International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 2, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n2.33
Journal homepage: https://wepub.org/index.php/IJCSIT/index

A Digital Image Steganographic Detection Method for LSB Steganography

Jiaqi Zhang [1], Dongpo Zhang [1] and Shang Zhang [2]

[1] School of Information Network Security, Xinjiang University of Political Science and Law, Tumushuke 843900, China

[2] Office of Higher Education Research, Xinjiang University of Political Science and Law, Tumushuke 843900, China

ABSTRACT

With the advancement of communication technology, communication information can no longer be transmitted merely through text but can be covertly conveyed via various types of communication carriers like images, audio, and video. This brings forth new challenges to traditional detection techniques that mainly target text information. Digital image steganalysis aims to detect and uncover communication information by recognizing steganographic behaviors contained within digital image files. This paper takes digital image steganographic activities based on least significant bit (LSB) as the main research object and conducts analysis and identification of digital images with steganographic information through visual attack method. It has been verified through experiments that steganographic activities based on LSB are hardly detectable through direct visual observation, but can be identified visually after undergoing visual attack processing.

KEYWORDS

Steganography; Steganalysis; Visual Attack

1. INTRODUCTION

In recent years, with the advancement of technology, information hiding techniques have matured increasingly and have emerged as a popular research topic in the domain of information security. Steganography refers to embedding secret information within a carrier by exploiting its redundant information or specific encoding methods, without inducing notable alterations in the carrier's appearance, statistical characteristics, and so forth [1]. For instance, in digital images, information can be concealed by modifying the least significant bits of pixels; in text, information can be hidden through the utilization of word spacing, punctuation marks, etc. In the military and intelligence fields, steganography is primarily employed for secret communication to prevent information from being intercepted and deciphered by the adversary. In the commercial realm, it is mainly utilized for intellectual property protection and the prevention of piracy and illegal replication. In personal privacy protection, sensitive information can be hidden in ordinary files to prevent being spied upon by others.

Steganographic detection refers to the process of finding and identifying whether there is secret information hidden in the carrier by various technical means. Steganography detection can prevent illegal information transmission through steganography technology and protect sensitive information of countries, enterprises and individuals [2]. It is helpful to crack down on illegal and criminal activities using steganography, such as espionage and intellectual property infringement. In some key communication fields, such as military communication and financial transactions, steganographic

detection can ensure the authenticity and reliability of communication. Steganographic detection plays an important role in ensuring information security, maintaining legal order and ensuring the reliability of communication.

With the continuous development of steganography technology, new steganography methods appear constantly, making steganography detection more difficult. On the other hand, the carriers of information steganography are diverse, and different types of carriers (such as images, audio, text, etc.) have different characteristics, so different detection methods need to be adopted for different carriers. In addition, steganographic detection methods may misinterpret normal vectors as containing steganographic information or fail to detect vectors containing steganographic information. In conclusion, steganography detection is a challenging task that requires constant research and development of new detection techniques to cope with ever-changing steganography threats [3, 4]. In this paper, we take the digital image steganographic vector based on least significant bit (LSB) as the main analysis object, and analyze the vector containing steganographic information by visual attack method, so as to identify whether the vector contains steganographic information.

2. RELATED WORK

With the advancement and development of steganography technology, steganography detection has been widely concerned. In recent years, many scholars and research institutions have carried out in-depth exploration and research in this field, and achieved fruitful results.

Chhikara et al. [5] attacked the original image data set to generate the cover image data set, and then applied steganography method to the original image data set and measured its detection accuracy. Steganographic analysis is performed with support vector machines and integrated classifiers using higher-order Markov features and newly introduced joint entropy-based features. The experimental results show that the embedding detection rate is reduced by 20% ~ 40% after the overlay image is preprocessed. Tan et al. [6] proposed a steganographic detection algorithm based on nonzero uniformity index, which is generally applicable to steganography based on homogeneous representation, and proposed three least square-based steganographic pixel ratio estimation algorithms, which are respectively applicable to three typical HRBS algorithms.

In order to solve some of the most challenging problems in multimedia forensics, especially in image forensics, Liu et al. [7] used ensemble learning-based methods based on big feature mining in intermediate image forgery detection, including seam engraving forgery and drawing forgery in JPEG images, and subsequent anti-forensics operations. Deep learning is also introduced, and well-known deep learning models are applied to image forgery detection and image steganography, which greatly improves the detection accuracy. Chaganti et al. [8] addressed the challenge of stegomalware, highlighting the need for improved detection methods for malware payloads hidden in images using steganography. Overall, the literature on steganography detection encompasses a wide range of techniques and approaches, from network protocols to image analysis, emphasizing the importance of robust detection methods in combating hidden communication channels and potential cybersecurity threats.

In this paper, the digital image steganography based on LSB is analyzed, and the image carrier containing steganography information is analyzed by visual attack method. This method can easily distinguish whether the carrier image contains steganographic information visually.

3. RELATED TECHNOLOGY

3.1. Steganography Principle

Usually, the multimedia file with a certain redundancy space is selected as the carrier. For example, in digital images, there may be small changes in the color values of pixels that are not easily detected by the human eye, which provides space for hiding information. Replace some data bits in the carrier file with bits of secret information. For example, in an image, the least significant bit of a pixel value can be replaced with a bit of secret information. Because the human eye is not sensitive to small changes in brightness in the image, this substitution is often difficult to detect. After receiving the carrier file with hidden information, the receiver needs to use a specific extraction algorithm to recover the secret information. The extraction algorithm usually corresponds to the embedding algorithm and extracts the secret information from the carrier file according to the rule and position of embedding [9]. If the carrier file is not tampered with or destroyed during transmission, the receiver can accurately recover the secret information.

In short, the basic principle of steganography is to use the redundant space of carrier files to embed secret information through a specific algorithm, while not affecting the appearance and quality of carrier files as much as possible, so as to achieve covert transmission of secret information.

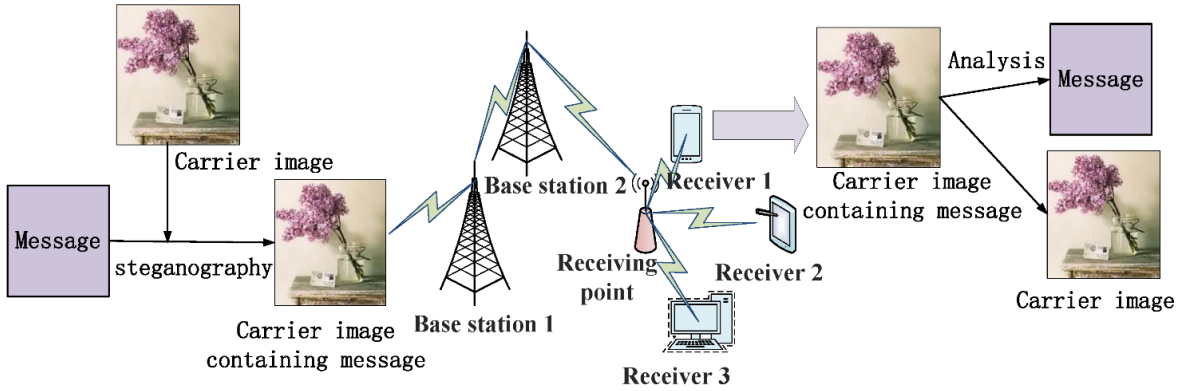

Figure 1. Architecture diagram of covert communication based on digital image steganography.

As shown in the Fig. 1, the information to be transmitted is first steganized in a digital image carrier through steganography technology, and the digital image carrier containing steganographic information is transmitted through the base station, wireless access point, etc. After receiving the digital image containing steganographic information, the receiving end first conducts steganographic detection on the image, analyzes it after determining that it contains steganographic information, and finally obtains the transmitted information.

3.2. Similarities and Differences Between Steganography and Encryption

Steganography and encryption are both techniques used to protect information in the field of information security, but there are obvious differences between them in many aspects. The main purpose of steganography is to hide secret information in a seemingly normal carrier, making it difficult for third parties to detect the existence of secret information. The focus is on the act of hiding the information itself, rather than the complex mathematical transformation of the information to prevent it from being cracked. Encryption is designed to convert information into an unreadable form through a specific algorithm, and only someone with the right key can decrypt it back to the original message [10]. The point of encryption is to make a high-intensity mathematical transformation of a message so that even if it is intercepted, an attacker without the key cannot understand its contents.

From the perspective of security, steganography mainly depends on the concealment of the hiding algorithm and the naturalness of the carrier. If the hiding algorithm is discovered, or if the carrier

arouses suspicion during transmission, then the secret information may be discovered. However, even if it is discovered, it is difficult to determine the specific content of the hidden information when there is no correct extraction method. Encryption mainly depends on the strength of the encryption algorithm and the security of the key. If the encryption algorithm is broken or the key is leaked, then the information will be completely exposed. Advanced encryption algorithms are usually proved by strict mathematics and a lot of practical tests, with high security, but once the key problems, the information will face great risks.

Steganography is often used in situations that require covert communication, such as intelligence transmission, military communications, etc. In some special cases, steganography can avoid attracting the attention of the enemy and realize the safe transmission of secret information. In addition, steganography can also be used for digital copyright protection to prove ownership of a work by hiding copyright information in a digital work [11]. Encryption is widely used in various scenarios that need to protect information security, such as network communication, e-commerce, database storage, and so on. In these scenarios, the confidentiality and integrity of information is critical, and encryption can effectively prevent information from being stolen, tampered with, or forged.

3.3. Image Steganography Based on LSB

In computer science, binary is a number system that uses two numbers, 0 and 1, to represent all numeric values. A bit is the smallest unit of a binary number. Each bit can be 0 or 1. LSB refers to the least influential bit of a binary number. In binary numbers, from right to left, each digit has twice the value of the previous digit. That is, the rightmost digit is 2 to the power of 0, the next digit on the left is 2 to the power of 1, then 2 to the power of 2, and so on. LSB refers to the rightmost binary number.

LSB, which stands for Least Significant Bit (least significant bit), is a steganography method to modify stored information based on the least significant bit of an image. When we change the value of the LSB, the change in the value is minimal. For example, if we change the LSB in the binary number 1011 from 1 to 0, the value will change from 9 to 8, changing by 1. If we change the leftmost bit (MSB), the value will change from 11 to 3, a change of 8, which is a relatively large change. LSB is a kind of spatial algorithm, which is to embed information into the lowest pixel bit in the image point to ensure that the embedded information is invisible.

Table 1. LSB steganographic information comparison table

Original Image Bytes	Message	Embedded Image Bytes
11001011	0	11001010
01110101	1	01110101
11001000	1	11001001
01011010	0	01011010

As shown in Table 1, when we use LSB to embed information "0110" into the carrier image, the information to be embedded will re-create the last bit of the image information. As shown in the table, the original image information "11001011" is rewritten as "11001010" after embedding information "0". Since the information is modified in the last bit, the resulting image changes are very small and almost indistinguishable to the naked eye.

3.4. Steganographic Detection Based on Visual Attacks

Steganography and steganographic detection are mutually reinforcing. Steganographic analysis refers to the technique of detecting, destroying, and even extracting secret information from carriers that may contain steganographic information. The main purpose of steganographic analysis is to distinguish whether the carrier contains steganographic information or not, and even to detect the

possible lines containing steganographic information in the carrier [12]. Although the carrier image using LSB for information steganography has a good visual concealment, statistical analysis tools can be used to determine whether the carrier image contains steganographic information.

In this paper, the visual attack method is used to determine whether the image contains steganographic information. The visual attack method denies that the least significant bit of a digital image is randomly arranged. The basic idea of this method is to remove all the original image content containing hidden information, so that the human visual system can distinguish the hidden information from the original information of the image. The core of the method is to embed the filter, which not only preserves the hidden information but also removes the original image information. For example, a 256-color palette image is replaced by a binary color palette, black replaces the sorted odd-bit color palette, and white replaces the sorted even-bit color palette, and the newly constituted image is observed through the human visual system.

4. EXPERIMENTAL ANALYSIS

4.1. LSB Steganography

In this paper, we randomly select an image from the BOSSbase_1.01 dataset as the digital carrier image, the image size is 257KB. First, we use LSB steganography to convert the string "This is a message!" Loop concatenation as hidden information. We steganographed 73,728 bits of binary data, and visually it was difficult to see the changes in the image before and after steganography.

As shown in Fig 2, Fig. 2 (a) is the original image of the digital image, and Fig. 2 (b) is the carrier image containing steganographic information. Visually, it is difficult to find the difference between the images. However, we can analyze the frequency distribution of the image, as shown in Fig. 3, which is the frequency analysis diagram of the original image and the image after steganography. From the frequency distribution of the image, we can find that the image containing steganographic information is different from the original image.

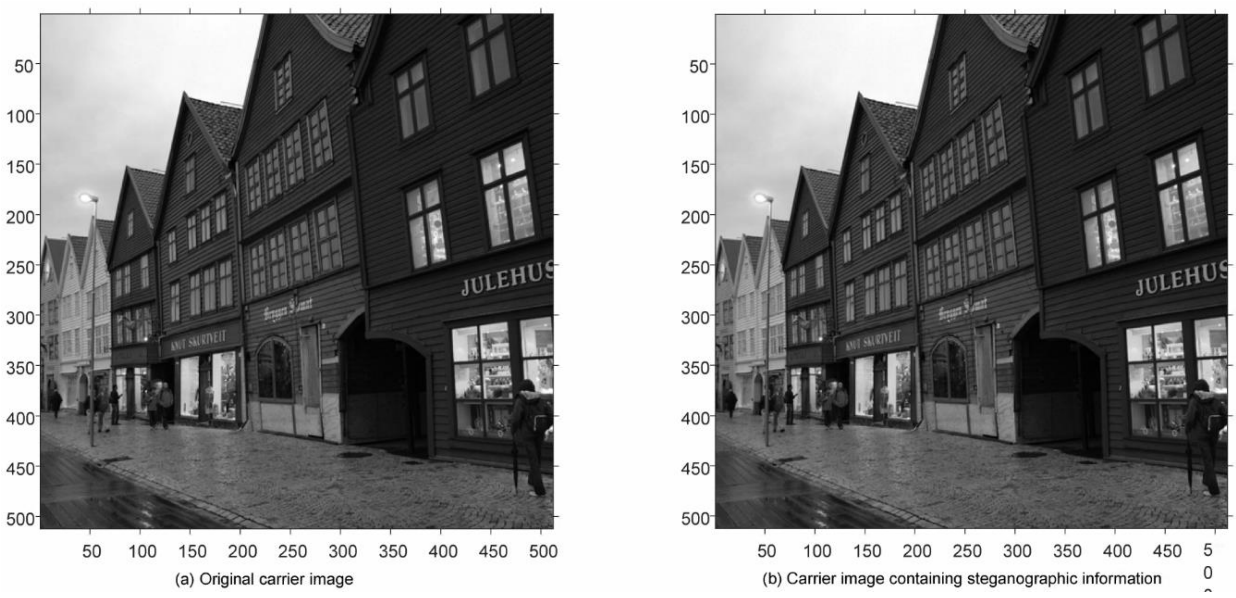

Figure 2. Comparison of carrier image changes before and after steganography.

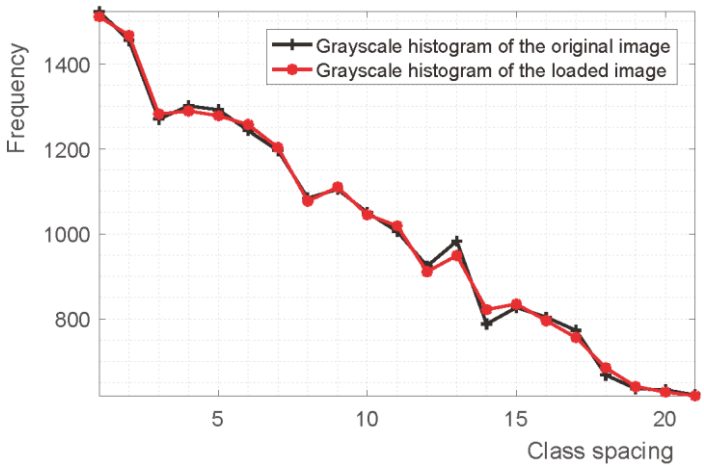

Figure 3. Comparison of carrier image frequency distribution before and after steganography.

4.2. Visual Attack Steganography Detection

It is difficult to detect whether the carrier image contains steganographic information directly from the visual point of view. In this paper, we adopt the visual attack method to carry out steganographic information detection on the image carrier containing steganographic information. We embed 31580bit (embedding rate is 12%) information in the carrier image. As shown in Fig. 4, Fig. 4 (a) is the effect diagram of the original carrier image after visual attack, Fig. 4 (b) is the effect diagram of the carrier image containing steganographic information after visual attack, and Fig. 4 (c) is the difference between the two images, if there is no change, it will show black.

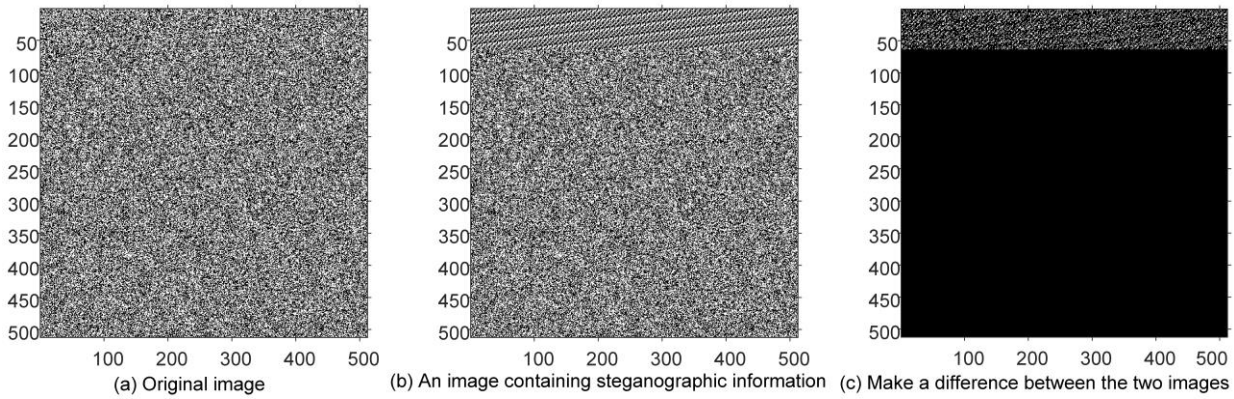

Figure 4. Comparison of visual attacks in carrier images (embedding rate: 12%).

As shown in Fig. 5, we embed 134,215 bits (51% embedding rate) of information in the carrier image. Fig. 5 (a) is the effect of the original carrier image after visual attack, Fig. 5 (b) is the effect of the carrier image containing steganographic information after visual attack, Fig. 5 (c) is the difference between the two images. Obviously, images containing steganographic information can be easily identified by the naked eye after a visual attack.

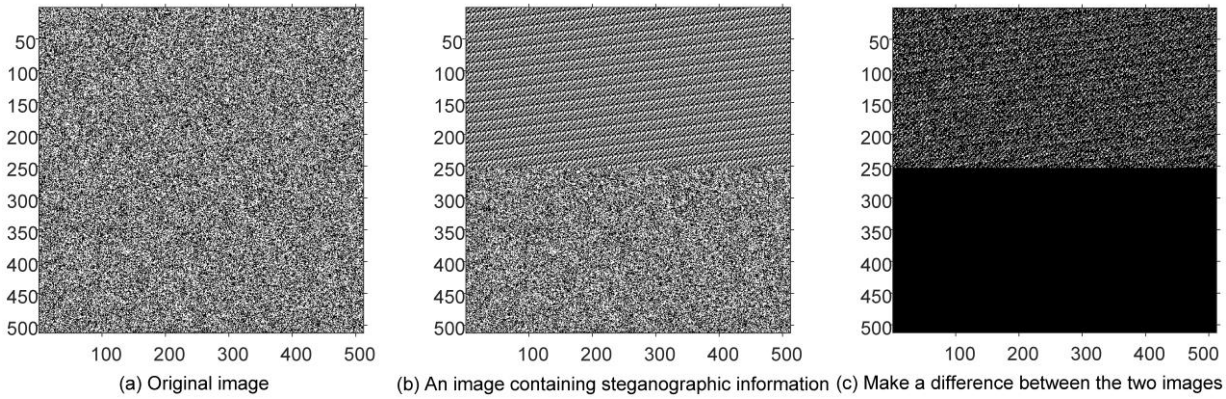

Figure 5. Comparison of visual attacks in carrier images (embedding rate: 51%).

5. SUMMARY

In this paper, the digital image steganography based on LSB is analyzed, and the image carrier containing steganography information is analyzed by visual attack method. This method can easily distinguish whether the carrier image contains steganographic information visually. This method is simple to implement and has little computational power, so it can be widely used in steganography. With the development of science and technology and the improvement of steganography technology, the difficulty of steganography detection will gradually increase. In the future work, we will gradually study the general model of steganography and analyze the carrier containing steganography information.

ACKNOWLEDGEMENTS

This work was supported in part by the President's Fund of Xinjiang University of Political Science and Law under Grants no. XZZK2022005.

REFERENCES

[1] Noura Khalil, Amany M. Sarhan, Mahmoud A. M. Alshewimy. A secure image steganography based on LSB technique and 2D chaotic maps [J]. Comput. Electr. Eng. 2024, 119: 109566.

[2] Laijin Meng, Xinghao Jiang, Tanfeng Sun. A review of coverless steganography [J]. Neurocomputing. 2024, 566: 126945.

[3] Sara Charoghchi, Samaneh Mashhadi. A secure secret image sharing with steganography and authentication by Hamming code (15,11) for compressed images [J]. Multim. Tools Appl. 2024, 83(11): 31933-31955.

[4] Lingamallu Naga Srinivasu, Vijayaraghavan Veeramani. Steganography using wavelet transform for secured data transmission [J]. Ambient Intell. Humaniz. Comput. 2023, 14(7): 9509-9527.

[5] Sonam Chhikara, Rajeev Kumar. Information theoretic steganalysis of processed image LSB steganography [J]. Multim. Tools Appl. 2023, 82(9): 13595-13615.

[6] Lei Tan, Chunfang Yang, Fenlin Liu, et al. Steganalysis of homogeneous-representation based steganography for high dynamic range images [J]. Multim. Tools Appl. 2020, 79(27-28): 20079-20105.

[7] Qingzhong Liu, Naciye Celebi. Large Feature Mining and Deep Learning in Multimedia Forensics [C]. IWSPA@CODASPY 2021: 3-4.

[8] Rajasekhar Chaganti, Vinayakumar Ravi, Mamoun Alazab, et al. Stegomalware: A Systematic Survey of MalwareHiding and Detection in Images, Machine LearningModels and Research Challenges [J]. CoRR. 2021, abs/2110.02504.

[9] Sabah Abdulazeez Jebur, Abbas Khalifa Nawar, Lubna Emad Kadhim, et al. Hiding Information in Digital Images Using LSB Steganography Technique [J]. Int. J. Interact. Mob. Technol. 2023, 17(7): 167-178.

[10] A. A. Karawia. Medical image steganographic algorithm via modified LSB method and chaotic map [J]. IET Image Process. 2021, 15(11): 2580-2590.

[11] Ziyun Yang, Zichi Wang, Xinpeng Zhang. A general steganographic framework for neural network models [J]. Inf. Sci. 2023, 643: 119250.

[12] Guofeng Li, Bingwen Feng, Mingjin He, et al. High-capacity coverless image steganographic scheme based on image synthesis [J]. Signal Process. Image Commun. 2023, 111: 116894.