Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation

Original Scientific Paper

Ammar Mohammedali Fadhil
Middle Technical University,
Institute of Technology , Department of Information and Communication Technology ,
Alzaafaraniya, Baghdad, Iraq
ammaral-khafaji@mtu.edu.iq

Hayder Nabeel Jalo
Middle Technical University,
Institute of Technology , Department of Information and Communication Technology ,
Alzaafaraniya, Baghdad, Iraq,
hayderjalo@mtu.edu.iq

Omar Farook Mohammad
Al-Hadba University College,
Computer Technology Engineering Department
Mosul, Iraq
ofmalobaidy@hcu.edu.iq

Abstract *– Since its inception, the steganography system (SS) has continuously evolved and is routinely used for concealing various sensitive data in an imperceptible manner. To attain high performance and a better hiding capacity of the traditional SS, it has become essential to integrate them with diverse modern algorithms, especially those related to artificial intelligence (AI) and deep learning (DL). Based on this fact, we proposed a DL-based SS (DLSS) to extract some significant features (like pixel locations, importance, and proximity to the imperceptibility) from the cover image using a neural network (NN) in a hierarchical form, thus selecting the candidate pixels for embedding afterwards. The pixel weight was expressed in terms of the position, imperceptibility, and its relationship with adjacent pixels to be a stego image. Performance evaluation revealed that the proposed DLSS achieved imperceptibility of 84 dB for images in training mode of a standard dataset.*

Keywords*: deep learning, steganography, neural network, embedding, imperceptibility*

1. INTRODUCTION

With the advent of the information communication technology (ICT), the transfer of various sensitive data in form of images, videos, and audio occurs primarily over the Internet. Meanwhile, many problems have been encountered related to the security and reliability of such accessible communication of information [1]. Thus, researchers in the field of information security became concerned about the legality of such information transfer and the freedom to have information, ensuring privacy-preserved data transfer [2]. In this rationale, the importance of diverse applications-based information transmission at the level of local and global networks appeared as one of the main focuses of the study. The main objective of this study is to protect the information (so-called privacy-preserved data communication) from penetration and plagiarism. In recent years, research on information penetration and data security revealed ever-increasing threats from hackers and adversaries, enforcing the rapid development of various protection techniques including the steganography system (SS) [3]. Previously, information security systems used data encryption algorithms to send data from one party to another, where such algorithms included encryption keys that contained all the information required to decrypt the information [4].

Digital data provide a comfortable environment for editing and modifying the data that can be copied

without losing data quality and content. The computer-processed digital data can be delivered from one device to another without any errors or external interference [5]. However, digital data distribution poses serious concern due to attacks or manipulation by unauthorized users, which leads to the loss of relevance, thus weakening its security aspect. Lately, the Internet access related insecurity of digital content has posed great challenges to all software developers, researchers, users, and distributors. A large part of the digital world is engrossed in the Internet, where several applications are implemented, considering the Internet service as a proven method of data communication between users. As the contemporary communication technologies empowered by the Internet and cloud computing have become an integral part of daily life, there is an urgent need to establish smart algorithms for highly secured and privacy-preserved information transfer over the Internet [6]. It has been realized that weak information security is mainly due to data transfer through insecure public channels. Thus, there must be some secure means to protect that information from unauthorized uses or illegal access by adversaries or hackers. To overcome this problem, dedicated research efforts have been made to achieve secure and confidential information communication, with information hiding technology constantly growing and becoming more complex. Information concealment technologies include digital media like images, video, and audio, providing an excellent carrier of hidden confidential information [7].

Using the data hiding technique, secret information and messages can be transmitted in a secure way through cover media, undetectable to viewers, hackers, and trackers. Over the decades, data hiding methods have been widely used to transfer confidential medical, military, agricultural, and other data. The SS has been most commonly used for concealing textual data securely that hide a specific text in one of the media, making them imperceptible [8] to others, except those who have the key to solving the algorithm. Until the secret data transmitted by the sender are received at the authorized recipient end, it remains hidden inside the medium [9]. Several daily life applications on the Internet use digital images, thus offering a suitable environment for data hiding. One can define the SS either perceptibly or imperceptibly through a high degree of security [10]. Any SS is very complex because it manipulates imperceptibly and efficiently the data of the transmission media. Consequently, the data hiding process suffers from various limitations related to the image size and the accuracy of transmitted information.

Despite the invisibility of hidden data, they are somehow visible to observers; however, useful information remains undisclosed without a key [11]. The major component of data concealment in the SS is called cryptography. It ensures that the information hidden in the digital medium cannot be perceived by the human eye, which is why the observer cannot detect the message included in the medium [12]. The main goal of any SS is to improve the security of data transmitted from the sender to the receiver. The purpose of using the SS is to hide confidential data from the public and make the transmitted image free of any information. Watermarking is the second part of the data hiding process [13], where by simple changes, the hidden data are often presented in the form of simple images. Cryptography [14] is a process of encrypting data (images or written text), whereby the data pose a challenge to the observer and cannot be decrypted. (Fig. 1) shows a classification scheme of information hiding.

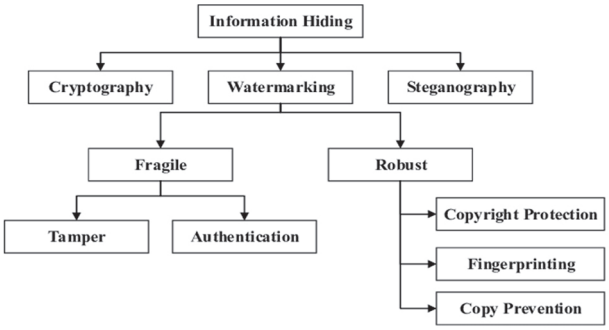


Fig. 1. Classification scheme of information hiding

Although each type of information hiding systems has its advantages and disadvantages, most researchers attempt to overcome the shortcomings of the SS. The main idea behind the improvement of the SS is to transmit information with high capacity, high security, and low imperceptibility. Table 1 gives a comparison of three types of information hiding schemes in terms of their main characteristics.

Table 1. Comparison of three types of information hiding schemes.

Attributes	Watermark	Cryptography	Steganography
Media	Image is popular, maybe text and video	Mostly text, sometimes image	Digital form of images, video, and audio
Imperceptibility	No	Yes	No
Visibility	Medium	High	Less
Key	Yes	No	Yes
Criteria	Capacity and imperceptibility	Security	Security, capacity, and imperceptibility
Results	Watermark	Cipher	Stego
Application	Authentication	Commerce	Many applications
Readability	Simi	Full	Full with extraction

Any information hiding system is composed of two components, a sender and a recipient [15]. The secret message (text) is embedded into the medium (a stego image) and then transmitted by the sender. Then, the message from the medium (a stego image) is extracted

by the recipient. The stego image embedded in the message is identical with the original image. The process of embedding and extracting requires specific algorithms that contain a key called a stego key. In short, by embedding, the sender generates a stego image and a key, while the recipient extracts the desired information (a secret message, and produces the original image) from the stego image by using the stego key (Fig. 2).

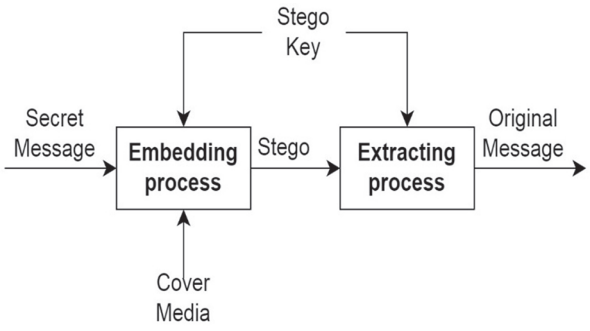


Fig. 2. Basic SS architecture

Most of the previous contributions related to the process of distributing secret data in the image. In this paper, we propose a method based on one of the artificial intelligence algorithms, i.e., deep learning. The cover image is initially divided into small images based on the color contrast of the image. After that the location of the secret bit is obtained by applying the neural network algorithm, and then we can use the weight factor to select the best pixel to embed the secret bit among more than one pixel.

One of the most important stages in steganography is the selection of the pixel to embed the secret bit, which must be done in such a way as to preserve imperceptibility. Therefore, the deep learning method was used to find the best pixel for embedding and thus to increase imperceptibility.

1.1. DEEP LEARNING (DL)

By using artificial intelligence (AI) it is possible to combine various modern technologies. The main goal of such unification is to mimic through artificial systems the cognitive abilities of humans and their intelligent behavior for further exploitation, especially in terms of solving complex problems such as detection, object recognition and self-driving [16]. Machine learning systems (MLS) consist of two main procedures, including feature extraction, and are designed for training [17]. Developers design a feature extraction protocol to extract different features from the data input into the system followed by their training to learn the system using the classifiers. This is performed to achieve a suitable function ensuring the absolute security of the private data transmitted by the sender and retrieved by the recipient. Despite the effectiveness of MLS in solving complex problems, they suffer from various limitations [18]. Many methods in the literature use deep learning techniques to solve different problems [19, 20]. In order to overcome these shortcomings, it is necessary to develop a suitable feature extractor. Creating a proper feature extractor is challenging because it requires experience and in-depth knowledge of the problem developers face. In addition, a particular feature cannot be generalized to another problem. In order to overcome this problem, DL has been recently widely used as part of ML. Fig. 3 illustrates a typical AI architecture.

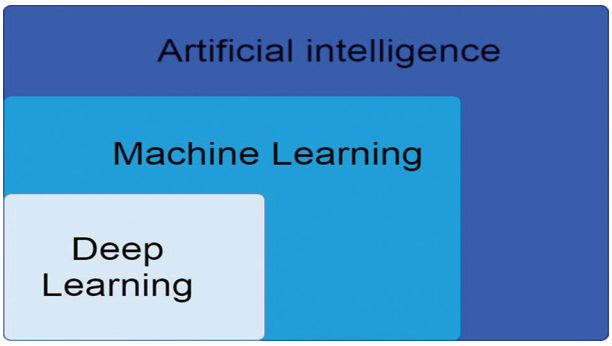


Fig. 3. General framework of AI

DL based on an improved artificial neural network (ANN) model is used in this paper. The ANN model is used to input the data into the neural system, and then the received output is fed back as an input, creating an experience for the system. Weight vectors such as $w=(w_1,w_2,..,w_m)$, with $w_i \in R$, can be manipulated at the neural system to produce the input vector such as $x=(xw_1, xw_2,.., xw_m)$, and applied as the following nonlinear function to obtain the output:

$$y = \sum_{i=1}^{n} w_i \times x_i + b, \quad (1)$$

where y is the output, which is the sum of weight (w_i) times the input vectors (x_i) plus bias (b).

2. RELATED WORK

Intensive studies have been conducted on the principle of hiding data as text in images or other media. Researchers have developed various modern technologies and linked them to data hiding or the SS [21], which used an inverted bit stream to increase imperceptibility, but the capacity was very low. Here, DL played a considerable role in data steganography advancement, especially for data in JPEG image format and other types of text [22] considering the number of attacks in terms of security to avoid secret data manipulation. Attempts were made to create a new paradigm of data steganography analysis using the concept of feature learning, a novel CNN-based method for feature extraction and classification, as well as techniques to improve imperceptibility [23]. One of the most important advantages of this method is the reliability of more than one type of image, but this method suffers from its inability to account for hacker attacks. The DL-based SS [24, 25] was implemented to improve the NN classifier, which achieves improved security and data

hiding capacity in the network. The information hiding method is good and effective, and it cannot embed a large amount of data, which most traditional methods suffer from. A new model [26] based on training the embedded images and an AI-assisted classifier could attain an embedding ratio of 70% in the training stage and of 30% in the examination stage, indicating an excellent outcome. The management of the training and the testing mode with the compatibility process between them were successful and the reason for increasing the security of embedding secret data with limited embedding data, which is the basis of the steganography system. A convolutional NN model was proposed [27] that consisted of three main stages, including calculation and data analysis, extraction of significant features, and classification of the extracted features in the digital image in order to embed hidden data into them, Although extracting important features from a cover image improves data security, it does not help to increase the imperceptibility of the stego image. A comprehensive review of the most recent existing reports in the literature related to data hiding (especially steganography) showed the use of diverse methods that mostly depend on the DL algorithms based on the celebrated ANN algorithms [28, 29]. DL algorithms [30] have been used to cover a digital image that include object border pixels within digital images, thus accurately classifying these pixels according to feature weights for further embedding. In all cases, embedding in a section or part of the cover image reduces the image capacity for secret data, which is important to sign for the method used to be feasible. Moreover, DL was directly applied [9] to the SS for the purpose of constructing an encoder and a decoder, enabling the learning of reversible steganography by distributing data according to the NN algorithm. However, it still needs to be improved in terms of security and robustness, which are the disadvantages of this method.

From the above, we can propose a method that takes advantage of existing methods and at the same time avoids the problems associated with the steganography system. The method depends on the method of selecting the hiding data position in the image (pixels) through deep learning (impact of a smart variable) to avoid the classical distribution and increase the imperceptibility. Furthermore, dividing the image into sub-images helps to avoid statistical attacks faced by the steganography system, thereby maintaining the security of the transmitted data.

3. PROPOSED STEGANOGRAPHY METHOD

An image steganography system processes a specific image enclosed by pixels, where each pixel has a decimal value consisting of one byte or 8 bits. Human eyes can easily recognize grey in four bits called the most significant bits (MSB) and cannot recognize the other four bits called the least significant bits (LSB). (Fig. 4) displays the process of hiding a secret message.

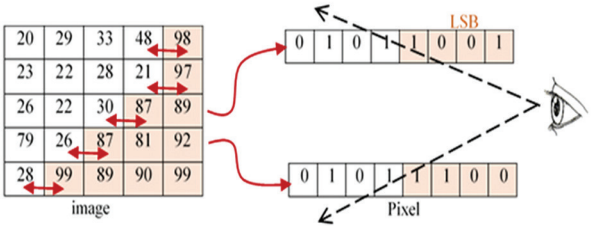


Fig. 4. Image recognition by human eyes

Hiding text in a given image involves two steps: in the first step, the text is converted into a series of binary bits from 0 and 1, while in the second step, these bits are embedded in the digital data of image pixels. Each pixel consists of 8 bits, which can contain one to two bits of a text message. Most of the existing methods take into account the embedding place, but with the same technique.

Feature selection is the most significant step in ML that works together with the NN algorithm. The candidate pixels act as NN inputs for embedding, where only those pixels that satisfy the condition $P_{con.}=P_1-P_2=16$ (decimal value) can be added to the LSB. Therefore, the number of pixels can be stored in the form of a vector (called the input layer) for input into the NN code (Fig. 5).

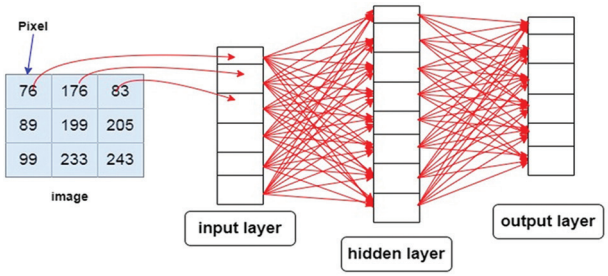


Fig. 5. The structure of the NN with the cover image

The image (Fig. 5) is comprised of pixels represented by their decimal values (act as an input layer of the NN). The NN has three major layers including the input, hidden, and output layers. Pixel values in the proposed NN are inserted into the input layer, producing a filter from the candidate pixels for embedding, where information is saved in the stego key. The output vector is delivered again to the image by maintaining the coordinate of the pixel (x, y) as the address. The cover image at the start is divided into several sub-images each having a definite size depending on the generated random function. The image is divided into sub-images so that the data are in multiple vectors. In this way several neural networks are achieved according to the number of vectors or images. Inputs x and corresponding weighs (w) are related by the following:

$$V = \sum = (x_1 \times w_1) + (x_2 \times w_2) \ldots + (x_n \times w_n) \quad (2)$$

$$z = \sum = x.w = w^T x \quad (3)$$

$$z = w^T x + b\,, \quad (4)$$

where $\hat{y}=g(z)$ is the output layer. V is considered as a vector of weight w and pixel data x.

Many sub-images imply various NNs, and each sub-image can be handled by a single NN. However, as shown in (Fig. 6), DL can deal with multiple NNs.

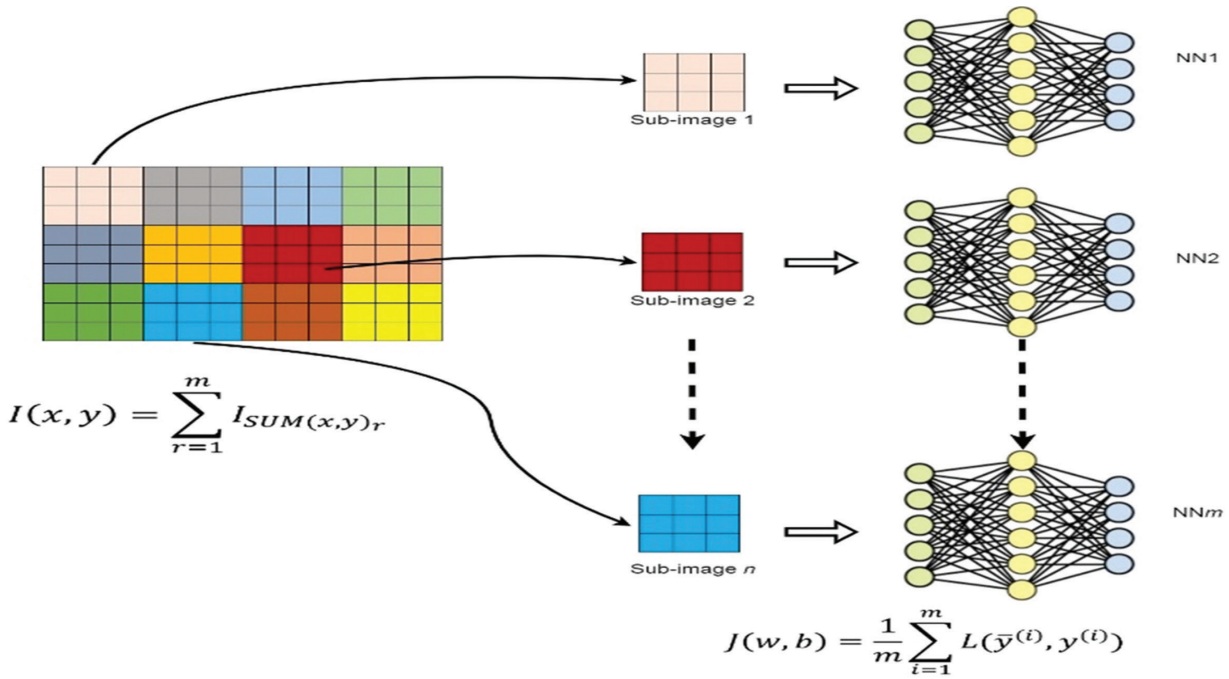


Fig. 6. DLNN system for the entire cover image

A convolutional layer with NNs considers the main issue, representing the main elements in the system, as well as the features, i.e., a set of features given by each NN is produced during the processing of the hidden layer. Convolution selects the pixel value of $I(x,y)$ with the assumed weight derived from the adjacent pixels called kernel $K \in R^{(2kf+1)\times(2ks+1)}$ such that kf and ks are sub-images of dimension (3x3). The stego pixel takes the form:

$$S(i,j) = S.k = \sum_{u=1}^{kf}\sum_{v=1}^{ks} I_{(i+u,j+v)}K_{(u,v)}, \quad (5)$$

where K is the kernel of the corresponding coordinate of cover pixel (u,v) aimed at producing stego pixel $S(i,j)$.

The number of hidden layers inside the system can be controlled, providing several feedback inputs until the appropriate stego pixels are due to the manipulation of cover pixels achieved under the corresponding weights. Fig. 7 displays a typical procedure for getting the secret text.

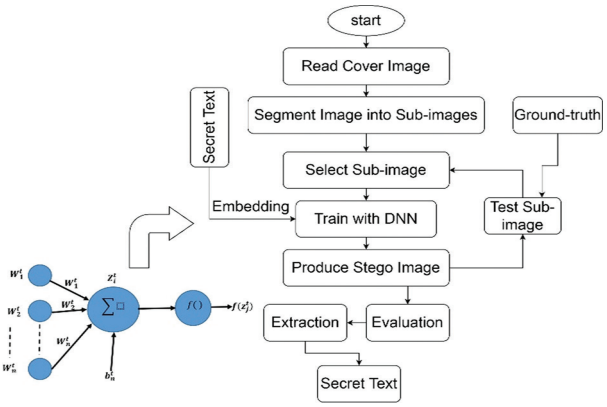


Fig. 7. General overview of the system

The proposed system first reads the cover or original image and then divides it into sub-images following a specific condition before being fed to each individual NN. First, the NN is selected under the features derived from sub-image pixels. Next, each NN contributes to a deep neural system with the submission of new features improved during the processing.

4. RESULTS AND DISCUSSION

Fig. 8 shows cover images used by the proposed DLSS together with the corresponding stego images. Numerous images of size (256 × 256) and (512 × 512) pixels from the standard dataset were used for performance evaluation.

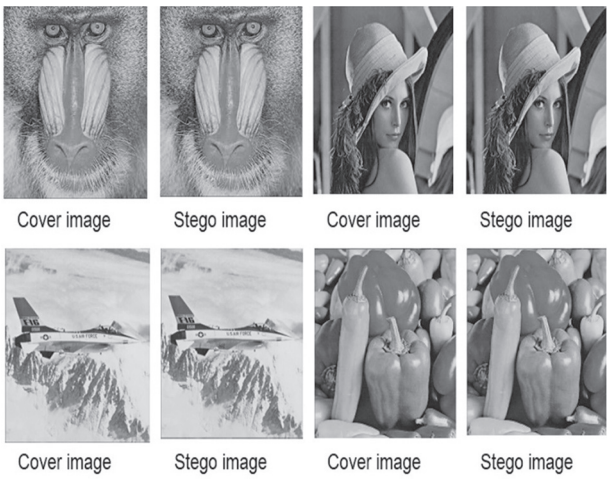


Fig. 8. Standard cover and stego images used in the proposed DLSS

Images like Lena, Baboon, Peppers, and Jet with different payload capacities were tested. The stego image is defined as the secret message inside the original image that remains indistinguishable from anything, meeting the purpose of steganography. The efficiency of the system was evaluated in terms of imperceptibility, payload capacity, secret bits embedded in the imperceptible part of the pixel (LSB) of the cover image, the peak signal-to-noise ratio (PSNR), and the mean square error (MSE).

As already mentioned (Fig. 7), human eyes cannot differentiate the cover from the stego image, which makes it difficult to observe the inner secret. For this reason, hackers or intruders use a statistical technique to figure out the secret message included in the stego image. Over the years, numerous image steganography techniques have been developed to obtain an optimal algorithm that can achieve the best results. However, specific benchmark criteria are needed to compare the performance of the proposed DLSS with the existing state-of-the-art methods. Although most existing SS can successfully hide private information, making it indistinguishable to human eyes, these techniques suffer from various statistical issues that need to be overcome. So, to properly validate the results obtained from the proposed DLSS, it is important to determine payload capacity of the secret message, indicating the robustness of the stego image (carrying data without distortion) against various attacks. In this study, PSNR and MSE parameters were used for validation.

4.1 PSNR

In terms of MSE of the proposed DLSS, PSNR values (in dB) were evaluated as follows:

$$PSNR = 10\log_{10}\left(\frac{max^2}{MSE}\right), \tag{6}$$

where max indicates the maximum pixel intensity value of 255, and PSNR is a measure of image resolution and distortion derived from the mean square error (MSE). For both greyscale and color images, PSNR as high as 70 dB and above is considered to be very good, in the range of 30 to 50 dB is acceptable, and below 30 dB is unacceptable. Table 2 summarizes the obtained imperceptibility and payload capacity results for different images in both greyscale and color images. Table 3 shows PSNR values for various standard images of different pixel sizes achieved by the proposed DLSS.

Table 2. Performance evaluation of the proposed DLSS.

Image	Image resolution	Payload capacity (bytes)	Embedding ratio	Pixel representation								PSNR (dB)
	256 × 256 (pixel)	32765	6.25%	1	0	1	1	0	1	0	½	76
Lena	256 × 256 (pixel)	53743	12.5%	1	0	1	1	0	1	0	1	61
	256 × 256 (pixel)	64752	18.75%	1	0	1	1	0	1	1	0	42
	512 × 512 (pixel)	32765	6.25%	1	0	1	1	0	1	0	½	84
Lena	512 × 512 (pixel)	53743	12.5%	1	0	1	1	0	1	0	1	70
	512 × 512 (pixel)	64752	18.75%	1	0	1	1	0	1	1	0	54

In the first NN iteration, when a 3K secret message was embedded, the secret bit appeared in the first bit of the LSB with every two pixels getting a one-pixel candidate. The neural system could present pixels with the ability to embed secret bits within the cover image. For an embedding ratio of 12.5%, all candidate pixels could replace the LSB (first bit) with the secret bit that appeared from the text message. In contrast, for an embedding ratio of 18.75%, the system made it possible to occupy two pixels from the LSB for embedding secret bits (Table 3).

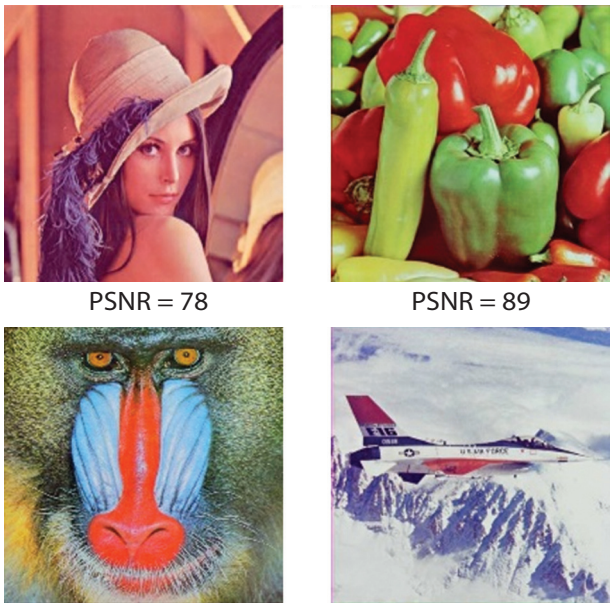
Table 3. Results of images used in the proposed method with their sizes.

Image	Image size (pixels)	PSNR (dB)
Baboon	256 × 256	79
Peppers	256 × 256	78
Jet	256 × 256	75
Baboon	512× 512	88
Peppers	512× 512	86
Jet	512× 512	83

One of the most important features of steganography results is imperceptibility, which is measured by PSNR. This factor depends on the strength of the distribution of secret data by image pixels, which results in the deep learning method in a smart distribution of data within the image.

PSNR values are found to depend on image information, e.g., a baboon image includes several pixel variations thus nominating the neural system to embed multiple pixels. One of the significant features used by a deep neural network (DNN) is the difference between certain pixels and adjacent pixels (4 or 8 neighbors). Thus, the Lena image achieved a lower PSNR value because of the uniform pixel values and the embedding ratio of 18% of the image. In contrast, the Baboon image had too many pixels variations, allowing a large number of pixels to be selected to store secret bits. In this study, the DNN was used to increase payload capacity while keeping the imperceptibility (image quality) of greyscale images (one channel represented by a one-pixel value) intact. The same strategy was used for

color images where the process included three channels according to red, green, and blue (RGB), indicating that each pixel consists of 24 bits (8 bits for each channel). In addition, as illustrated in (Fig. 9), PSNR values in color images were higher than in grey images. It was asserted that the training system containing different images over 205 is worth improving the variable hidden layer with the neural system, thereby improving image imperceptibility.



PSNR = 78 PSNR = 89

PSNR = 84 PSNR = 81

Fig. 9. PSNR of (256 × 256) color images with a 6.25% embedding ratio

4.2. MSE

The MSE values of the proposed DLSS were evaluated based on the difference between the original image (prior to embedding) and the stego image (carrying a secret message) by the expression:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (G1_{ij} - G2_{ij})^2, \quad (7)$$

where M and N are the row and the column of the image, and G1 and G2 are the cover and the stego image pixels, respectively, representing the ith row and the jth column. The obtained MSE value for the greyscale image was 100.0 (worst), and reduced to 0 (better). A 10-bit image with a corresponding pixel value of [0,1023] became undetectable, which indicates the excellent performance of the DLSS because the main purpose of any steganography system is to reduce the MSE value as much as possible. The achieved MSE value of 0 clearly indicates that there is no difference between the cover image and the stego image.

Table 4 compares the present results with results obtained in other studies described earlier in the literature. In order to demonstrate the superior nature of the proposed DLSS compared to the existing state-of-the-art SS, the achieved results were additionally compared with the most significant findings published in the literature. Different steganography techniques have shown different performances in terms of payload capacity and PSNR values, indicating that the best one is the current DLSS. The obtained improvement in payload capacity and PSNR values was attributed to the excellent embedding ratio by the DLNN. The PSNR value with an embedding ratio of 6.25% (green bar) was higher due to fewer secret messages or less information being embedded into the image, causing a smaller image degradation or distortion effect. In addition, the blue bar represented a higher embedding ratio to obtain a low PSNR. It is important to note that some studies did not evaluate all capacities, hence the missing bars. The high imperceptibility achieved by the proposed DLSS was mainly due to the use of a large number of iterations and new features such as pixel variations and differences between pixel values. In conventional methods, pixel values are limited such that the difference is fixed in advance (for example, difference = pix1(value) - pix2(value) = 40). In the proposed DLSS with a DNN, all variables were changed through system training by increasing and decreasing the number of hidden layers and nodes.

Table 4. Comparison of the present results with results obtained in other studies described earlier in the literature, using the USC-SIPI database with a 6.25% embedding ratio.

Authors	Year	Image used	Method	PSNR
[31] Diar D. et al.	2021	Lena	LSB+CRT+PVD	73.0
[32] U. Pilania & P. Gupta	2020	Lena &Baboon	IWT-SVD Scheme	54.1
[33] M. Oudah et al.	2020	Lena	DWT Transform	70.5
[34] Q. Li et al.	2020	Baboon	Chaos Encryption	61.2
[35] M. Kumar, & H. Nagar	2021	Lena	Hybrid LSB+ AES cryptography	75.2
[36] A. Hindi, et al.	2019	Baboon	Index XOR LSB	74.4
[37] S. Almutairi, et al.	2019	Baboon	2 bits LSB	79.3
Proposed		Lena +Baboon	DNN + region segmentation	84.3

5. CONCLUSION

In this paper, a robust DLSS is proposed for extracting different significant features from the cover image using DL combined with a NN in a hierarchical form. In this way, candidate pixels are selected for embedding. The use of DL in steganography has made the hiding process more secure, allowing more payload capacity

to be embedded for digital images. By this method, DL as an AI algorithm could extract features that are later processed according to weight and importance. Steganography consisted of the cover and stego images, where the cover image was used to extract significant features of the images. Here, pixel position provided the basis for work in addition to image weight and imperceptibility. The NN was used to determine the suitability of embedding sites, resulting in high imperceptibility (84.3 dB for a 512 ×512 image) of the stego image. The results revealed that it is possible to embed huge amounts of information instead of the previously approved random embedding. Performance evaluation showed that the proposed DLSS outperformed the existing steganography in terms of PSNR, MSE, and imperceptibility values, indicating high data security against attacks with capacities of a 12.5% and 18.75% embedding ratio. It is worth taking a valuable part of the image or dividing the image into several parts to further improve the DLSS. Furthermore, it may be interesting to adopt the NN algorithm by selecting a section and hierarchical division.

ACKNOWLEDGMENT

The authors are grateful to the Middle Technical University (MTU), and the Al-Hadba University College, Iraq, for technical assistance.

6. REFERENCES

[1] Y. Li, Y. Tu, J. Lu, Y. J. S. Wang, "A Security Transmission and Storage Solution about Sensing Image for Blockchain in the Internet of Things", Sensors, Vol. 20, No. 3, 2020, p. 916.

[2] K. Del Villar, E. Close, R. Hews, L. Willmott, B. White, "Voluntary assisted dying and the legality of using a telephone or internet service: The impact of Commonwealth 'Carriage Service' offences", Monash University, Vol. 47, 2021, p. 125.

[3] Y. Zhang, X. Le, Y. Jian, W. Lu, J. Zhang, T. Chen, "3D Fluorescent Hydrogel Origami for Multistage Data Security Protection", Advanced Functional, Vol. 29, No. 46, 2019, p. 1905514.

[4] A. A. Yazdeen, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, O. M. Ahmed, R. R. Zebari", FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review", Qubahan Academic, Vol. 1, No. 2, 2021, pp. 8-16.

[5] D. M. Abdullah et al. " Secure Data Transfer over Internet Using Image Steganography: Review", Asian Journal of Research in Computer Science, 2021, pp. 33-52.

[6] J. Molina-Ríos, N. Pedreira-Souto, "Comparison of development methodologies in web applications", Information and Software Technology, Vol. 119, 2020, p. 106238.

[7] R. Tabares-Soto et al., "Digital media steganalysis", Digital Media Steganography, Elsevier, 2020, pp. 259-293.

[8] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, K.-H. Jung, "Image steganography in spatial domain: A survey", Signal Processing: Image Communication, Vol. 65, 2018, pp. 46-66.

[9] C.-C. Chang, X. Wang, S. Chen, I. Echizen, V. Sanchez, C.-T. Li, "Deep Learning for Predictive Analytics in Reversible Steganography", arXiv:2106.06924, 2021.

[10] Y. Ke, J. Liu, M.-Q. Zhang, T.-T. Su, X.-Y. Yang, "Steganography Security: Principle and Practice", IEEE Access, Vol. 6, 2018, pp. 73009-73022.

[11] S. A. Parah, J. A. Sheikh, J. A. Akhoon, N. A. Loan, G. M. Bhat, "Information hiding in edges: A high capacity information hiding technique using hybrid edge detection", Multimedia Tools and Applications, Vol. 77, No. 1, 2018, pp. 185-207.

[12] Y. Li, S. Yao, K. Yang, Y.-A. Tan, Q. Zhang, "A High-Imperceptibility and Histogram-Shifting Data Hiding Scheme for JPEG Images", IEEE Access, Vol. 7, 2019, pp. 73573-73582.

[13] C. Qin, Z. He, H. Yao, F. Cao, L. Gao, "Visible watermark removal scheme based on reversible data hiding and image inpainting", Signal Processing: Image Communication, Vol. 60, 2018, pp. 160-172.

[14] S. Singh and Y. Sharma, "A Review on DNA based Cryptography for Data hiding", Proceedings of the International Conference on Intelligent Sustainable Systems, Palladam, India, 21-22 February 2019, pp. 282-285.

[15] A. Chatterjee, S. K. Pati, "Data Hiding with Digital Authentication in Spatial Domain Image Steganography", Computational Intelligence in Pattern Recognition, Springer, 2020, pp. 897-907.

[16] Y. Ma, Z. Wang, H. Yang, L. Yang, "Artificial intelligence applications in the development of autonomous vehicles: a survey", IEEE/CAA Journal of Automatica Sinica, Vol. 7, No. 2, 2020, pp. 315-329.

[17] B. T. Atiyha, S. Aljabbar, A. Ali, A. Jaber, "An improved cost estimation for unit commitment using back propagation algorithm", Malaysian Journal of Fundamental and Applied Sciences, Vol. 15, No. 2, 2019, pp. 243-248.

[18] M. I. Fazal, M. E. Patel, J. Tye, Y. Gupta, "The past, present and future role of artificial intelligence in imaging", European Journal of Radiology, Vol. 105, 2018, pp. 246-250.

[19] D. Božić-Štulić, M. Braović, D. Stipaničev, "Deep learning based approach for optic disc and optic cup semantic segmentation for glaucoma analysis in retinal fundus images", International Journal of Electrical and Computer Engineering Systems, Vol. 11, No. 2, 2020, pp. 111-120.

[20] D. Velasco-Montero, J. Fernández-Berni, R. Carmona-Galán, Á. Rodríguez-Vázquez, "Performance assessment of deep learning frameworks through metrics of CPU hardware exploitation on an embedded platform", International journal of electrical and computer engineering systems, Vol. 11, No. 1, 2020, pp. 1-11.

[21] A. M. Fadhil, "Bit inverting map method for improved steganography scheme", Universiti Teknologi Malaysia, 2016, PhD thesis.

[22] M. Chaumont, "Deep learning in steganography and steganalysis", Digital Media Steganography, Elsevier, 2020, pp. 321-349.

[23] G. Sulong, A. Mohammedali, "Recognition of human activities from still image using novel Classifier", Journal of Theoretical and Applied Information Technology, Vol. 71, No. 1, 2015.

[24] Y. Zou, G. Zhang, L. Liu, "Research on image steganography analysis based on deep learning", Journal of Visual Communication and Image Representation, Vol. 60, 2019, pp. 266-275.

[25] H. Ruiz, M. Chaumont, M. Yedroudj, A. O. Amara, F. Comby, G. Subsol, "Analysis of the Scalability of a Deep-Learning Network for Steganography "Into the Wild"", Proceedings of the International Conference on Pattern Recognition, 2021, pp. 439-452.

[26] A. Mohammedali, "Human Activities Recognition in Still Image", LAP LAMBERT, Tech Science Press, 2016.

[27] J. Yang, K. Liu, X. Kang, E. K. Wong, Y.-Q. Shi, "Spatial Image Steganography Based on Generative Adversarial Network", arXiv:1804.07939, 2018.

[28] J. Ye, J. Ni, Y. Yi, "Deep Learning Hierarchical Representations for Image Steganalysis", IEEE Transactions on Information Forensics and Security, Vol. 12, No. 11, 2017, pp. 2545-2557.

[29] C. Zhang, C. Lin, P. Benz, K. Chen, W. Zhang, I. S. Kweon, "A Brief Survey on Deep Learning Based Data Hiding, Steganography and Watermarking", arXiv:2103.01607, 2021.

[30] B. Ray, S. Mukhopadhyay, S. Hossain, S. K. Ghosal, R. Sarkar, "Image steganography using deep learning based edge detection", Multimedia Tools and Applications, Vol. 80, No. 24, 2021, pp. 33475-33503.

[31] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography", Multimedia Tools and Applications, Vol. 80, No. 6, 2021, pp. 8423-8444.

[32] U. Pilania, P. Gupta, "Analysis and implementation of IWT-SVD scheme for video steganography", Micro-Electronics and Telecommunication Engineering, Springer, 2020, pp. 153-162.

[33] M. K. Oudah, A. N. Abed, R. S Khudhair, S. M. Kaleefah, "Improvement of Image Steganography Using Discrete Wavelet Transform", Engineering and Technology Journal, Vol. 38, No. 1, 2020, pp. 83-87.

[34] Q. Li et al., "A Novel Grayscale Image Steganography Scheme Based on Chaos Encryption and Generative Adversarial Networks", IEEE Access, Vol. 8, 2020, pp. 168166-168176.

[35] M. Kumar, S. Kumar, H. Nagar, "Enhanced Text and Image Security Using Combination of DCT Steganography, XOR Embedding and Arnold Transform", Design Engineering, 2021, pp. 732-739.

[36] A. Y. Hindi, M. O. Dwairi, Z. A. AlQadi, Technology, "A Novel Technique for Data Steganography", Engineering, Technology & Applied Science Research, Vol. 9, No. 6, 2019, pp. 4942-4945.

[37] S. Almutairi, A. Gutub, M. Al-Ghamdi, "Image Steganography to Facilitate Online Students Account System", Review of Business and Technology Research, Vol. 16, No. 2, 2019, pp. 43-49.