Transactions on Machine Intelligence 3(4) (2020) 251-259

ISSN Online: 2821-1693

Transactions on Machine Intelligence

Journal Homepage: https://tmachineintelligence.ir/index.php/TMI

A Method to Hide Information in Image Based on Selected Pixels

S. Khosravi[1,*]

[1] Department of Computer, Payame Noor University, Tehran, Iran

ARTICLE INFO

Article History:
Received 24 July 2020
Received in revised form 10 November 2020
Accepted 27 December 2020
Available online 29 December 2020

Keywords:
Steganography, Pixel Value, Color Intensity, Image Quality, Image Size

ABSTRACT

There are various methods for concealing information or transmitting it covertly, with steganography being a prominent approach for secret communication. Unlike watermarking and fingerprinting, steganography aims to hide information in a way that its presence remains undetectable. Steganography is commonly applied to electronic media, particularly audio and image files. This paper provides an overview of image steganography, its applications, and different techniques. The objective is to outline the key features of an effective steganography algorithm. The ultimate goal is to develop a cross-platform solution capable of concealing a message within a digital image file. An image comprises numerous pixels, each with three color values, and is composed of millions of such numbers. Modifying a few color values in specific pixels typically results in an image that closely resembles the original. This paper introduces a technique that involves altering selected pixel color values based on the intensity criteria of colors in the image. The method strives to minimize image quality degradation, maintain information security, and, whenever possible, avoid changes in the image size.

1. INTRODUCTION

Since the advent of the Internet, ensuring the security of information has become a critical aspect of information technology and communication. Cryptography emerged as a method to safeguard the confidentiality of communication, leading to the development of various encryption and decryption techniques to keep messages secret. However, in certain situations, it is not sufficient merely to conceal the contents of a message; it becomes imperative to also conceal the very existence of the message. This implementation technique is known as steganography.

The term "steganography" is derived from the Greek words "stegos," meaning "cover," and "grafia," meaning "writing" [1], defining it as "covered writing."

Information is communicated in diverse forms and serves various applications. In many instances, maintaining secrecy in communication is desired. Such confidential communication spans from evident cases like bank transfers, corporate communications, and credit card purchases to a significant portion of everyday emails [2].

* Corresponding Author: khosravi_un@yahoo.com
Department of Computer, Payame Noor University, PO BOX 19395-3697, Tehran, Iran

http://dx.doi.org/10.47176/TMI.2020.251

There has been a rapid surge in interest in the field of steganography over the past decade, primarily driven by two main factors [3]:

Publishing and Broadcasting Industries: There is a growing interest in techniques to conceal encrypted copyright marks, serial numbers, and other identifiers in digital films, audio recordings, books, and multimedia products. This interest is fueled by the recognition of new market opportunities arising from digital distribution, coupled with concerns about the ease of copying digital works.

Government Restrictions on Encryption Services: Various governmental efforts to restrict access to encryption services have spurred investigations into methods for embedding private messages within seemingly innocuous cover messages. The ease with which this can be accomplished serves as an argument against imposing restrictions.

Steganography's capacity, security, and robustness are the three key aspects influencing its effectiveness [4]:

Capacity: Refers to the amount of data bits that can be hidden in the cover medium.

Security: Relates to the difficulty an eavesdropper may encounter in deciphering the hidden information.

Robustness: Concerns the resistance to modification or destruction of the concealed data in steganography.

This paper will specifically focus on concealing information in images. Numerous techniques exist for implementing steganography across various electronic media. The chosen technique relies on digital images, leveraging their often-substantial amount of redundant data, which steganography utilizes for message concealment. By altering the image content, such as changing pixel colors, a significant volume of data can be hidden within the image. While the changes may not be readily perceptible to the human eye, simple statistical analysis by a computer can distinguish between the original and modified images.

2. HISTORICAL INSTANCES OF STEGANOGRAPHY

Steganography has a rich historical background, with examples dating back to ancient times. In 440 BC, Herodotus documented instances of steganography in his histories. One involved Demeratus, who warned Greece of an impending attack by inscribing a message on a wooden panel covered in wax. Another account mentioned Histiaeus, who tattooed a message on his slave's shaved head, concealing it until the slave's hair regrew [5].

During World War II, invisible inks became prevalent for hiding information in seemingly ordinary memos. Substances like milk, vinegar, fruit juices, and urine, which darken when heated, were commonly used. The sources' ready availability made these inks effective during wartime [6].

In the Second World War, the Germans developed the Microdot technique, reducing information, especially photographs, to an extremely small size, making it challenging to detect [7].

While steganography is an ancient practice, its modern formulation often references the prisoner’s problem proposed by Simmons [8]. In this scenario, two inmates wish to communicate secretly to plan an escape, with their communication passing through a warden. The warden, who may be passive or active, examines all communication to detect covert information. A passive warden reports suspected covert communication without blocking it, while an active warden deliberately alters communication to remove hidden information [9][10].

3. DIFFERENT KINDS OF STEGANOGRAPHY

In the realm of hiding secret information within images, various steganographic techniques exist, each with its own complexity and strengths and weaknesses. Figure 1 illustrates the four main categories of file formats commonly utilized for steganography.

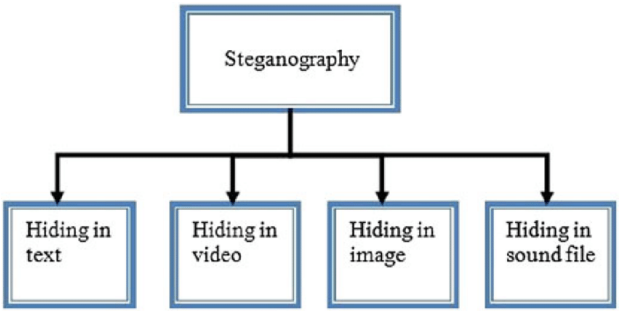

Fig. 1. Category of steganography.

Historically, hiding information in text has been a significant method of steganography. One approach involved concealing a secret message by selecting every nth letter of every word in a text message. However, with the advent of the Internet and various digital file formats, the importance of text-based steganography has diminished [10].

Given the widespread use of digital images, particularly on the Internet, and the inherent redundancy in the digital representation of images, they have become the most popular cover objects for steganography. This paper will primarily focus on concealing information in images. While similar techniques are applied to hide information in audio files, audio steganography introduces unique methods like masking, leveraging the human ear's ability to ignore faint sounds in the presence of louder ones [10]. Although audio files possess steganographic potential comparable to images, their larger size makes them less popular [1].

Protocol steganography pertains to embedding information within messages and network control protocols used in network transmission. Within the layers of the OSI network model, covert channels exist where steganography can be applied. For instance, information can be concealed in the header of a TCP/IP packet in fields that are optional or rarely used. Ahsan and Kundur's paper provides further insights into this technique [13].

4. DIFFERENCE STEGANOGRAPHY WHIT OTHER TECHNOLOGIES

Steganography and cryptography serve distinct purposes: cryptography focuses on keeping the contents of a message secret, while steganography aims to conceal the mere existence of a message. Although both technologies contribute to information protection, neither is infallible and can be compromised. The effectiveness of steganography is compromised if the presence of hidden information is revealed or suspected. To enhance the strength of steganography, it is often combined with cryptography.

Two other technologies closely related to steganography are watermarking and fingerprinting. These technologies primarily focus on the protection of intellectual property, resulting in different algorithmic requirements compared to steganography [10, 14]. In watermarking, all instances of an object are marked in the same way, typically with a signature indicating origin or ownership for copyright protection. Conversely, fingerprinting involves embedding different, unique marks in distinct copies of the carrier object supplied to various customers. This enables the intellectual property owner to identify customers violating their licensing agreement by supplying the property to third parties [15].

In watermarking and fingerprinting, the fact that information is hidden inside the files may be publicly known, and sometimes even visible, while in steganography, the imperceptibility of the information is crucial.

5. CURRENT WORK

An image is a composition of pixels, each representing a color and specified by a numerical value. Consequently, an image can be viewed as an array of numbers representing different light intensities across its various regions, forming a grid with individual points referred to as pixels.

Pixels are often represented with multi-bit sets, and the bit depth, indicating the number of bits used for each pixel, is crucial. In current color schemes, the smallest bit depth is typically 8. Monochrome and grayscale images,

for instance, utilize 8 bits for each pixel, allowing them to display 256 different colors or shades of gray. Digital color images are commonly stored in 24-bit files, utilizing the RGB color model (true color).

In a 24-bit image, each pixel's color variations are derived from three primary colors: red, green, and blue. The 24-bit binary number representing a pixel consists of 8 bits for red, 8 bits for blue, and 8 bits for green. This arrangement allows for 256 different values for each color, resulting in more than 16 million possible color combinations. Naturally, the greater the number of colors that can be displayed, the larger the file size. In image steganography, the technique often involves altering a few pixels color values.

5.1. Convert Text to Byte

The process involves converting data into bytes, where each character in the message is represented by its ASCII equivalent. If the message is password-protected, the recipient must enter the correct password to view the message. As an example, let's consider the character "a." In this case, "a" is represented as 01100001 in a byte array. This is because the ASCII value for "a" is 97, and its binary equivalent is 01100001.

5.2. Hide the Text in the Image

At 8 bits of the color number, if we change 2 least significant bit, our sighted system can detect changes in pixel. In this case, leas significant bits have 4 states, which is shown in Table.1.

Table 1. Four states of LSB

11	10	01	00

If we aim to store information in 2 bits, in the worst-case scenario, only 2 bits will be changed. For instance, if the red color number is represented as 10111011 pixels, and we intend to store information in the 2 least significant bits, in the worst situation, the red color number might change to 10111000. Examinations show that the Human Visual System (HVS) cannot distinguish this alteration. Therefore, we choose to save our information in the least significant bits of the color representation.

5.3. Message Embedding in Digital Image

Hiding information in an image involves embedding the message into the digital image. Each pixel typically has three numbers associated with it— one each for red, green, and blue intensities— and these values often range from 0 to 255. To hide the message, the data is first converted into byte format and stored in a byte array. The message is then encrypted, and each bit is embedded into the least significant bit (LSB) position of each pixel.

The method utilizes the first pixel to hide the length of the message (the number of characters). In this approach, only specific bits that determine the "one place" and the "two place" are altered, ensuring that the original pixel color value is changed by a minimal amount (3 degrees). The process involves using four bytes in two pixels to store an 8-bit character.

Here's an illustration of the color distribution in two pixels for storing an 8-bit character:

- First color in the first pixel: r7 r6 r5 r4 r3 r2 r1 r0
- Second color in the first pixel: g7 g6 g5 g4 g3 g2 g1 g0
- Third color in the first pixel: b7 b6 b5 b4 b3 b2 b1 b0
- First color in the second pixel: r7 r6 r5 r4 r3 r2 r1 r0

Assuming the character has bits (c7 c6 c5 c4 c3 c2 c1 c0), two of these bits are placed in the lowest red pixel, two in the lowest green pixel, two in the lowest blue pixel, and the remaining two in the lowest red pixel of the second set.

As an example, considering a pixel with values (255, 64, 64) and character "a," the process would result in a new pixel value of (253, 64, 64). This demonstrates that the new pixel is almost identical to the old pixel (255, 64, 64), ensuring minimal color difference and making the change less noticeable in the image.

For storing the text "save the text in the image" in the image, 26 characters are stored in 104 colors. In a 24-bit BMP format image, with 3 bytes per pixel, the information is processed, and details are stored in 33 pixels. Fig. 2 illustrates an image before storing the text into it.

Fig. 2. Before storing the text.

It appears that you intended to reference an image (Fig. 3) after storing the text into it. However, I'm unable to view or analyze images. If you have specific details or questions regarding the content or process related to the stored text in the image, feel free to describe them, and I'll do my best to assist you.

Fig. 3. After storing the text.

5.4. Algorithm to Find the Pixel

The proposed technique in this paper introduces a novel algorithm. This algorithm assesses pixel intensity and subsequently conceals data within randomly selected pixels, aiming to maximize the concealment of data in each pixel without introducing additional artificial noise. To execute this operation and identify pixels with higher intensity, we calculate the average color number elements within the image. This number serves as a threshold for discerning elements with higher intensity; elements exceeding the average number exhibit greater color intensity. Consequently, pixels with higher intensity in the image are chosen, creating a scattered distribution among the selected pixels. The selected elements represent pixels with higher intensity and greater scatter. Figure 4 illustrates the carrier picture essential for implementing this algorithm.

Fig. 4. The career pictures.

In Fig. 5, pixels whit higher intensity are greater average number are marked with black color.

Fig. 5. Pixels whit higher intensity.

The total number of pixels in Figure 5 is 215,232, with 58,468 pixels marked. To identify pixels with higher intensity, a factor, denoted as 'k,' is added to the average number. The choice of 'k' influences the number of selected pixels; higher values of 'k' result in fewer selected pixels. For instance, in Figure 5, when k = 50, the number of marked pixels is reduced to 23,405.

To enhance efficiency and identify pixels with a specific complexity in the image, we partition the image into blocks of size n*n. Pixels with higher intensity are compared with their neighboring areas, and operations are conducted to ascertain the pixel with the highest intensity within each block.

To execute this operation and identify pixels with higher intensity, n^2 color data elements from the n*n block are arranged in a matrix. The average color of this block is then computed, and this value serves as a threshold for discerning elements with higher intensity within the block. Elements exceeding the average possess greater color intensity in that block. The results for different values of 'n' in Figure 5 are presented in Table 2 for reference.

Table 2. Specified results whit different n

n	Total Blocks	Total Pixel Selected
8	3363	45286
50	90	57573
100	25	66477

So, we use this algorithm for embedding the massage text.

1) First, we chose the image and massage text, that we should use them on the picture
2) We covert massage text to binary code.
3) Image divided into n blocks
4) We determine pixel with Higher intensity in each block
5) We estimate the least significant bits in pixel marked.
6) Embed the text into the LSB

5.5. Message Extraction

In this section, we will delve into the process of retrieving a message from an image, irrespective of its file format. Once the message is extracted, it needs to be converted back to its original form. This conversion involves reading the embedded data from the file, resulting in data represented in byte format. This is achieved by extracting the pixels of the output image and organizing them into a single array.

The decoding process mirrors the reverse of the encoding process. Specifically, the initial pixel value indicates the number of characters in the message. Subsequent pixels represent the ASCII values of the message characters, which are then stored in a byte array.

- To visually present the stored information in the image, the algorithm follows these steps:
- First, we select the image containing the embedded text.
- We retrieve the least significant bit (LSB).
- The eight bits are combined and converted into a single character.

5.6. Decreasing Rate of Change

In the context of three-dimensional representation using separate colors, each pixel in a 24-bit BMP image is composed of three colors. Consider a color pixel represented as 10101000, 11010101, 01010110 in binary. In this representation, the first 8 bits signify R (Red), the second 8 bits represent G (Green), and the third 8 bits represent B (Blue).

Images, being the most prevalent cover objects for steganography, involve the conversion of a message into a digital image. To conceal the message, it is initially converted into byte format and stored in a byte array. The message is then encrypted, and each bit is embedded into the least significant bit (LSB) position of each pixel. The proposed approach involves modifying the LSB of each pixel byte (RGB) rather than solely the green byte. This modification minimizes the distortion rate, preserving the original appearance of the image. The information is stored in the first byte of green, with the option to use other colors later. This disperses more pixels, enhancing the security of the image.

To further enhance security, the technique involves reducing the number of LSB bits used. By using fewer LSB bits in a BMP image, the change and noise introduced are minimized, albeit at the cost of reducing the amount of stored data in the image.

6. CONCLUSION

The outcome of this paper is the development of a cross-platform tool capable of effectively concealing a message within a digital image file. Image steganography serves various applications, including facilitating secret and covert communication between two parties. Moreover, it finds utility in the secure transportation of high-level or top-secret documents among international governments. Additionally, image steganography contributes to copyright protection for digital files by utilizing the message as a digital watermark.

While image steganography has legitimate uses, such as those mentioned, it is crucial to recognize its potential misuse. Hackers may exploit it to send viruses and Trojans, compromising computer systems. In conclusion, with increasing emphasis on copyright protection, privacy, and surveillance, steganography is anticipated to gain significance as a protective mechanism.

This paper explores the integration of the image as the cover to enhance message security, resulting in the creation of a cross-platform, self-evaluating tool. The approach is highlighted for its benefits, including increased message security and a reduced distortion rate. The investigation suggests that considering the image as the cover contributes to the overall effectiveness of steganographic techniques.

Transparency Statement

The data supporting this study are available upon reasonable request to the corresponding author, subject to ethical and confidentiality considerations.

Acknowledgments

We would like to express our gratitude to all individuals who contributed to this project.

Declaration of Interest

The authors declare that they have no competing interests.

Funding

This research received no specific grant from any funding agency, commercial, or not-for-profit sectors.

REFERENCES

[1] Kaur, S., Bansal, S., & Bansal, R. K. (2014). Steganography and classification of image steganography techniques. In *Proceedings of the 2014 International Conference on Computing for Sustainable Global Development (INDIACom)*. https://doi.org/10.1109/IndiaCom.2014.6828087

[2] Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2018). A comparative study on the advancement of text steganography techniques in digital media. *ARPN Journal of Engineering and Applied Sciences, 13*, 1854-1863.

[3] Bhatt, S., Ray, A., Ghosh, A., & Ray, A. (2015). Image steganography and visible watermarking using LSB extraction technique. In *Proceedings of the 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*. https://doi.org/10.1109/ISCO.2015.7282315

[4] Bucerzan, D., & Raţiu, C. (2016). Testing methods for the efficiency of modern steganography solutions for mobile platforms. In *Proceedings of the 2016 6th International Conference on Computers Communications and Control (ICCCC)*. https://doi.org/10.1109/ICCCC.2016.7496734

[5] Chakraborty, S., Jalal, A. S., & Bhatnagar, C. (2017). LSB based non blind predictive edge adaptive image steganography. *Multimedia Tools and Applications, 76*(6), 7973-7987. https://doi.org/10.1007/s11042-016-3449-4

[6] Cui, W., Liu, S., Jiang, F., Liu, Y., & Zhao, D. (2020). Multi-stage residual hiding for image-into-audio steganography. In *Proceedings of the ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. https://doi.org/10.1109/ICASSP40776.2020.9054033

[7] Dalal, M., & Juneja, M. (2018). Video steganography techniques in spatial domain: A survey. In *Proceedings of the International Conference on Computing and Communication Systems*. https://doi.org/10.1007/978-981-10-6890-4_67

[8] Chandramouli, R., Kharrazi, M., & Memon, N. (2003). Image steganography and steganalysis: Concepts and practice. In *Proceedings of the International Workshop on Digital Watermarking*. https://doi.org/10.1007/978-3-540-24624-4_3

[9] Emad, E., Safey, A., Refaat, A., Osama, Z., Sayed, E., & Mohamed, E. (2018). A secure image steganography algorithm based on least significant bit and integer wavelet transform. *Journal of Systems Engineering and Electronics, 29*(3), 639-649. https://doi.org/10.21629/JSEE.2018.03.21

[10] Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access, 8*, 25777-25788. https://doi.org/10.1109/ACCESS.2020.2971528

[11] Joshi, K., Gill, S., & Yadav, R. (2018). A new method of image steganography using 7th bit of a pixel as an indicator by introducing the successive temporary pixel in the grayscale image. *Journal of Computer Networks and Communications*. https://doi.org/10.1155/2018/9475142

[12] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. *Neurocomputing, 335*, 299-312. https://doi.org/10.1016/j.neucom.2018.06.075

[13] Khan, S., Irfan, M. A., Arif, A., Ali, A., Memon, Z. A., & Khaliq, A. (2020). Reversible-enhanced stego block chaining image steganography: A highly efficient data hiding technique. *Canadian Journal of Electrical and Computer Engineering, 43*(2), 66-72. https://doi.org/10.1109/CJECE.2019.2938844

[14] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50*(1), 73-80. https://doi.org/10.1109/TSMC.2019.2903785

[15] Liu, J., Ke, Y., Zhang, Z., Lei, Y., Li, J., Zhang, M., & Yang, X. (2020). Recent advances of image steganography with generative adversarial networks. *IEEE Access, 8*, 60575-60597. https://doi.org/10.1109/ACCESS.2020.2983175