An Extensive Study of Digital Image Steganography Techniques

Juhi Singh[*1] *and Mukesh Singla*[2]

Abstract

The rise of digital technology raises the importance of data security when transmitting data across a wireless communication medium. Steganography is a method of ensuring information security on a digital media. The goal of this work is to look at information hiding techniques in images which are in the spatial domain. This paper will also distinguish between watermarking and steganography, the two most popular domains of information concealment. The paper examines the benefits and drawbacks of existing algorithms, tools, and strategies to safeguard data in the digital image steganography domain.

Keywords : **Data hiding, information security, steganography, time domain techniques, watermarking**

I. INTRODUCTION

Hiding information behind any cover medium is not a new concept; it has existed since ancient times. Securing digital information over the internet is challenging as per the technological advancement in transmission technology. To obtain the security of the transmitted data, the integrity of information hiding approaches plays a vital role in hiding information that is being shared. In this paper, the focus is on the information hiding approaches, which can be broadly classified into Watermarking and Steganography [1]. A detailed comparison is included in Table I. As compared to data encryption techniques, Steganography and Watermarking are somehow related to each other. Watermarking approaches are generally used for copyright protection in data as well as images whenever there is an issue of authenticity of data [2]. Robust watermarking works better in protecting copyright issues of information and fragile watermarks protect the authenticity of information [3]. As far as information security is concerned, digital watermarking would be an appropriate term rather than watermarking. For better results, spatial or transform domains can be applied to hide the information [4]. To detect the embedded information, watermarking can be classified into three groups. A non-blind category requires the cover image at the time of detection but blind techniques are not required. In a semi-blind approach, the key is also required alongwith watermarked document [5]. Generally, steganography and watermarking can be considered a similar approach but this is not the reality. Watermarked images are limited with imperceptibility and robustness but both can't be achieved at the same time. To attain robustness, low-frequency signals should be added to the original signal, whereas imperceptibility should be added in high-frequency components of the original signals of an image. It is clear that the watermarking system works better with low-frequency signals and sometimes it is under the attack of image degradation and image enhancement attacks [1, 6, 7].

Steganography techniques can be broadly categorized into linguistic and technical steganography [8] as shown in Fig. 1.

Manuscript Received : July 5, 2022 ; Revised : July 16, 2022 ; Accepted : July 18, 2022. Date of Publication : August 5, 2022.

J.Singh[*1], *Research Scholar,* Department of Computer Science & Engineering, Baba Mastnath University, Rohtak - 123 106, Haryana. Email : juhisingh17@gmail.com ; ORCID iD : https://orcid./org/0000-0003-1599-2412

M. Singla[2], *Professor,* Department of Computer Science & Engineering, Baba Mastnath University, Rohtak - 123 106, Haryana. Email : mukesh27singla@yahoo.co.in ; ORCID iD : https;//orcid.org/0000-0002-3172-9780

DOI : https://doi.org/10.17010/ijcs/2022/v7/i4/172378

TABLE I.

CHARACTERISTIC TABLE OF STEGANOGRAPHY AND WATERMARKING [2, 4]

Characteristic	Steganography	Digital watermarking
Target	Presence of information from detection	Maintaining the authenticity
Cover selection	Any medium	Restricted
Visibility	None	Sometimes
Key	Optional	Optional
Output	Stego-image	Watermarked file
challenges	Imperceptibility, capacity, and security	Robustness
Attack	Steganalysis	Any image processing system
Approach	Generally Irreversible	Generally reversible

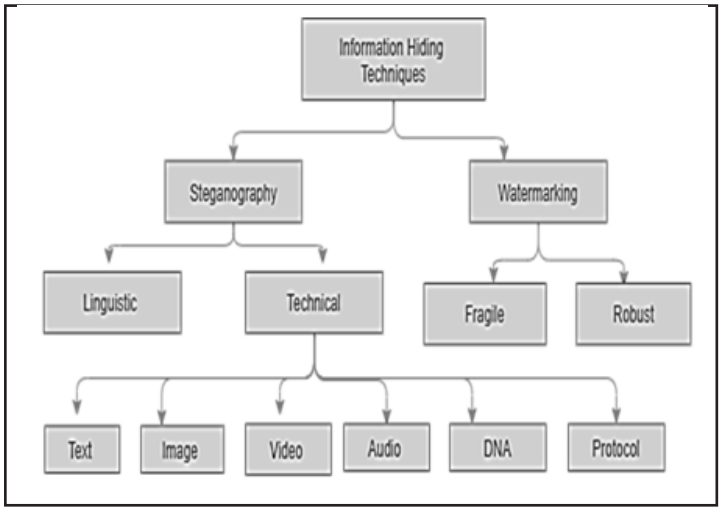

Fig. 1. Data Hiding Approaches [9]

A. Linguistic Steganography

In linguistic steganography, natural languages are being used as a medium to conceal information. The sophisticated approaches in linguistic steganography try to capture the same syntax as the natural languages and also apply the context-free grammar of the natural language syntax as a cover medium [4]. The linguistic Steganographic approach works better by dividing into two sub- approaches, (a) synonym substitution, and (b) semantic transformation. The synonym substitution has an issue of low security and the semantic transformation approach suffers from semantic spam, yet both approaches can provide high invisibility and robustness in one or another way.

B. Technical Steganography

This technique uses the scientific method to conceal secret information by using microdots or some invisible ink. It can also utilize size reduction methods in cover images [10]. The hiding can be done in audio, video, text, and digital images. Technical steganography is comparatively more popular than linguistic steganography because it has a similar advantage as text steganography in terms of performance and development of the data hiding process. Lack of security and low performance are the key reasons and more on the linguistic approaches are not time efficient while performing the hiding [11].

II. STEGANOGRAPHY

Steganography requires multiple steps at the receiver end and transmitter end. Art of concealing the existence of information during digital communication by embedding of a secret message into any medium as described in Fig. 1 through any devices and services.

A. Steganography Procedure

Data hiding can be achieved by following steps [12]:

- Media carrier : Used to covert information concealed within it via transmission.
- Secret data : This might be data, a file, or an image, among other things.
- Secret Key : A covert key that is used to encode and decode hidden information.
- Stego media (Y) : Following the process of embedding the covert information at this level [13].

The text, audio, video, protocols, DNA, and digital images are the major information carriers in technical steganography systems to conceal the information. Table II describes their advantages and disadvantages.

The text, audio, video, protocols, DNA, and digital images are the major information carriers in technical steganography systems to conceal the information. Table II describes their advantages and disadvantages.

B. Parameter of Evaluation

To evaluate the performance of image steganography different aspects are used. Some of the important and popular matrices are included in this paper as below [2, 15]:

(a) Peak Signal to Noise Ratio (PSNR) : This parameter compares the two images and how much they are like each other. If both images are similar then this parameter has a large value. As shown in eq. (1) it is used to calculate the Mean Square Error, i.e. MSE and after by using eq. (2) the PSNR value would be calculated.

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (1)$$

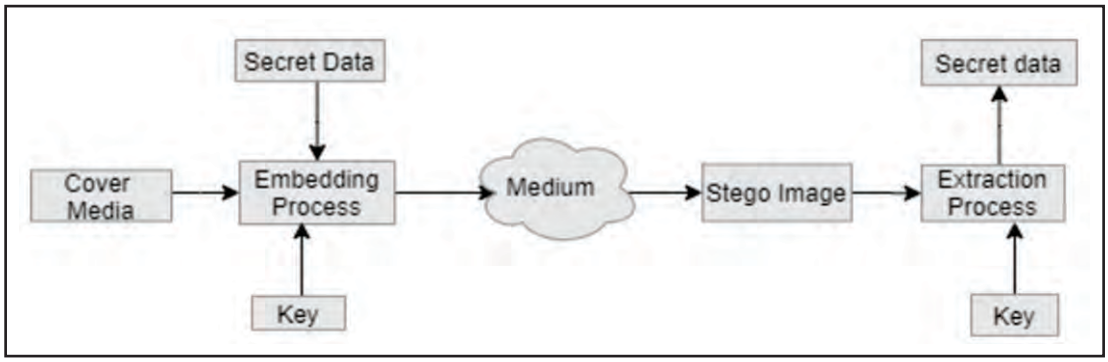

Fig. 2. Process of Steganography [12]

TABLE II.

PROCESS OF INFORMATION HIDING IN DIFFERENT MULTIMEDIA CARRIERS [14]

Carrier medium	Hiding Process	Advantages	Disadvantages
Text	Changing the text layout and rules can hide the information hidden in text	Easy implementation	Security, time efficiency, and performance
Image	Modifying the edge value of RGB in case of color images or modifying the LSB (in the time domain) and transforming the frequency or wavelet	Imperceptibility and security	Distortion due to frequency modulation
Audio	Frequencies that humans can't detect.	High capacity and payload	Distortion due to frequency modulation
Video [4]	Manipulating the compressed bit stream	Robustness, low distortion	High sensitivity
Protocol	Allows network protocols to hide the information	High security	Prone to network vulnerability
DNA	Use a double layer of data hiding by altering DNA sequencing	Comparatively better hiding capacity	High complexity

$$PSNR = 10 \text{ LOG }_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

Where,

I_1 & I_2 are m×n monochrome image

M & N are the dimensions of the image

m & n are the pixels of image

R is maximum signal value

(b) Structural Similarity Index Measures (SSIM) : Like the PSNR, the structural index also measures the similarity between windows of any two images as shown in Eq. (3) [16]

$$SSIM(x,y) = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3)$$

$$C_1 = (k_1 L)^2$$

$$C_2 = (k_2 L)^2$$

Where,

μ_x : the average of x

μ_y : the average of y

σ_x^2 : the variance of x

σ_y^2 : the variance of y

σ_{xy}^2 : the covariance of x and y;

c_1 & c_2 : two variables to stabilize the division with weak denominator;

k_1 = 0.01(default value)

k_2 = 0.03(default value)

L : the dynamic range of the pixel-values

x & y *are window of images of* NxN size

Here μ_x *and* μ_y show mean intensity values and σ_x^2, σ_y^2, and σ_{xy}^2 show the variance of the corresponding variable in suffix respectively. The two stabilizing parameters are c_1 and c_2, L is the limit of a pixel, and k_1 and k_2 content.

III. IMAGE STEGANOGRAPHY

It uses an image as a carrier that hides the information/secret data into the image itself. This will be helpful to protect the intellectual property of an image from any unwanted attacks. The entire process has three segments [1]:

- Hiding information into cover images: concerns where to hide the message
- Security of embedded process
- Payload capacity

Steganography can be majorly categorized into spatial domain and transform domain [17]. A comprehensive comparison between spatial and transform domains are included in Table III [17. 5, 15, 11].

A. Spatial Domain Image Steganography

The image domain or spatial domain uses the intensity distribution to conceal secret information into the pixel intensity of an image by directly manipulating the image pixels [17, 18]. Spatial domain techniques provide several methods to embed data into any cover medium but among all methods of spatial domain techniques, the Least Significant Bit (LSB) is one of the most significant methods [13, 19].

B. Transform Domain

The frequency domain or transform domain provides high

TABLE III.

THE CHARACTERISTIC DIFFERENCE BETWEEN SPATIAL AND TRANSFORM DOMAIN

Characteristics	Spatial Domain	Transform Domain
Embedding Capacity	High	Low
Computation Cost	Low	High
Computational Time	Less	More
Robustness	Fragile	High
Security	Geometric attacks [1]	Resistant to geometric attacks
Imperceptibility	High [1]	Less controllable
Format dependency	Dependent	Independent

embedding rate due to its discreteness. Transform domain techniques are very time efficient and comparatively secure against attack. Discrete Cosine Transform (DCT) and Discrete Wavelength Transform (DWT) are very popular frequency domain techniques [17, 20].

IV. CONCLUSION

A recent research of image steganography techniques in digital photographs is presented in this work. This study also includes a full treatment of watermarking and image steganography. Image steganography approaches carrier-based classification and domain-based classification are also discussed. Technical steganography, according to literature is used to conceal information in any medium, whereas linguistic steganography, which is similar to text steganography is used to conceal information in any medium. However, most of the previous references do not elaborate on linguistic steganography, which is included here. Hence, this paper concludes that transform domain techniques are better in terms of security and robustness as compared to spatial domain. Spatial domain techniques provide better PSNR but suffer from noise.

AUTHORS' CONTRIBUTION

Juhi Singh is the author and performed the entire work describe in this paper under the guidance of Mukesh Singla. She did all the survey and analysis.

CONFLICT OF INTEREST

The authors certify that they have no affiliation with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter in materials discussed in the manuscript.

FUNDING ACKNOWLEDGEMENT

The authors have not received any financial support for this research, authorship, and/or for the publication of the article.

REFERENCES

[1] J. Singh and M. Singla, "Image Steganography Technique based on Singular Value Decomposition and Discrete Wavelet Transform," *Int. J. Electr. Electron. Res.,* vol. 10, no. 2, pp. 122–125. [Online]. Available: https://ijeer.forexjournal.co.in/papers-pdf/ijeer-100212.pdf

[2] G. C. Kessler and C. Hosmer, "An overview of steganography," *Advances Comput.*, vol. 83, pp. 51–107, 2011, doi; 10.1016/B978-0-12-385510-7.00002-3.

[3] A. K. Singh, J. Singh, and H. V. Singh, "Steganography in images using LSB technique," *Int. J. Latest Trends Eng. Technol.*, vol. 5, no. 1, pp. 426–430, 2015. https://www.ijltet.org/wp-content/uploads/2015/02/60.pdf

[4] A. U. Rahman, K. Sultan, D. Musleh, N. Aldhafferi, A. Alqahtani, and M. Mahmud, "Robust and fragile medical image watermarking: A joint venture of coding and chaos theories," *J. Healthcare Eng.*, vol. 2018, 2018, Art. no. 8137436.

[5] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," *Signal Process.: Image Communication*, vol. 65, pp. 46–66, 2018, doi: 10.1016/j.image.2018.03.012.

[6] S. Jeevitha and N. A. Prabha, "A comprehensive review of steganographic techniques and implementation," *ARPN J.Eng. Appl. Sciences*, vol. 13, no. 17, pp. 4780–4791, 2018. http://www.arpnjournals.org/jeas/research_papers/rp_2018/jeas_0918_7268.pdf

[7] J. Nanwal and P. Nanwal, "Design and implementation of Spatial Domain Technique in Steganography using RSA Encryption with genetic algorithm," *Indian J. Comp. Sci.*, vol. 2, no. 5, pp.13–18, 2017.

[8] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "A comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2018.

[9] F. Y. Shih, "Digital watermarking and steganography: Fundamentals and techniques, 2017. CRC press.

[10] H. N. Khalid and A. H. M. Aman, "Digital Image

Steganography in spatial domain: A critical study," Technol. Reports of Kansai University, vol. 62, pp. 4559–4569, 2020.

[11] A. K. Singh, H. V. Singh, and J. Singh, "Highly Impartible Spatial Domain Steganography in Double Precision Images," *2nd Int. Conf. Inventive*, 2018, pp. 768–771.

[12] M. S. Abuali, C. B. M. Rashidi, M. H.Salih, R. A. A. Raof, and S. S. Hussein, "Digital Image Steganography in Spatial Domain a comprehensive review," *J. Theoretical Appl. Inf. Technol.*, vol. 97, no. 19, pp. 5081–5102, 2019. http://www.jatit.org/volumes/Vol97No19/10Vol97No19.pdf

[13] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications, and attacks," *Int. J. Eng. Innovative Technol.*, vol. 2, no. 9, pp. 165–175, 2013. https://www.ijeit.com/vol%202/Issue%209/IJEIT1412201303_31.pdf

[14] S. Utama, R. Din, and M. Mahmuddin, "A comparative study of Text Steganography and Linguistic Steganography," in *Proc. Conf. Eng. Technol*., Vocation Educ. Social Sci., 2015, Universiti Pendidikan Sultan Idris,Tanjung Malim.

[15] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," *Neurocomputing*, vol. 335, pp. 238–250, 2019, doi: 10.1016/j.neucom.2018.09.091

[16] Z. Wang, E.P. Simoncelli, A. C. Bovik, "Multiscale structural similarity for image quality assessment," in *Conf. Record 37th Asilomar Conf. Signals, Syst. & Comput.*," vol. 2., pp. 1398–1402, 2003, doi: 10.1109/ACSSC.2003.1292216.

[17] B. T. Ahmed, "A systematic overview of secure image steganography," *Int. J. Advances Appl. Sci.*, vol. 10, no. 2, pp. 178–187, doi: 10.11591/ijaas.v10.i2.pp178-187.

[18] D. M. Abdullah, S. Y. Ameen, N. Omar, A. A. Salih, D. M. Ahmed, S. F. Kak, H. M. Yasin, I. M. Ibrahim, A. M Ahmed, and Z. N. Rashid, "Secure data transfer over internet using image steganography: Review," *Asian J. Res. Comp. Sci.*, vol. 10, no. 3, pp. 33–52, 2021, doi: 10.9734/ajrcos/2021/v10i330243.

[19] A. K. Singh, J. Singh, and H. V. Singh, "Steganography in images using LSB technique," *Int. J. Latest Trends Eng. Technol.*, vol. 5, no.1, pp. 426–430, 2015.

[20] S.A. Kumar, S. Juhi, S. H. Vikram, "DCT- and DWT-Based Intellectual Property Right Protection in Digital Images," In: Bapi, R., Rao, K., Prasad, M. (Eds.) *First Int. Conf. Artif. Intell. Cogn. Comput. Advances Intell. Syst. Comput.*, vol. 815. Springer, Singapore, 2019.

About the Authors

Juhi Singh is Assistant Professor at Amity University, Haryana, India. She is research scholar at Baba Mastnath University, Rohtak, India. She has published more than 30 research articles in reputed journals and presented her research in various conferences, and attended several national and international conferences and workshops.

Dr. Mukesh Singla is a Ph.D. Supervisor and is working as a Professor at Baba Mastnath University, Rohtak, India. He has 18 years of rich teaching and research experience. He has published more than 35 research paper in reputed international journals, and presented papers in more than 15 international conferences. He has edited more than 4 books and has also published 2 patents.