A Study and Review on Image Steganography

Trishna Paul, Sanchita Ghosh, and Anandaprova Majumder

Abstract Steganography is the science that involves encrypting data in a suitable multimedia carrier, such as image, audio, and video files. The main purpose of image steganography is to hide the data in images. This means that it encrypts the text in the form of an icon. Steganography is done when there is communication takes place between sender and receiver. In a day of data transfer over the network, security is paramount. Before the development of stenography, data security is a major research concern for researchers. Steganography is gaining importance due to the rapid development of users on the Internet and secret communication. In this paper, we discuss about various type of existing image steganography techniques and analyze the advantages and disadvantages of different types of image steganography techniques.

Keywords Steganography · Multimedia carrier · Communication · Data transfer · Security · Image steganography

1 Introduction

The challenges in protecting individuals' privacy are becoming more difficult as digital communication technology progresses and computing capacity and storage rises. The degree to which people value privacy varies from one person to the next. To protect personal privacy, numerous methods have been investigated and developed. The most noticeable is possibly encryption, followed by steganography. Encryption is sensitive to noise and is commonly observed, whereas steganography is not. Steganography is a widely used technique that manipulates information to hide their existence. Although steganography provides good security, the term stenography comes from the Greek words Stegano's (in enclosure) and Graptos (written) which

T. Paul (✉) · S. Ghosh · A. Majumder
Department of Computer Science and Engineering (CSE), Dr. B.C. Roy Engineering College,
Fuljhore, Durgapur, West Bengal 713206, India

A. Majumder
e-mail: anandaprova.majumder@bcrec.ac.in

S. Smys et al. (eds.), *Computer Networks and Inventive Communication Technologies*,
Lecture Notes on Data Engineering and Communications Technologies 75,
https://doi.org/10.1007/978-981-16-3728-5_40

literally translates “cover writing.” Stenography is commonly called ‘hidden’ contact. Steganography means hiding the presence of messages in other messages (audio, video, image, and communication). Multiple media such as images, audio, video, etc., are used as cover media by today’s stenography systems since digital images are frequently sent via email or distributed via other Internet communication applications. This is not the same as saving a message’s original material. In simple terms, it is the same as hiding information in other records [1–3].

1.1 Types of Steganography

Various stenographic techniques have been used to achieve protection depending on the type of core object.

Image Steganography: In stenography, covering as an image is referred to as a picture stenography. Typically, this technique uses pixel intensity to hide information [2].

Text Steganography: It consists of hiding data contained in text files. In this way, every text message’s ninth letter conceals sensitive information. In text files, there are several ways to hide data. These techniques are (a) Method based on format, (b) random and statistical method, and (c) linguistic method. Since a text file is not a suitable medium for steganography, it is one of the most challenging methods. It can be used to hide records. Knowledge is hidden in electronic texts and records and is one of the most critical of these technologies (e-documents). Another example is the use of text to hide information on web pages [4, 5].

Audio Steganography: Audio steganography is when audio is used as a carrier to conceal information. Audio steganography is accomplished using digital audio formats like WAVE, MIDI, MPEG AVI, or stenography. (a) Low-bit encoding, (b) phase coding, and (c) spread range are different techniques of audio steganography [4].

Video Steganography: It is a process used in digital video formats to hide some kind of files or information. As a carrier for printed content, video (a series of images) is used. Typically, the value of the discrete cosine transformation (DCT) (e.g., 6.668 to 7) that is used to hide the information that is visible to the human eye in each picture in the video varies. Steganography for video uses H.264, Mp4, MPEG, AVI, or other video formats [4].

Network Steganography: Network protocols such as TCP, UDP, ICMP, and IP are also used for application of steganography. Network protocol stenography is when you take key artifacts and use the protocol as a carrier. In the OSI network layer model, stencils can be retrieved from unused header bits in the TCP/IP field via encrypted channels [2]. Different steganography types are shown in Fig. 1 as follows.

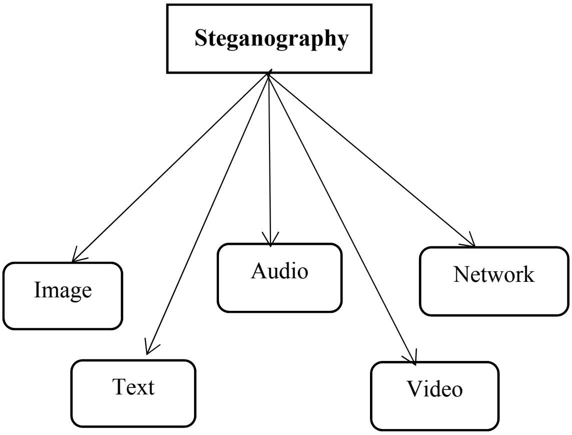

Fig. 1 Types of steganography diagram

2 History

Wax Table: People wrote hidden messages on wood in ancient Greece and then covered it with wax [6].

Shove Head: It was also used back in ancient Greece. The slave's head was shaken and secret messages were written on his skull. Then, the slave's hair was allowed to grow and the secret message came to the recipient after shaving his head again [6].

Invisible Ink: Encrypted messages were written using invisible ink which only appeared when the message-carrying paper was heated. As invisible inks, liquids like milk, vinegar, and fruit juice were used [6].

Morse Code: Hidden messages had been written on the yarn in Morris code. The fabric that the carrier wore was made of wool. Furthermore, at a television conference, Jeremiah Denton turned a blind eye to the Morse code for spelling the word "torture" This prompted the US military to ensure that in North Vietnam, US POWs were tortured [6].

3 Image Steganography Materials and Process

Stego-Key: The stego key is the key used to encrypt information in a coating and then take out the information. It can be a password or a digit provided with the support of a pseudorandom number generator for determining possible embedding locations [6].

Message: It is information that must be concealed in some type of digital media [6].

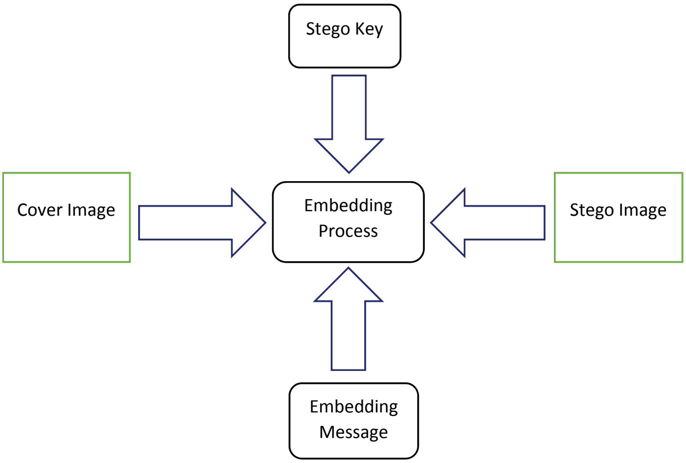

Fig. 2 Image steganography process

Cover Image: It is the medium by which messages like images, audio, video, and other digital media are transmitted [6].

Stego Image: The cover image is the stego image that has a hidden message hidden inside it. It is used to retrieve the secret message at the receiver location [6].

Usually, image steganography is a secret method of knowledge sketching and produces a stego image. This image of stigma was then sent via a well-known channel to the other party, where the other party does not realize that there is a secret message in this image of stigma. With or without a stego key, the secret message after the stego picture can be retrieved until the end of the received message [7]. The process of image steganography is shown in Fig. 2 as follows.

4 Image Steganography Techniques

The techniques of image steganography can be broken down into subsequent domains.

4.1 Spatial Domain Method

LSB and level encoding were used to modify the cover image and hidden data in the spatial domain. To begin, the cover image is decomposed into bit planes. After which, the LSB is replaced with hidden data suit. The most common steganographic technique is LSB substitution. Since it will not impact the value of the original pixel, this substitution definition involves embedding at the lowest weighting bit [8, 9].

Local domain techniques are broadly categorized into:

LSB (Least Significant Bit): To hide data, this method is commonly used. Embedding is done with bits of sensitive data in this form, removing the LSB of image pixels. After embedding, the image obtained is very close to the real picture as the shift in the least significant bit of the image pixel does not make any difference to the image [4, 9].

PVD (Pixel Value Differencing): Two consecutive pixels are chosen in this method to embed the data. Testing the difference between two consecutive pixels and determining whether the two pixels belong to an edge region or a flat area decide the payload [4, 10].

GLM (Gray Level Modification): Previously suggested, the procedure was developed in 2004 by Potdaret al. This method used to map the data (not embedding or hiding it) by altering the grey level values. This technique uses weird and even number concepts for map figures within an image. From the math function, pixels are selected from a given cover image. The gray surface values of these pixels are tested and compared to the bitstream that has to happen mapped in the picture [7].

PCM (Parity Checker Method): This technique made use of the notions of even and odd parity and the parity checker. Even parity refers to the presence of an even number of 1 s in the pixel value, while odd parity refers to the presence of an odd number of 1 s in the pixel value [11].

4.2 Transform Domain Method

To conceal data, the transform domain employs MSB. Because of its picture freedom, this technique is commonly used. Since it focuses on parts that have not changed, such as image editing, cutting, or resizing, transform domain is more powerful than LSB. In both harmful and illegal compression images, transform domain works best. Techniques for transforming domains are [2, 12]:

DFT (Discrete Fourier Transformation)

A discrete Fourier transform is a strictly discrete transform that transforms discrete time indicators into multiple frequencies of multiple frequencies in this technique. These techniques are changing a limited list of evenly spaced patterns of an event, including a list of rules for a complete set of complex sinusoids arranged by their frequency. It can be said that the sampling function is often converted from its real domain to a frequency domain along the line with time or position [13].

DCT (Discrete Cosine Transformation): DCT is one approach to convert signal to initial frequency ingredients. It displays an image as a summary of the sinusoids, different frequencies and dimensions [12].

DWT (Discrete Wavelet Transformation): This is a numerical instrument for figuratively dissolving an image. Useful for this signal processing which is non-stationary. The change is based on small waves of varying frequency and duration, called wavelets. Wavelet transformation is based on small waves of varying frequency and duration. The wavelet transform gives you image frequency as well as spatial clarity [12, 14].

4.3 Distortion Technique

By distorting the signal, this method is used to store hidden data. The encoder process modifies the cover image in a series of steps, and the decoder phase uses a hidden key to decipher the encrypted information back to the real information with the hidden data [13].

During the decoding process, distortion methods necessitate details about the original cover, and the code of conduct functions to measure the discrepancy between the initial cover picture and the new cover picture and the altered cover image in order to recover the encrypted message. The encoder modifies the cover image in a number of ways. As a result, information is known as signal distortion storage. The stego object is generated using this method by making various changes to the cover image. This collection of adjustments is made to match the coded message that must be transmitted. The message is encoded using pseudonyms and pixels chosen at random. The message bit returns ‘1’ if the stego-image at the given message pixel differs from the cover image, otherwise it returns ‘0’ [6].

4.4 Masking and Filtering

The data is hidden by labeling an image in this technique. When watermarks become a part of the picture, this method is advantageous. Rather than hiding the data in the noisy part of the image, it will be embedded where it is more important. Watermarking methods are more integrated into the picture and can be used without fear of destroying it. For the cover picture, the hidden message is more relevant. In 24-bit and greyscale images, this technique is used [4, 13].

5 Analysis of Different Domain and Techniques of Image Steganography

Domain	Techniques	Advantages	Disadvantages
Spatial	LSB	It is used for data insertion purposes It is really easy to execute [2]	Recovered quickly by an unauthorized individual [2]
	PVD	Strong embedding capability and exceptional stego-image imperceptibility [2]	Two connecting pixels divide the cover image into non-overlapping blocks, in each section, in each block (pair), for embedded data and adjustments to different pixels [2, 10]
	GLM	It has a low computational complexity and a large capacity for knowledge concealment [7]	Include binary data. It is necessary to map from one to one The modification of the image causes data loss Embedding capacity is limited [7]
	PCM	For message insertion and retrieval, there is an odd and even parity Recovery of message bits from all locations is permitted [7]	The capability of payloads is low [7]
Transform	DFT	Changes can be applied to the entire image [2]	Such types of approaches are computationally complex [2]
	DCT	Peak signal-to-noise ratio is high (PSNR)[2]	Noticeable secret data artifact [2]
	DWT	It is only useful for binary images [2]	It is not useful for color image support [2, 14]
Masking and filtering	(i) Process LSB is more efficient. The data is unaffected by the compression of the image [15] (ii) Data is hidden in parts of the image that are visible [2]		These techniques are limited to 24 bits and can only be used on grayscale images [2]

6 Conclusion

We reviewed several articles on steganography methods in this research paper. Steganography is an ancient and robust technique used in a variety of applications, including confidential data sharing. When used in conjunction with cryptography, steganography becomes more powerful. The advantages and disadvantages of various image stenography methods are discussed. It is impossible to foresee the best route. Message concealment can be achieved effectively using LSB, according to recent local domain techniques.

Acknowledgements I would like to express my gratitude to my supervisor, my friend, Ms.Sanchita Ghosh (Student of Dr. B C Roy Engineering College), who guided me throughout this paper. I would also like to thanks my professor Mrs. Anandaprova Majumder (Asst. Professor of Dr. B C Roy Engineering College), who advised and helped me to finalized my project.

References

1. Nosrati, M.: An introduction to steganography methods, Aug 2011 (2016)
2. Hussain, M., Hussain, M.: A survey of image steganography techniques (2013)
3. Chanu, Y.J., Tuithung, T., Manglem Singh, K.: A short survey on image steganography and steganalysis techniques. In: 2012 3rd National Conference on Emerging Trends and Applications in Computer Science, Shillong, India, pp. 52–55 (2012). https://doi.org/10.1109/NCETACS.2012.6203297
4. Kour, J.: Steganography techniques—a review paper, vol. 9359, no. 5, pp. 132–135 (2014)
5. Singh, P., Chaudhary, R., Agarwal, A.: A novel approach of text steganography based on null spaces. IOSR J. Comput. Eng. (2012) academia.edu
6. Tiwary, A.: Different image steganography techniques : an overview. Int. J. Comput. Eng. Appl. 0–13 (2019)
7. Hashim, M.M., Rahim, M.S.M., Alwan, A.A.A review and open issues of multifarious image steganography techniques in spatial domain. J. Theor. Appl. Info. Technol. **96**(4), 956–977 (2018)
8. Rakhi, & Gawande, S.: A review on steganography methods. IJAREEIE, **2**(10), 4635–4638 (2013)
9. Hashim, M.M., Rahim, M.S.M., Johi, F.A., Taha, M.S.: Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. Int. J. Eng. Technol. (2018) uruk.edu.iq
10. Rawat, P., Pandey, A.K., Singh Kushwaha, S.: Advanced image steganographic algorithms and breaking strategies. Int. J. Comput. Appl. (IJCA) concern (2014)
11. Rajkumar, Rishi, R., Batra, S.: A new steganography method for gray level images using parity checker. Int. J. Comput. Appl. **11**(11), 18–24 (2010). https://doi.org/10.5120/1627-2188
12. Sharma, S., Kumar, U.: Review of transform domain techniques for image steganography. Int. J. Sci. Res. ISSN (Online Index Copernicus Value Impact Factor) **4**(5), 194–197 (2015). https://doi.org/10.13140/RG.2.1.4797.1928
13. Arya, A., Soni, S.: A literature review on various recent steganography techniques, pp 143–149 (2018)

14. Nag, A., Biswas, S., Sarkar, D., Sarkar, P.P.: A novel technique for image steganography based on DWT and Huffman encoding. Int. J. Comput. Sci. Secur. (2011)
15. Chandramouli, R, Memon, N.: Analysis of LSB based image steganography techniques. In: Proceedings of 2001 International Conference on Image Processing (Cat. No. 01CH37205), pp. 1019–1022 (2001)