International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 July – 2022
DOI:10.46647/ijetms.2022.v06i04.001 ISSN: 2581-4621

A Comprehensive study of digital Image Steganography Techniques

Dr Arun Kumar Singh
Department of Electronics and Comm. Engineering,
Amity University
Arunsingh86@gmail.com

Abstract: In the digital era of the internet, steganography is critical for data security. Steganography is a new field that is used to hide hidden information, and there has been a lot of research done so far. Based on the reviewed literature, this paper describes image steganography technology and its evaluation criteria. The main goal of this research is to demonstrate the potent influence of image steganography in concealing information regardless of media. If the PSNR is larger than 40db, imperceptibility is one of the essential evaluation requirements to ensure security.
Keywords: Image Steganography; spatial domain, transform domain; evaluation criteria

1. Introduction

Image steganography refers to hiding information i.e. text, images or audio files in another image or video files into the image in such manner so that it cannot be identified by human visual system. Image steganography majorly being performed into spatial or transform domain techniques though it is categorized into four domains as shown in fig 1. The aims of this paper is to provide a brief of image steganography techniques, terminology and evaluation parameter along with a detail literature which gives the insight of a work done in this domain.

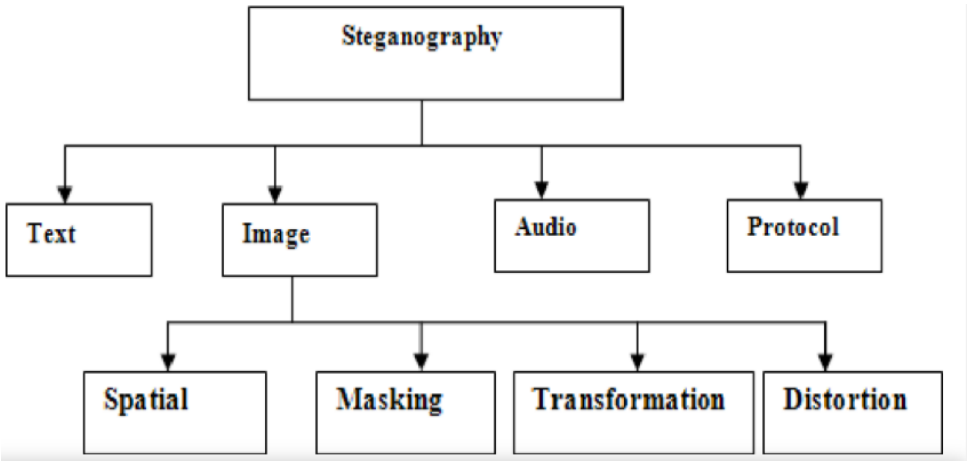

Figure 1: Classification techniques of Image steganography [13]

2. Image Steganographic Techniques [9]

Image steganography techniques can be divided into following domains depending on method used.

- **Spatial Domain Methods**

There are numerous different types of spatial steganography, all of which hide data by changing some bits in the image pixel values. The least significant bit (LSB)-based steganography approach is the most widely used spatial domain steganography technology, which hides a secret message in the LSBs of pixel values without creating many observable distortions. The human visual system cannot detect changes in the LSB value .

- **Transform Domain Technique**

The method of embedding data in a signal's frequency domain is far more powerful than embedding principles in the time domain. It is one of the most powerful Image steganography systems in the transform domain. Transform domain techniques outperform spatial domain techniques by hiding information in portions of the image that are less susceptible to compression, cropping, and image processing. Some transform domain approaches appear to be unaffected by picture format, and they may be able to outpace lossless and lossy format conversions.

- **Distortion Techniques**

While decoding, this approach requires the information from the original cover image. In order to restore the secret message, the decoder checks for variations between the original cover image and the deformed cover image. The encoder modifies the cover image in a series of steps. As a result, signal distortion is used to describe how information is stored. A stego object is made using this technique by applying a series of alterations to the cover image. This modification sequence is used to match the secret message that must be transmitted.The message is encoded at pseudo-arbitrarily chosen pixels, and the "1" value pixels are modified so that the image's attributes are not altered. The message bit is a "1" if the stego-image differs from the cover picture at the provided message pixel. The message bit is a "0" otherwise. The alteration can even be reversed and the original message recovered provided the message is encoded with error correcting information.

- **Masking and Filtering**

These methods encrypt data by leaving a mark on an image, similar to how watermarks do. Rather of merely burying the information in the commotion level, these strategies embed it in more significant regions. The cover art is more important because of the hidden message. Since then, watermarking techniques have become increasingly widely used in photos, without regard for the loss of image quality caused by lossy compression.

3. LITERATURE REVIEW

A Lot of research work have been done in the field of image steganography, the work proposed,the enthusiasm of quick development for steganography for two primary reasons:

i. The distributing and broadcasting ventures have turned out to be keen on procedures for covering up scrambled copyright imprints and serial numbers in advanced movies, sound chronicles, books and sight and sound items.

ii. Moves by different governments to limit the accessibility of encryption administrations have inspired individuals to examine techniques by which private messages can be implanted in apparently safe cover. [8]

Cheddad et al. (2010) propose the notion of concealing data in digital images using common rules and, after analysing the various approaches, recommend the embedding mechanism of data into images that are not traceable by the human visual system. Modern digital technology has shattered trust in the integrity of visual representation. The authors

Website: ijetms.in Issue: 4 Volume No.6 July – 2022
DOI:10.46647/ijetms.2022.v06i04.001 ISSN: 2581-4621

presented a security solution that uses self-embedding techniques to safeguard scanned documents from counterfeiting. The approach not only detects forgeries, but it also allows legal or forensics specialists to obtain the original document, even if it has been tampered with [4].

Bera et al. (2010) use two methods to discover hidden data in images. The first approach compares the histograms of the stego and cover image to detect hidden data. In the second technique, the probability distribution function is employed to detect concealed data using an image smoothening technique. The detection of the cover picture is based on the difference in statistical parameters of the stego image [2].

Ibrahim et al. (2011) created a Steganography Imaging System (SIS) to test the proposed system and to determine the viability of various data sizes stored inside the photos. For each of the photos evaluated, the PSNR (peak signal-to-noise ratio) is also recorded. The stego image, which has a higher PSNR value than the other images, is particularly effective at hiding the data within the image [10].

Al-shatnawi et al. (2012) proposed a simple and fast method that produces great image quality while achieving a higher accuracy of 83 percent. When comparing the LSB benchmarking approach to the proposed method, the proposed method achieves a greater accuracy. It is used to conceal a hidden message on two Bmp images [1].

Rahna et al. (2013) developed a new lossless approach with indefinite payload capacity and better security by changing the image in a way that the human visual system cannot detect. The degree of communication security, key size, and payload capacity are the fundamental concerns that have yet to be adequately solved [16].

Roy et al. (2013) compares multiple algorithms for digital picture steganography in the spatial and transform domains with varied parameters in order to provide insight into future research [17].

Fadel Alwan et al. (2015) propose two methods: the first uses a genetic algorithm with LSB to provide a high PSNR value and payload, and the second technique is utilised to retain picture quality during image restoration to achieve superior visual quality[8].

Caeiro et al. (2015) advocate that Huffman encoding be modified from Progressive DCT, Huffman encoding to Baseline DCT, Huffman encoding in order to make it more difficult to detect the concealed message in the process. The steganography file does not contain the original file's comment. The fact that the file sizes differ implies that the files are steganographic [3].

Umbarkar et al. (2016) compare the various spatial domain image steganography approaches on colour and grayscale images to hide data, and they prefer the LSB techniques to hide data in the sharper region and subsequently in the smooth part of an image. The quality, colour, and texture of an image, as well as the size of the message, all influence data embedding. They developed a novel method for improving efficiency and performance without sacrificing image quality by analysing various methodologies [20].

Munesh et al. (2017) introduced data concealing strategies in images by combining LSB techniques with the AES encryption algorithm. Because encryption is utilised here and files are password secured, the concealed file could be either a text or an audio file, providing extra protection while transmitting the stego image [15].

By comparing prior known watermarking approaches, Douglas et al. (2018) proposed steganography strategies to efficiently disguise biometric data (fingerprint). In water marking, the hidden information might be visible or invisible to human eyes, however steganography is used to hide crucial information that is invisible to human eyes since the quality of the stego image is maintained at the same level as the original image[7].

Website: ijetms.in Issue: 4 Volume No.6 July – 2022
DOI:10.46647/ijetms.2022.v06i04.001 ISSN: 2581-4621

According to Joshi et al. (2018), 7bit concealing techniques in the frequency domain provide great capacity and have a high frequency of availability across the internet. The PSNR and MSE parameters were used to test the method's efficiency after it was implemented [11].

Cui et al. (2019) propose a generative adversarial network based picture steganography technique as a mainstream approach to convert communication. These processes prefer data concealment in the well-textured region, which reduces the likelihood of hidden data detection. Message embedding can be executed directly into the chosen cover image with greater accuracy utilising GAN-based image steganography. In GAN, the foreground object region is created onto a given cover image by the GAN, and the secret data is embedded in the foreground object region at the same time that the region is being generated [6].

Optimized was proposed by Corley et al. (2019) to delete Steganographic content while maintaining the perceived quality of the original image. In comparison to existing state-of-the-art filtering approaches, our model is capable of providing a high rate of destruction of Steganographic image material while keeping a good visual quality, as demonstrated by testing results [5].

Zhang et al. (2019) proposed employing generative adversarial networks to hide arbitrary binary data in photos, allowing us to optimise the perceived quality of the images produced by our model. The suggested method achieves state-of-the-art data concealment with 4.4 bits per pixel payloads, evades detection by steganalytic tools, and works on images from multiple datasets [23].

Varalakshmi et al. (2020) proposed adopting the spatial domain Steganographic technique to protect sensitive information from being steganalytical attacked by embedding the data into the cover image. They built a novel encoding and decoding algorithm in Matlab that outperforms the old approach in terms of performance evaluation [21].

Wu et al. (2020) proposed an improved security of image steganography with the least amount of distortion; these models must keep the feature maps created by task-specific networks independent of any concealed information buried in the carrier. To help alleviate the security issue, this paper incorporates a binary attention method into picture steganography to aid enhance embedding payload capacity, and in the meantime [22].

Kumar et al. (2020) suggested a steganalytic method based on artificial intelligence that uses deep features extracted from stego pictures using deep CNN techniques. This work [14] also presented a steganalytic based on low embedding rate pictures and multi-class steganography.

3. Image Steganography Terminologies

- **Cover-Image:** Original image which is used as a carrier for hidden information.
- **Message:** Actual information which is used to hide into images. Message could be a plain text or some other image.
- **Stego-Image:** After embedding message into cover image is known as stego-image.
- **Stego-Key:** A key is used for embedding or extracting the messages into cover-images or from stego-image respectively.

4. Performance evaluation Parameters

Image quality assessment metrics are based upon the MSE and PSNR. These metrics are simple to calculate, mathematically convenient, and have clear physical meanings. A new

Website: ijetms.in Issue: 4 Volume No.6 July – 2022
DOI:10.46647/ijetms.2022.v06i04.001 ISSN: 2581-4621

approach to assess image quality independent of the type and size of pixel size of concerned stego images is the estimation of Structural Similarity indices using Structural Similarity Index metric (SSIM) and Payload.

- **Imperceptibility:** steganography algorithm's imperceptibility refers to its invisibility. Bec ause it is the first and most important prerequisite, because steganography's strength reside s in its ability to go unnoticed by the human eye [13].
- **BitError Rate:**The secret information can be recovered using the communication channel successfully. It must be ideal, but in fact, the error arises when concealed data is retrieved, and BER measures this. It's the proportion of image errors to total bits delivered [13].
- **Mean-Square Error (MSE):** The cumulative square error between the compressed and original picture is represented by the mean-square error, and the peak error is represented by the PSNR. The smaller the MSE, the smaller the error. To compare image compression quality, the mean-square error and peak signal-to-noise ratio are used [8].
- **Peak Signal-to-Noise Ratio (PSNR):** The original cover picture and stego image's quality is measured using the peak signal-to-noise ratio. The measurement is in decibels, and the PSNR value should be larger than 30 decibels in general. The higher the PSNR, the higher the image quality of the stego image [8].

$$\text{MSE}=\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|f(i,j)-g(i,j)|^2$$

$$\text{PSNR}=20\log_{10}[\frac{f(i,j)_{max}}{MSE^{1/2}}]$$

Where,

M &N are size of cover image,

f(i,j) is cover image and,

g(i,j) is stego image,

- **Structural similarity index measure (SSIM):**The structural similarity index measure (SSIM) is a parameter that measures how similar the cover picture and the stego image are. The two photos are compared using statistical characteristics such as mean and variance [8].
- **Payload:**The amount of hidden information per pixel in a stego image is measured in bits per pixel (BPP).

5. Conclusion and Future Scope:

This paper discussed various domains of image steganography techniques for hiding the secret information. The imperceptibility is one the important measure for image steganography that can be considered by achieving high PSNR value depending upon the MSE value, das discussed in section 4. Based on the conducted literature in this paper it can be calculated that transform domain techniques is better for image steganography in terms of quality and security. There are factors that must be considered in future:

- Increasing embedding efficiency
- Decreasing the embedding distortion
- Choosing the alternative color spaces

References:

1. Al-Shatnawi, A. M. (2012). A new method in image steganography with improved image quality. Applied Mathematical Sciences, 6(79), 3907-3915.

2. Bera, S., & Sharma, M. (2010). Steganalysis of Real Time Image by Statistical Attacks. International Journal of Engineering Science and Technology, 2(9), 4396-4405.

3. Caeiro, D., & Sanjana, S. Detection of Steganography using Metadata in Jpeg Files. (http://dx.doi.org/10.5769/J201501003)

4. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3), 727-752.

5. Corley, I., Lwowski, J., & Hoffman, J. (2019). Destruction of Image Steganography using Generative Adversarial Networks. arXiv preprint arXiv:1912.10070.

6. Cui, Q., Zhou, Z., Fu, Z., Meng, R., Sun, X., & Wu, Q. J. (2019). Image steganography based on foreground object generation by generative adversarial networks in mobile edge computing with Internet of Things. IEEE Access, 7, 90815-90824.

7. Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications, 77(13), 17333-17373.

8. fadelAlwan, N., &Abdulwahid, N. N. (2015). PSNR Comparison for LSB Steganography using Genetic Algorithm or Image Restoration. International Journal of Recent Scientific Research, 6(10), 6830-6835.

9. Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques.International Journal of Advanced Science and Technology Vol. 54.

10. Ibrahim, R., &Kuan, T. S. (2011). Steganography algorithm to hide secret message inside an image. arXiv preprint arXiv:1112.2809.

11. Joshi, K., Gill, S., & Yadav, R. (2018). A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image. Journal of Computer Networks and Communications, 2018.

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, 299-326.

13. Kaur, H., & Rani, J. (2016). A Survey on different techniques of steganography. In MATEC Web of Conferences (Vol. 57, p. 02003). EDP Sciences.

14. Kumar, V., Rao, P., & Choudhary, A. (2020). Image Steganography Analysis Based on Deep Learning. Journal homepage: http://iieta. org/journals/rces, 7(1), 1-5.

15. Munesh Kumar, Gaurav Yadav2 Ashish Kumar Keshari, Sandhya Katiyar(2017). Image Processing using Steganography. International Journal of Engineering Science and Computing , 7(4).

16. Rahna, E., & Govindan, V. K. (2013). A Novel Technique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegoimage. International Journal of Advances in Engineering & Technology, 6(3), 1263.

17. Roy, R., Changder, S., Sarkar, A., & Debnath, N. C. (2013, January). Evaluating image steganography techniques: Future research challenges. In 2013 International Conference on Computing, Management and Telecommunications (ComManTel) (pp. 309-314). IEEE.

18. Savitha Bhallamudi (2015). Image IMAGE STEGANOGRAPHY. Technical Report DOI: 10.13140/RG.2.2.21323.18727

19. Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., &Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.

20. Umbarkar, A. J., Kamble, P. R., & Thakre, A. V. (2016). COMPARATIVE STUDY OF EDGE BASED LSB MATCHING STEGANOGRAPHY FOR COLOR IMAGES. ICTACT Journal on Image & Video Processing, 6(3).

21. Varalakshmi, R. (2019). DIGITAL STEGANOGRAPHY FOR PREVENTING CYBERCRIME USING ARTIFICIAL INTELLIGENCE TECHNOLOGY. Journal of Critical Reviews, 7(6), 2020.

22. Wu, P., Chang, X., Yang, Y., & Li, X. (2020). BASN—Learning Steganography with a Binary Attention Mechanism. Future Internet, 12(3), 43.

23. Zhang, K. A., Cuesta-Infante, A., Xu, L., &Veeramachaneni, K. (2019). SteganoGAN: High capacity image steganography with GANs. arXiv preprint arXiv:1901.03892.