Article │ Received 1 June 2023; Accepted 20 July 2023; Published 8 December 2023
https://doi.org/10.55092/pcs2023020011

An improved steganography system based on contrast variation with Fibonacci decomposition to increase imperceptibility

Amjed Fadhil Hamody Al-Bayati[1], Mesut ÇeviK[1], Ammar Mohammedali Fadhil[2,*]

[1] Altinbas University, Department of Electrical and computer engineering, Institute of Science, Istanbul, Turkey
[2] Middle Technical University, Institute of Technology, Baghdad, Iraq

* Correspondence author; E-mail: ammaral-khafaji@mtu.edu.iq.

Abstract: There are currently many obstacles in the way of the design and development of a reliable image steganography system. These include low capacity, weak robustness, and invisibility. Overcoming these restrictions requires enhancing the steganography system's capacity and security while keeping the signal-to-noise ratio (PSNR) high. Considering these considerations, the purpose of this research is to create a technique to successfully embed secret data into a cover image, thereby realizing a strong steganography scheme. The planning and execution of the suggested method occurred in multiple stages. To boost the scheme's text security and payload capacity, a novel encryption approach dubbed shuffle the segments of the secret message was integrated with an improved Huffman compression algorithm. To further strengthen the approach, the bit depth of each pixel was doubled from 8 to 12 using a Fibonacci-based picture transformation decomposition method. Third, the schemes were made stealthiest using an enhanced embedding technique that combined a random block or pixel selection with the implicit secret key generation. Experimental evaluations of the suggested scheme's performance are conducted to determine its stealth, security, robustness, and capacity. Against the proposed scheme, resistance is analyzed for its resistance to non-structural, type 2, and statistical steganography detection attacks. The acquired PSNR values indicated that the proposed technique was successful in achieving higher imperceptibility and security than the reported findings while preserving a larger capacity. In a nutshell, the problems were fixed since the proposed steganography system was superior to existing data hiding schemes on the market.

Keywords: Steganography system; machine learning; deep learning; least significant bit; Fibonacci decomposition

1. Introduction

The Internet has become more critical for data transfer and communication. Concerns over personal privacy have increased the need for robust data security measures. Much of the data that passes via the Internet, from medical diagnoses to financial records to classified military plans, is very sensitive and must be protected at all costs. The practice of secretly storing data has roots that stretch back over a thousand years. In practice, it often fails since all it does is rely on a technique called encryption to make the contents of messages less visible. Suppressing the discovery of a communication's existence is often essential in competitive situations to prevent the suspicion of rivals [1]. As the Internet has developed, digital material has become a fast and efficient means of disseminating information (*i.e.*, images, audio, textual documents, and videos). Developing forgeries tools and programs that enable criminals to steal, change, or delete data while in transit is a negative side effect of this progress. Information encryption and information concealment are the two primary tenets of the security system introduced to handle information security and avoid manipulation. Cryptography is a method of encoding information so that only the intended recipient, via an "agreed upon" mechanism, can read the encoded message. However, cryptography is not foolproof since an unauthorized intruder might inject and combine unwanted data, which can interfere with the scent information. Further, encrypting sensitive data isn't always a good idea because it might invite unwanted attention. For this reason, communication must sometimes be difficult. For this very reason, some kind of secret-keeping system is essential. Similarly, in steganography, "information hiding" refers to secretly transmitting information by embedding it inside seemingly innocuous visual or linguistic cues. Information can be concealed in various formats, including text, images, videos, audio, and protocols. Neither one is without flaws. However, photographs are often used in online media since they are readily accessible and straightforward to use [3]. Hiding information means keeping a message hidden without making its presence obvious [2]. Steganography and watermarking are two methods that can be used to accomplish this goal. In many ways, steganography and watermarking are the same, but with opposite ends. Watermarking is commonly used to guard intellectual property rights because it may preserve sensitive data while hiding or revealing the presence of communication. In contrast, steganography focuses on hiding the fact of communication and keeping hidden information safe from prying eyes, according to the authors [3,4]. Regarding secret messaging, steganography has recently been the adopted method. In a combat zone, the military may swap top-secret maps or surveillance footage [5]. Medical pictures, such as X-rays and MRI scans, are encrypted whenever they are sent between medical facilities or stored on a server [6]. The same is true of commercial and monetary institutions like banks, which can safeguard their clients' account information against theft or other forms of unlawful usage. To effectively conceal sensitive information, the communication technologies mentioned above necessitate digital steganography. Different sorts of picture steganography techniques are used to accomplish the steganographic goals, and they are discussed in various works of literature. Least Significant Bit (LSB), Pixel Value Differencing (PVD), Exploiting Modification Directions (EMD), Pixel Pair Matching (PPM), Prediction Error Edge Based, Histogram Based, and Hybrid Steganography Algorithms are all prevalent steganography techniques [4]. The primary emphasis of this research will be on hybrid steganographic techniques; using a pixel value decomposition technique based on the Fibonacci sequence will increase the security of picture steganography. The system's security will be increased by switching the LSB to an unusual form.

1.1. Research contribution

To improve the imperceptibility and reduce the ratio (MSE) and thus increase the PSNR, we will use the variance technique as a condition in the embedding process. This is applied by randomly choosing two neighboring pixels from the cover image, one of which has a high intensity value and the other a low intensity value, and the difference between the two pixels values is determined in advance. For example, if we set the value of the difference to 50, any two neighboring pixels with a difference of 50 between their intensities will contain the secret code. The secret code will be embedded in the pixel based on the value of the intensity of the two pixels; if the value of the secret code is (1), it will be included in the low-intensity pixel, but if the secret code value is (0), it will be included in the high-intensity pixel. To avoid standard embedding, such as the existing method that embeds directly in the LSB of the pixels, we aim to embed differently, which depends on decimal embedding, not digital like before, in addition to using Fibonacci decomposition to analyze the pixel value in 12 bits instead of 8 bits in binary decomposition.

1.2. Objective of study

The main goal of this research is to improve the security of hiding information in an image by using a new embedding method based on contrast variation and Fibonacci decomposition. Therefore, this proposal is carried out to fulfill the following objectives:

- To improve image steganography security by using an algorithm based on Fibonacci decomposition for pixels' values. Changing the LSB to an unfamiliar form will increase the system's security.
- To increase the imperceptibility of the system by a new embedding strategy to make a balance between payload capacity and image quality.

1.3. Research organization

This is the outline of the thesis: In Section II, this study examines the current work related to stenographic methods for images. In Section III, we provide a complete description of the proposed approach. In Section IV, we provide a thorough explanation of our model and run its simulations, recording the results. Finally, in Section V, we draw a line under our work and consider its potential future applications.

2. Literature review

This section provides a brief description of some of the most common image stenographic techniques.

2.1. Steganographic algorithms

Over time, advances in steganography and Steg system design have made it possible to conceal data transmission. However, capacity, complexity, and security must be considered when deciding on a technique. Therefore, there is no one steganographic technique that can meet all the needs. The procedures used in steganography often include substituting a pseudorandom secret message for a noise component of a digital picture and are typically categorized according to the domain into which the data was entered. In the spatial domain, the concealed message is embedded directly, and the most prevalent approach is the LSB. However, the LSB is notoriously vulnerable to visual and statistical assaults; thus, new statistical analysis techniques have had to be developed to compensate.

2.2. The least significant bit family

Because of its ease of use, the LSB approach is the most popular. The incapacity of the human eye to detect subtle variations at the pixel level is exploited by LSB. When an image is embedded, its least significant bit is swapped out for message bits in the spatial domain, making it vulnerable to noise and transportation faults. Pseudorandom or sequential replacement are both possible. Each cover image pixel is updated sequentially with the embedded bits in the succeeding replacement. In contrast, pseudorandom replacement uses a key as input to a random number generator, changing each pixel's specification number. Data concealed by the LSB technique is vulnerable to nearly every picture change, even if security measures are strictly adhered to [7]. Because the LSB method is applied to noise, the result will likely be affected by further compression, filtration, *etc.*

2.3. Machine learning in steganalysis

Optimal detectors are used by most classic steganography detection methods [8]. However, Machine learning, specifically SVMs and ANNs, has recently become the norm in statistical analysis. Put differently, using a statistical model of covered objects, determine which statistical test is best for some criterion. In both the spatial and transform domains, SVM is used as a classifier by the authors of this research [9]. The author of this study has created a steganalysis technique based on a spatial domain SVM classifier with a Gaussian kernel, with an emphasis on detecting anomalous pixels [10]. The authors recently employed linear, polynomial, and Gaussian SVM kernels to detect the stage picture with 73% accuracy and estimate the length of the concealed message with 33.6% accuracy [11]. Recent work uses the spatial domain Rich Model as a feature extractor and SVM as a classifier to improve S-detection UNIWARD's error rate to about 42% [12]. There has been a lot of work on steganography using ANNs. Authors examined a particular type of DL framework in picture steganalysis [13], whereas studies [14,15] and [16] developed CNN-based steganalysis for the

BOSS Base dataset and focused on the spatial domain. In CNN-based structural analysis, a well-designed neural network is used to construct a feature extractor and classifier that operates from beginning to end. In this study [17], the accuracy of J- UNIWARD (the UNIWARD algorithm applied in the transform domain) was 72.9% by utilizing convolutional DCTR kernels, while in [18], the testing error for steganalysis using Combined CNN was 45% and the detection error was 42.93%. In the field of visual steganography, neural networks are very effective. Multichannel neural networks allow S-UNIWARD steganalysis to achieve 81.55 multichannel accuracy, as recently demonstrated by [19].

Many steganographic techniques have been developed as steganography has grown in popularity. Also, there have been attempts to streamline the steganographic process using automation. This chapter offers a high-level overview of steganography. The steganographic review, on the other hand, demonstrates how challenging it is to find ways to improve upon existing approaches. Although various steganography approaches have been developed to uncover hidden data, much work must still be done to decipher messages. In addition, the classification stage in contemporary steganography accounts for the importance of machine learning.

3. Proposed approach

Any steganography system includes three main stages: the preprocessing stage, the embedding stage, and finally the evaluation stage. In the first stage, an image is selected to encode a hidden message. For this purpose, first we perform preprocessing on the input data. We must prepare the secret message and cover image in the pre-processing stage. The proposed method converts messages into binary bits and images into a Fibonacci decomposition. For embedding, we contribute the embedding position within image pixels in terms of contrast variation. Evaluation of the system used three critical criteria Peak Signal Noise Ratio (PSNR), measuring the quality of the image and the Human Visual System (HVS) to stand against any attack, and Capacity Detection (CD). The flow chart of the proposed embedding process algorithm is depicted in Figure 1. The main aim of this study is to improve the security of image steganography by using an algorithm based on Fibonacci decomposition for pixel values. Changing the LSB to an unfamiliar form will increase the system's security. The input image consists of small units called pixels, which are numerical values that reflect the color luminance in the image. The numerical peak of a pixel is from 0 to 255, and to be accepted as a numeric value, it takes 8 bits. In our proposed system, we get out of the standard method and use the Fibonacci decomposition to be the numerical value of the 12-bit pixel, as shown in Figure 2. First, we take an input image and perform some preprocessing steps. After that, the proposed approach involves preparing the secret message. Now, Fibonacci decomposition is used. After that, the evaluation is used, and the stego image is found.

3.1. Data pre-processing

The pre-processing step is an important part of the suggested steganography system because it makes it easy to figure out how secret the hidden message is. Thus, at this stage, the cover image and the secret message are both being prepared simultaneously. An effective embedding procedure, known as cover image preparation, is achieved by applying a pre-processing stage to the proposed scheme prior to the embedding process. The methods of picture splitting and image transformation decomposition are broken down in depth below.

3.2. Image splitting technique

Before doing anything with the provided image, this stage involved selecting and analyzing it. First, an image is chosen at random from the available set. Now, the suggested system deals directly with 8-bit grayscale image selecting and analyzing it. First, an image is chosen at random from the available set. Now, the suggested system deals directly with 8-bit grayscale images. If the image is 24 bits RGB, however, the suggested approach first performs a channel-by-channel analysis of the RGB image to evaluate whether it is suitable for further implementation. After the separation process is complete, the single 8-bit matrix's picture channels all grow to the size of the original image. Simply put, an 8-bit image is created in this stage for each of the three channels. To determine which of the three channels has the secret bit, the system must examine all three values for each pixel.

3.3. Steganography system

The steganography system consists of two sides: the sender that embeds hidden text and the receiver that extracts the secret message from the stego image. Extracting on the contrary of embedding in terms of algorithm. The flow chart of the proposed extraction process algorithm is depicted in Figure 3, and the general architecture of the steganographic system is shown in Figure 4. Assume that you have a message that you want to convey to someone using steganographic transmission. To conceal the embedded message, the sender must first input a cover message into the cryptosystem. The term "embedded message" refers to a secret message. Something buried in the cover is called an embedded message, and a steganographic method mixes the cover massage with this hidden message. Steganographic keys (stage keys) are optionally used secret information that may or may not be required for the algorithm to complete the concealed procedure. In most cases, you'll need the original key (or a similar one) to get to the hidden message again.

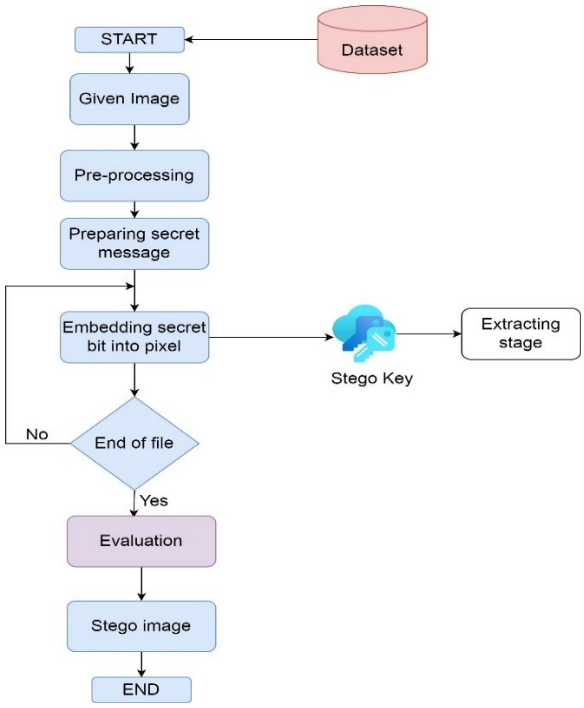

Figure 1. The flow chart of the proposed embedding process algorithm.

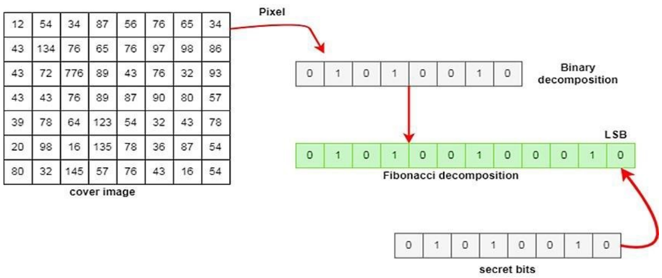

Figure 2. Flow of Fibonacci decomposition.

3.4. LSB decomposition

The Least Significant Bit approach is one of the simplest ways to store data inside a digital cover secretly [20]. The pixel values in an IJ picture are represented by decimal numbers in a range proportional to the number of bits utilized. Each pixel in an 8-bit grayscale picture takes on a value between zero and 255, and equation 1 may be used to represent any positive integer.

$$F_{10}= f_0+f_1B^1+f_2B^2+\ldots=\sum_{i=1}^{n} f_iB^i \quad (1)$$

Where B is the constant, this feature enables the picture to be broken down into binary images by segmenting them into n bit planes. Traditional LSB embedding strategies include substituting the least significant bits of the cover image with the secret message or modifying them using an ’inverse’ function. Sequential insertion, selected text embedding in "noisy" places, or random dispersal over the picture are other viable options for the embedding approach. In more modern approaches, LSB is used in the LSB plane and in additional planes or as a hybrid of the two. Based on the number of pixels picked based on brightness and contrast attributes, the quantity of embedded data might be constant or variable in size. The primary benefit of this method is that the amplitude of the fluctuation in pixel values is limited to within a range of l; thus, the alteration of the LSB plane does not degrade the image in the eyes of the viewer. Under typical viewing conditions, the human visual system has masking features that make large volumes of embedded information invisible to the naked eye. The term "masking" describes the situation in which one signal becomes undetectable to an observer due to the existence of another signal. Refer to [21,22] and [23] for a comprehensive analysis of these methods. Low-density block (LSB) data concealment also boasted a large embedding capacity and a low computing cost. The key drawbacks relate to the system's vulnerability to manipulation, geometric assaults, filtering, and compression.

3.5. Fibonacci decomposition

The proposed steganography strategy's central idea is to conceal a message inside the original image, maintain the hosted image's quality so that it looks identical to the original, and transfer the two images from the sender to the authorized receiver side without raising suspicion among uninitiated viewers. Using steps like pixel selection and implicit essential creation, this research proposes a new steganography technique for concealing secret messages behind cover images. The intensity of the two pixels is used to determine which pixel the secret code will be embedded in; if the secret code value is one, the pixel will have a low intensity, and if it is zero, the pixel will have a high intensity. The Fibonacci-based decomposition method was utilized to make embedding the private data more secure and efficient. In this study, the pixel count was converted from its original decimal form to its Fibonacci decomposition before further processing. The Fibonacci decomposition was used to conceal information within the cover art, suggesting that the numbers formed an integral design component. Due to the binary encoding, the bit plane of an image was an 8-bit plane. As a result, the Fibonacci decomposition was logically converted to the 12-bit planes through implementation. The detailed process is explained in a study of Leonardo of Pisa [24].

4. Experimental analysis and results

Various evaluation metrics establish that the applied processing via the proposed approach impacted image quality and led to some information loss. Both objective and subjective methods can be used to assess the stereo image. Finding the differences between two data sets required objective approaches to apply mathematical criteria and use many criteria, including ground truth and prior knowledge of the statistical issue at hand. Contrarily, subjective approaches relied solely on human observation and subjective judgment, with no referring criteria provided. The embedding capacity (EC), peak signal-to-noise ratio (PSNR), mean square error (MSE), and bit per pixel (BPP) were considered as objective approaches for evaluating the proposed scheme in this research. In the suggested technique, the EC value is proportional to the ratio of message bits to the number of cover pixels. One pixel could contain an arbitrary number of message bits, and the EC is written as:

$$EC = \frac{Number\ of\ textbit}{Number\ of\ image\ pixel} \quad (2)$$

The simulation runs on the following set of parameters:

- When 1 bit of two pixels was incorporated, the total size of the image was 16,384 bytes, or 6.25 percent. The image had a resolution of (512 by 512) pixels.
- When 1 bit of 1 pixel is embedded, the total number of bytes required to store the image is 32,768 (12.5 percent), if each pixel in the image has a value of 8 bits (1/8 = 12.5%).
- Since each two pixels were allocated to 16 bits, 3/16 = 18.75% while 1.5 bit with one pixel was inserted, the number of bytes required to store a 512 by 512-pixel image was 49,152, or 18.75%.

To maintain parity with previously published works in this area, the current study utilized a range of payload capacities and presented them as percentages. Figure 5 displays examples of stego pictures employed in the suggested method. As mentioned earlier, the image produced after embedding is called a "Stego" image. To evaluate the quality of a stereo image, we use a peak signal-to-noise ratio (PSNR) scale and a mean square error (MSE) scale. The PSNR block calculates the peak signal-to-noise ratio, in decibels, between two images. This ratio is used as a quality measure between the original image and the compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image. After the embedding procedure, the image quality is assessed by calculating the PSNR and comparing the original and stego versions of the image. When the PSNR is less than 30 decibels, data embedding is deemed unnoticeable to the HVS. This expression is used to derive the PSNR value:

$$\text{PSNR}=10\ \log_{10}\left(\frac{\text{MAX}_\text{I}^2}{\text{MSE}}\right) \quad (1)$$

While, the MSE scale indicates the difference of pixel by pixel between the Stego image and the cover image, which is calculated as in the following equation:

$$\text{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}[I(i,j)\text{-}K\ (i,j)]^2 \quad (1)$$

Where, m is no. of row in original image and n is no. of column in original image. The PSNR is calculated from the MSE that had a negative impact. PSNR parameters allowed the equation to be standardized across all approaches and image formats. The testing and training phases are important to the success of the suggested method. To test whether a stereo image is undetectable in traditional image processing, one would use the PSNR scale. The PSNR metrics are used to compare the stego image to its original carrier image and determine how authentic the stego image is. We may compare the stereo picture's distortion to that of the carrier image in terms of decibels (dB). Since a lower PSNR score indicates a lower likelihood of detecting an attack using the HVS, a higher PSNR value indicates a higher-quality image. During the training phase, the PSNR decreased as the MSE grew, suggesting that the mismatch between the actual picture and the stego message had grown more severe. Due to the inverse relationship between MSE and PSNR, the results are unsatisfactory when MSE is high. The issue is resolved in the testing phase, and the resulting results are superior to those obtained by other methods. In this work, we used three distinct embedding techniques to assess the efficacy of the developed method with varying EP: a straightforward LSB embedding, an embedding using the Fibonacci decomposition method, and an embedding with the grayscale standard SIPI images (Lena, Baboon, and Tiffany (512512)). The experimental results show the final variation in images, as shown in Figure 6. Different stego pictures with varying amounts of EP are used to evaluate the effectiveness and quality of the proposed method. Compare the STEGO images in Figure 5.3 to the original image in different payload capacities to see the similarities. As seen in the second row of the figure, the original image looked like a stego image with a reasonable degree of embedding. However, as the final row of the graphic shows, the image is destroyed when the embedding limit is exceeded, making it recognizable by a hacker.

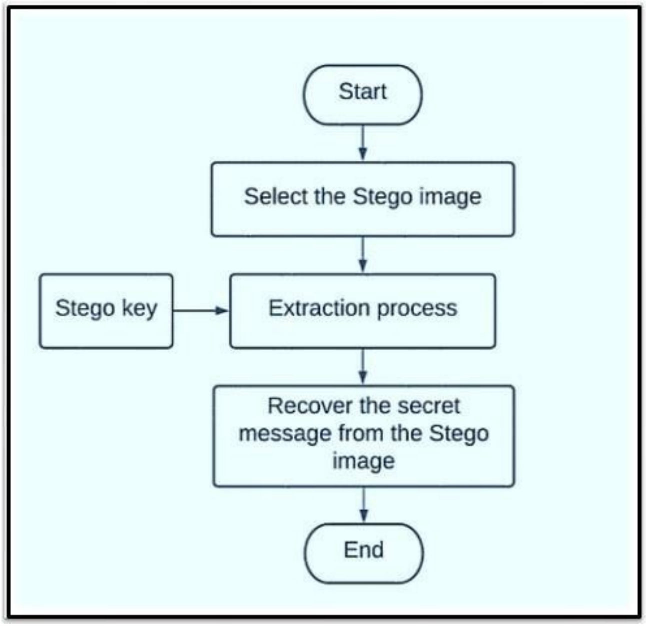

Figure 3. The flow chart of the proposed extraction process algorithm.

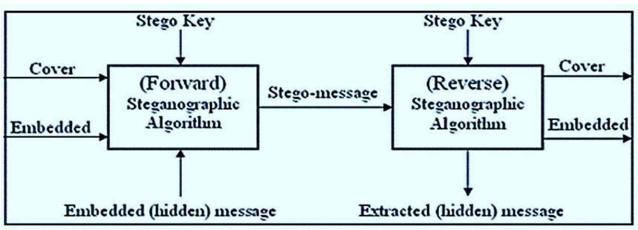

Figure 4. A general steganography system.

Figure 5. Various stego images using proposed approach.

Figure 6. Variations of original and stego images.

5. Conclusion

In this study, we offer a strong image-based steganographic method for sending private information over the web in a safe way. Today's security applications require more than just a steganographic technique that doesn't compromise on aesthetics or payload. Using the proposed steganography method, this research looked at the results of the experiments, analyzed them, talked about them, and made comparisons. There are three main ways to judge the outcome and see if it fixed the most important issues with the steganography scheme. Using a new decomposition method that the hacker doesn't know about helps to improve capacity and robustness. Using encryption and random selection during the embedding process, the new method improves the system's security, which is based on the distinction grade value and integrity system. For each criterion, the results are shown in tabular and graphical formats to make them easy to read and understand. Many promising future avenues were uncovered by this effort. For instance, combining the frequency domain and the special domain can improve security. The resulting security and robustness may be improved. The results suggest that combining the suggested approach with the DWT and embedding may produce high coefficients. This is not a new consideration because numerous methods have previously used large embedding coefficients. Yet, DGV adoption has the potential to improve outcomes, including security and stealth.

Conflicts of interest

The authors declare no conflict of interest.

References

[1] Wu M, Liu B. Multimedia data hiding. *Springer Science & Business Media* 2003.
[2] Fadhil AM. Bit inverting map method for improved steganography scheme. *PhD Thesis, Universiti Teknologi Malaysia* 2016.
[3] Singh S, Singh R, Siddiqui TJ. Singular value decomposition based image steganography using integer wavelet transform. In *Advances in Signal Processing and Intelligent Recognition Systems: Proceedings of Second International Symposium on Signal Processing and Intelligent Recognition Systems (SIRS-2015)* 2015, 593-601.
[4] Subhedar MS, Mankar VH. Current status and key issues in image steganography: A survey. *Comput Sci Rev* 2014, 13:95-113.
[5] Jenifer KS, Yogaraj G, Rajalakshmi K. LSB approach for video steganography to embed images. *Int J Comput Sci Inf Technol* 2014, 5(1): 319-322.
[6] Liu J, Tang G, Sun Y. A secure steganography for privacy protection in healthcare system. *J Med Syst* 2013, 37:1-10.
[7] Rocha A, Goldenstein S. Steganography and steganalysis in digital multimedia: Hype or hallelujah? *Rev Inform Teór Apl* 2008, 15(1):83-110.
[8] Ker AD, Bas P, Böhme R, Cogranne R, Craver S, *et al.* Moving steganography and steganalysis from the laboratory into the real world. In *Proceedings of the first ACM workshop on Information hiding and multimedia security* 2013, 45-58.
[9] Fadhil AM, Jalo HN, Mohammad OF. Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation. *Int J Electr Comput Eng Syst* 2023, 14(1):73-81.
[10] Cogranne R, Sedighi V, Fridrich J, Pevný T. Is ensemble classifier needed for steganalysis in high-dimensional feature spaces? In *2015 IEEE International Workshop on Information Forensics and Security (WIFS)* 2015, 1-6.
[11] Menori MH, Munir R. Blind steganalysis for digital images using support vector machine method. In *2016 International Symposium on Electronics and Smart Devices (ISESD)* 2016, 132-136.
[12] Boroumand M, Fridrich J. Applications of explicit non-linear feature maps in steganalysis. *IEEE Trans Inf Forensics Secur* 2017, 13(4):823-833.
[13] Qian Y, Dong J, Wang W, Tan T. Deep learning for steganalysis via convolutional neural networks. In *Media Watermarking, Security, and Forensics* 2015, 9409:171-180.
[14] Pibre L, Jérôme P, Ienco D, Chaumont M. Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover source-mismatch. *arXiv*, 2015, arXiv:1511.04855.
[15] Xu G, Wu HZ, Shi YQ. Ensemble of CNNs for steganalysis: An empirical study. In *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security* 2016, 103-107.
[16] Xu G, Wu HZ, Shi YQ. Structural design of convolutional neural networks for steganalysis. *IEEE Signal Process Lett* 2016, 23(5):708-12.
[17] Zeng J, Tan S, Li B, Huang J. Large-scale JPEG image steganalysis using hybrid deep-learning framework. *IEEE Trans Inf Forensics Secur* 2017, 13(5):1200-1214.
[18] Hu D, Shen Q, Zhou S, Liu X, Fan Y, *et al.* Adaptive steganalysis based on selection region and combined convolutional neural networks. *Secur Commun Netw* 2017.

[19] Liu K, Li X, Zhang Q, Kang X. Multi-channel neural network for steganalysis. In *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* 2017, 1210-1213.
[20] Rustad S, Syukur A, Andono PN. Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *J King Saud Univ Comput Inf Sci* 2022, 34(6):3559-3568.
[21] Lin ET, Delp EJ. A review of data hiding in digital images. In *PICS* 1999, 299:274-278.
[22] Yeung MM, Mintzer F. An invisible watermarking technique for image verification. In *Proceedings of international conference on image processing* 1997, 2:680-683.
[23] Maity SP, Kundu MK. Robust and blind spatial watermarking in digital image. In *ICVGIP* 2002.
[24] McClenon RB. Leonardo of Pisa and his Liber Quadratorum. *Am Math Mon* 1919, 26(1):1-8.