2 method rather than the LSB method.

B. PBC vs. SNR Using the LSB and the Proposed DCT LSB-2 Techniques

To achieve a more robust steganography system, there is a requirement to maintain the SNR/PSNR of stego-images at maximum or approximately constant throughout the range of the PBC [1-4, 11, 13, 18].

Hence, as observed from Figs. 8 and 9, the proposed DCT LSB-2 method shows a more stable/constant SNR response in all the PBC regions than the LSB technique. It can be stated that the proposed method maximizes the efficiency of the neural network by keeping the SNR stable even at a higher data payload (higher PBC).

C. Optimum Rate for Hiding Data

As seen in Table I, the LSB technique’s average optimum rate of embedding capacity over the total pixels of the four cover images is 2.57275 bpp. Hence the equation of approximating the optimum secret data to embed before the image becomes unrecognizable can be modeled as in Eq. (7):

\[ q = 2.57275p \]  

where \( q \) is the optimum hidden data, and \( p \) is the total cover image pixel size.

<table>
<thead>
<tr>
<th>TABLE I. OPTIMUM EMBEDDING RATE—LSB TECHNIQUE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LSB Performance Parameter</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td><strong>Total Number of Cover Image Pixels</strong></td>
</tr>
<tr>
<td><strong>Embedding Capacity (Bytes)</strong></td>
</tr>
<tr>
<td><strong>Optimum Embedding Rate (Bpp)</strong></td>
</tr>
</tbody>
</table>
As shown in Table II, the average optimum rate of hiding data in the DCT LSB-2 technique is 2.529 bpp. Hence, the equation of the maximum DCT LSB-2 embedding payload before the stego image becomes unrecognizable is modeled as in Eq. (8):

\[ y = 2.529x \]  

(8)

where \( y \) is the optimum hidden data, and \( x \) is the total cover image pixel size.

<table>
<thead>
<tr>
<th>TABLE II. OPTIMUM EMBEDDING RATE—PROPOSED DCT LSB-2 TECHNIQUE</th>
<th>Performance Parameter</th>
<th>Cover Image1</th>
<th>Cover Image2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Cover Image Pixels (#)</td>
<td>50246</td>
<td>230400</td>
<td></td>
</tr>
<tr>
<td>Embedding Capacity (Bytes)</td>
<td>125000</td>
<td>592000</td>
<td></td>
</tr>
<tr>
<td>Optimum Embedding Rate (Bpp)</td>
<td>2.488</td>
<td>2.569</td>
<td></td>
</tr>
</tbody>
</table>

D. LSB vs. Proposed DCT LSB-2 Techniques

Comparison at Maximum Robustness

From the results in Table III, it can be stated that for both cover images with 259 \( \times \) 194 and 360 \( \times \) 640 pixels, respectively, the proposed DCT LSB-2 technique is the best encoding method for an image steganography system rather than the standard LSB technique. The DCT LSB-2 method yields higher PSNR values, lower mean square error, higher secret data payload, and maximum neural network prediction confidence than the LSB method. All these performance parameters yield the best robustness in the steganography system and maximize neural network efficiency.

<table>
<thead>
<tr>
<th>TABLE III. ROBUSTNESS COMPARISON—LSB AND PROPOSED DCT LSB-2 TECHNIQUES</th>
<th>Performance Parameter</th>
<th>Cover Image1 (259( \times )194 pixels)</th>
<th>Cover Image2 (360( \times )640 pixels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR (dB)</td>
<td>LSB</td>
<td>DCT LSB-2</td>
<td>LSB</td>
</tr>
<tr>
<td>18.067</td>
<td>42.268</td>
<td>14.449</td>
<td>33.14</td>
</tr>
<tr>
<td>MSE (square pixels)</td>
<td>1014.799</td>
<td>3.857</td>
<td>2334.427</td>
</tr>
<tr>
<td>Embedded Secret Data Size (Bytes)</td>
<td>93900</td>
<td>125000</td>
<td>450000</td>
</tr>
<tr>
<td>PBC (%)</td>
<td>72.57</td>
<td>96.6</td>
<td>75.11</td>
</tr>
</tbody>
</table>

Hence, from the comparison between the LSB and the DCT LSB-2 methods, the DCT LSB-2 is the best encoding algorithm to use in an image steganography system.

E. Optimum Data Payload Comparison

From Tables IV and V, the DCT LSB-2 method yields the best optimum payload and allows more data to be hidden in the images. Hence, it is the best method to achieve maximum data payload from the two tested methods.

| TABLE IV. OPTIMUM DATA PAYLOAD—LSB TECHNIQUE | LSB Algorithm | Cover Image1 (259\( \times \)194 pixels) | Cover Image2 (300\( \times \)168 pixels) | Cover Image3 (195\( \times \)259 pixels) | Cover Image4 (360\( \times \)640 pixels) |
| --- | --- | --- | --- | --- |
| Maximum data payload (Bytes) | 93900 | 124200 | 109000 | 450000 |

<table>
<thead>
<tr>
<th>TABLE V. OPTIMUM DATA PAYLOAD—PROPOSED DCT LSB-2 TECHNIQUE</th>
<th>DCT LSB-2 Algorithm</th>
<th>Cover Image1 (259( \times )194 pixels)</th>
<th>Cover Image2 (360( \times )640 pixels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum data payload (Bytes)</td>
<td>125000</td>
<td>592000</td>
<td></td>
</tr>
</tbody>
</table>

F. PBC vs. Neural Network Prediction Confidence Analysis for LSB and Proposed DCT LSB-2 Techniques

The LSB technique decreases neural network efficiency for PBC values greater than 35%, while the proposed DCT LSB-2 method constantly maintains the neural network’s efficiency throughout all the PBC regions. As more than 35% of the image pixels are altered with noise, the LSB technique decreases the neural network efficiency. Hence, it can be stated from Fig. 10 and Fig. 11 that the proposed DCT LSB-2 method maximizes neural network efficiency. Although for PBC values less than 35%, the LSB method performs well compared to the proposed DCT LSB-2 technique.
VII. CONCLUSION

This paper presented an investigation and the implementation of an image steganography technique that maintains the efficiency of an existing image recognition ANN. This model can be applied in various fields of application and can be implemented to run on different platforms according to the required specifications.

Comparisons have been conducted between the LSB and the proposed DCT LSB-2 algorithms to determine the best algorithm to insert data in an image steganography system. From the results obtained in the experiments, the proposed DCT LSB-2 is the best encoding algorithm to hide data in a steganography system compared to the LSB algorithm.

Even though the proposed method showed improved performance under the neural network prediction test, the process can still have minor/negligent signs of pixel modification on the stego-images. Hence, the DCT coefficients and the quantization table indicated in Eqs. (4)–(6) should be calculated and mapped when designing the proposed DCT LSB-2 method to limit steganalysis.

Furthermore, the maximum data payload before an image is unrecognizable by the network is determined using both the LSB and the DCT LSB-2 algorithms. As can be observed from the results, the DCT LSB-2 method yields a higher data payload while minimizing visible changes in the cover image and does not cause the network to misclassify.

The LSB method results in signs of pixel modifications, and the LSB stego images cause the network to fail and misclassify at higher values of the PBC. The optimum embedding rate has been determined using the LSB and DCT LSB-2 algorithms.

In future work, the proposed DCT LSB-2 technique with the thresholds obtained in this study will be applied and implemented in an android mobile app for flexible operation in the application. The system will further be automated to dynamically detect and discard all the stego images that do not complement some given criteria. It will prohibit stego-images that do not meet the minimum thresholds for secure transmission to be sent through to the communication channel. Hence, the system will not be compromised for cross-detection and hacking. Also, the use of Television Wide Space (TVWS) will be considered as the transmission channel in the model [19, 20] and see how it responds. Lastly, a comparative study of all steganography techniques and image recognition ANNs techniques will be examined, and the concepts will be analyzed [21–30].

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHORS CONTRIBUTIONS

All authors carried out the conceptualization. The investigation methodology was done by Caswell Nkuna and Ebenezer Esenogho. Caswell Nkuna, and Ebenezer Esenogho, did the software simulation, while validation was done by Caswell Nkuna, Ebenezer Esenogho, Reelyn Heymann, and Edwin Matlotsee. Caswell Nkuna, and Ebenezer Esenogho, initiated the formal analysis. Caswell Nkuna and Ebenezer Esenogho prepared the original draft, and Reelyn Heymann and Edwin Matlotsee reviewed and edited it. Supervision was under Ebenezer Esenogho and Reelyn Heymann. Reelyn Heymann and Edwin Matlotsee carried out project administration—funding for the APC will be done by Ebenezer Esenogho and Edwin Matlotsee. All authors had approved the final version.

FUNDING

This work was supported by the University of Johannesburg’s Centre for Collaborative Digital Networks, South Africa and the Department of Electrical Engineering, University of Botswana, Gabonore.

REFERENCES


Copyright © 2023 by the authors. This is an open access article distributed under the Creative Commons Attribution License (CC BY-NC-ND 4.0), which permits use, distribution and reproduction in any medium, provided that the article is properly cited, the use is non-commercial and no modifications or adaptations are made.