International Journal of Research in Computer & Information Technology (IJRCIT),
Vol.7, Issue 4, Sept 2022
E-ISSN: 2455-3743
Available online at www.ijrcit.co.in

Study of Steganographic Techniques for Data Hiding

[1]Pankaj M. Bhuyar, [2]Dr. S. W. Mohod

Abstract— Nowadays, the volume of data shared over the Internet is growing. As a result, data security is referred to as a major issue while processing data communications through the Internet. During communication procedures, everyone requires their data to remain secure. Steganography is the science and art of embedding audio, message, video, or image into another audio, image, video, or message to conceal it. It is used to secure confidential information from harmful attacks. This research offers a classification of digital steganography based on cover object categories, as well as a classification of steganalysis art. Image visual quality, structural similarity, mean square error, Image Fidelity, embedding capacity, and robustness are some of the important aspects of steganography. Researchers have made tremendous advances in the realm of digital steganography. Nonetheless, it is vital to emphasize the advantages and disadvantages of modern steganography techniques. This paper first presents a literature survey of information hiding, then classifies the proposed methods, and finally introduces a comparative study between the different methods.

Keywords— Steganography, Data Embedding, Steganalysis, Embedding Capacity

I. Introduction

Recently, several methods are developed to protect important information. The developed methods may be classified into two categories: steganography and watermarking. Both steganography and watermarking are data embedding methods. Steganography aims to embedding huge amount of secret data in multimedia carrier such as text, image, audio, and video. On the other hand, watermarking, that may be mainly used for proving copyright, aims to hiding small amount of secret data in multimedia carrier. Although steganography and cryptography have a common goal and are related concepts, the usage and the way of both are somewhat different. Steganography is hiding the message existence completely whereas cryptography is securing the sent message. Steganography's main factors are un-detectability, robustness, and capacity. These factors separate steganography from other related techniques e.g., cryptography and watermarking. Figure 1 presents different branches of information hiding [1]. More details and comparisons are discussed in [1][2]. This paper concerns with steganography-based information hiding. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. In other words, steganography is the process of embedding a file, message, image, or video within another file, message, image, or video. The expression steganography combines the Greek word "stego" which means "cover" and the Greek word "grafia" which means "writing", resulting "covered writing" [3].

Steganography has various useful applications. Secret Communications: secret information can be transmitted without being afraid of alerting danger from potential attackers [4]. Feature Tagging Elements: secret data can be embedded beyond an image, such as names of individuals tagged in a photo some locations in a map [5]. Copyright Protection: Aims to prevent data from being copied [5]. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden [6].

The idea of steganography was first presented in [7] at 1983. Figure 2 presents the scenario of steganography system [8]. Steganography scenario can be summarized in two different phases: encoding (embedding) phase with the help of secret key and decoding (extracting) secret data phase with the manner of preserving information invisible. In the embedding phase, the secret message is embedded in an actual/original multimedia carrier (cover message) by using an embedding algorithm and a secret key. The key is used to aid in encryption and to decide where the information should be hidden in the multimedia carrier. After hiding the secret message, one can call it stego-medium and the key which is used for hiding process is called stego-key. In the extracting phase, the secret message is extracted from the multimedia carrier by using an extracting algorithm and the same secret key.

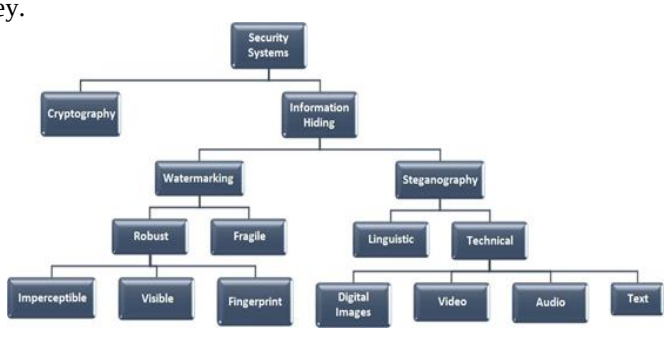

Figure 1: Classification of Data Hiding Methods

Manuscript Received August 5, 2022; Revised 25 August, 2022 and Published on September 20, 2022
Pankaj M. Bhuyar, *Department of Electronics & Telecommunication Engineering, Prof Ram Meghe Institute of Technology & Research Badnera, Amravati, Maharashtra, India. Mail Id: pankajbhuyar@gmail.com*
Dr. S. W. Mohod, *Department of Electronics & Telecommunication Engineering, Prof Ram Meghe Institute of Technology & Research Badnera, Amravati, Maharashtra, India. Mail Id: sharadmohod@rediffmail.com*

DOI: 10.5281/zenodo.7180942

International Journal of Research in Computer & Information Technology (IJRCIT),
Vol.7, Issue 4, Sept 2022
E-ISSN: 2455-3743
Available online at www.ijrcit.co.in

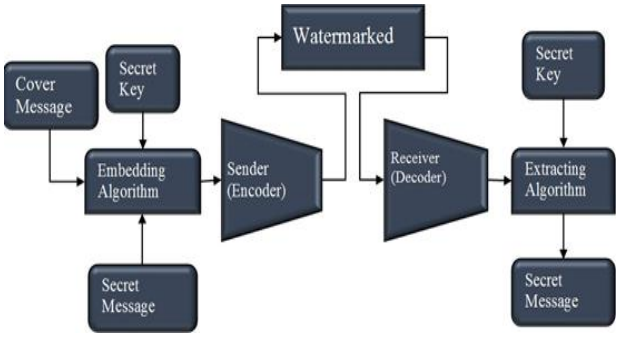

Figure 2: Graphical Version of the Steganographic System

In steganography, the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information hidden and may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image. A possible formula of the process may be represented as:

Cover medium + embedded message + stego key = stego-medium

fE : steganographic function "embedding"
fE-1 : steganographic function "extracting"
cover: cover data in which emb will be hidden
emb: message to be hidden
stego: cover data with the hidden message

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide.

II. IMAGE STEGANOGRAPHY

Image steganography concerns with hiding secret information in digital images. There exists a large variety of image steganography techniques. Some of these techniques are more complex than the others, and all of them have respective strong and weak points. Image steganography techniques can be classified into spatial domain (image domain) steganography, transform domain (frequency domain) steganography, spread spectrum steganography and model based steganography. Figure 3 shows a classification tree of image steganography techniques. The following sections describe the different methods of image steganography.

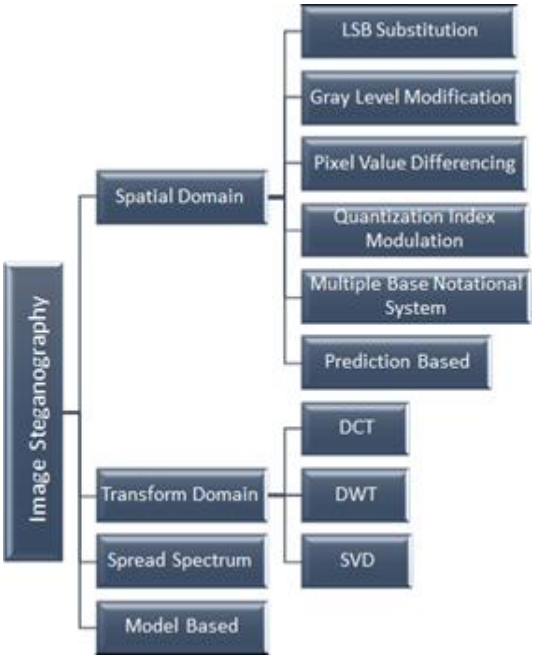

Figure 3: Classification of image steganography techniques [9]

III. SPATIAL DOMAIN METHODS

Image domain applies bit insertion and noise manipulation of a covered image. In spatial domain steganography, embedding the secret message will be done to the pixels directly [10], for example, Least Significant Bit (LSB), gray level modification, pixel value differencing, quantization index modulation, multiple base notational system, and prediction based.

A. Least Significant Bit

LSB is a simple and common method for burying information on cover image [11]. Digital images can be classified as grayscale (8-bit-planes) or colored (24 bit-planes) which depends on each pixel intensity levels, i.e., each pixel can be represented by 24-bits, 8-bits or even only one bit. If every pixel of the digital image is assumed as n bits then the digital image can be composed of n numbers of 1-bit planes in the range from bit-plane zero to bit-plane n-1 [12]. For example, in a gray scale image each pixel is represented by eight bits, so the image can be sliced onto eight slices (bit planes) from bit-plane zero to bit-plane 7. These eight slices are divided onto two parts: Most Significant Bits (MSE) and Least Significant Bits (LSB) [13]. LSB do not hold visually important data, so that is the perfect environment for embedding watermark bits. In this method, the process of embedding depends on choosing a subset of cover image and applying the substitution operation on them. That exchanges the LSB of cover image by the watermark [14]. The LSB method is characterized by simplicity, high capacity, easy to

International Journal of Research in Computer & Information Technology (IJRCIT),
Vol.7, Issue 4, Sept 2022
E-ISSN: 2455-3743
Available online at www.ijrcit.co.in

understand and implement, and can't be noticed by the naked eye [15]. However, the drawbacks of this methods are that lacks robustness (Easy manipulation by attackers), susceptible to noise, scaling and cropping.

B. Image Downgrading and Covert Channels

Image downgrading is considered as substitution system where images act as both covers and secret messages. This case had been discussed in [16], where the authors had fears about security threats which face operating systems with high-security which is called image downgrading because it could help on exchanging images secretly.

The main idea of image downgrading depends on making the cover-image and the secret image equal in dimensions. Then, the sender exchanges the four least significant bits values of the cover image (grayscale or color) with the four most significant bits of the chosen secret image. In extraction, the receiver extracts the four least significant bits out of the watermarked image, and then it gets to the most significant bits of the secret image. In many cases, the degradation of the cover image is not noticeable by naked eye, as four bits are enough for transmitting rough approximation of the secret image. In the multilevel security systems, like the system used by the army, sometimes it is necessary to declassify the form of some information. For example, if they want to change it from 'top secret' onto 'confidential'' or from 'confidential' onto 'public' or even from 'top secret' to 'public'. This is not easy specially if they need to downgrade images [17].

C. Gray Level Modification

In 2004, Potdar et al. [18] discussed a technique based on a mathematical function. This technique maps data by altering gray levels of the pixels without embedding or hiding it and uses the conception of even and odd numbers in mapping the data in the cover image. For example, even values are mapped with zero and odd values are mapped with one. The gray level modification method is characterized by low computational complexity and high capacity.

D. Pixel Value Differencing

In 2003, Da-Chun et al. [19] developed a new embedding method, called Pixel Value Differencing (PVD), based on the difference between pixel values.

IV. TRANSFORM DOMAIN TECHNIQUES

Transform Domain applies image transformation and manipulation of algorithm. In transform domain steganography, embedding the secret requires transforming the image from the spatial domain to the frequency domain by using any of the transforms, for example, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Single Value Decomposition (SVD). After the transformation process, the embedding process will be done in proper transform coefficients.

A. Discrete Cosine Transformation

Discrete Cosine Transform (DCT) is based on transforming signal or image from spatial domain to frequency domain. The DCT split the image as shown in figure 4 up to spectral sub-bands (parts) of different significance with respect to the visual quality of the image [29]. Embedding positions Choices: (i) Low- frequency coefficients: Bad invisibility, because human eye is sensitive to noise on it, as it contains the image visual parts, (ii) High-frequency coefficients: bad robustness, as the image could be corrupted through noise attacks or compression, and (iii) Middle-frequency coefficients: good invisibility and robustness, so it is the best choice.

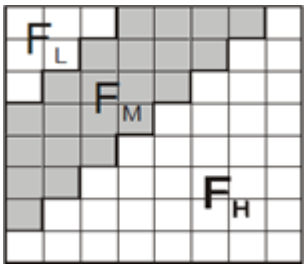

Figure 4: Discrete Cosine Transform

B. Discrete Wavelet Transformation

Wavelet transform is used in a wide range in signal processing applications and image compression. It separates the signal to set of basic functions which are called wavelets. Discrete Wavelet Transform (DWT) is described as an efficient and very flexible method for decomposing signals sub bands. In recent years, JPEG committee releases a new standard of image coding is called 'JPEG-2000' which is based on DWT [34].

DWT is used in a wide range in signal processing applications for example audio, video and image compression. In case of one-dimensional DWT, image is decomposed into 4 bands denoted by Low-Low (LL) level, High-Low (HL) level, Low-High (LH) level and High-High (HH) level [35], as shown in Figure 5. Where, H symbolizes high-pass filter (High frequency) and L symbolizes low-pass filter (Low frequency).

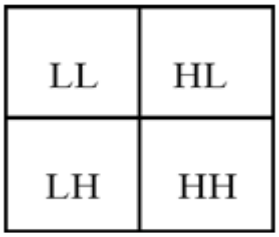

Figure 5: Discrete Wavelet Transform (DWT)

DOI: 10.5281/zenodo.7180942

International Journal of Research in Computer & Information Technology (IJRCIT),
Vol.7, Issue 4, Sept 2022
E-ISSN: 2455-3743
Available online at www.ijrcit.co.in

C. Singular Value Decomposition

Singular Value Decomposition (SVD) is a mathematical technique based on a linear algebra theorem which declares that the rectangular matrix (A) can be analyzed into three matrices [40]: U (Orthogonal matrix), S (Diagonal matrix), and V (Transpose of an orthogonal matrix). The theorem is presented usually like: $A = USV^T$

D. Spread Spectrum

In this technique secret data is spread over wide frequency bandwidth. This technique provides very good robustness. If signal to noise ratio in every frequency band is small then it is difficult to detect presence of secret data. “Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data” [9].

V. Research Issue

Image steganography faces the major problem of hiding secret bits in the cover image with minimum detectability, high security, robustness against alteration/interception, and high payload. Despite the research effort in this domain for some time now, it is still a problem to achieve the above-listed requirements. A major issue is relatedness between these attributes as the mutual relationship between steganographic properties entails that while enhancing some properties, others are adversely affected. This issue persists due to the lack of a practical solution to achieve these properties at once. Some of the proposed methods for improving the performance of the existing steganographic methods are given below:

A. Hybrid steganographic techniques

The combination of several steganographic methods into one method may improve data security and confuse specific steganalysis methods as the strengths of the combined methods will be exploited to address their weaknesses during the design of the hybrid method [22].

B. Merging of cryptography with steganography

This could add a layer of security to secret data as they will be encrypted first before embedding. An attacker may intercept the steganographic algorithm but will still have to contend with the cryptographic scheme to be able to recover the encrypted data.

C. Secured lightweight encryption-based steganographic techniques

As most of the existing steganographic techniques are prone to modern steganalysis, coupled with the high cost of secret data protection using the conventional encryption method, it has become necessary to design a lightweight encryption method that can protect secret data in a cost-efficient manner [27].

D. Additive noise distortion function reduction

This is another way of protecting the existing steganographic techniques from steganalysis. Most of the modern steganalysis methods deploy the method of computing the specific features of the cover and stego-images to determine their types. These distinctive features are mostly generated by additive noise in stego-images. Hence, there is a need to devise ways of minimizing this additive when designing new steganographic methods.

E. Merging of reversible and irreversible methods

This may improve payload and secret data security. Different reversible and non-reversible methods can recursively employ the same pixels at the same time, making it hard for the attacker to extract the secret data [12].

F. Location sensitive embedding

This is also called adaptive steganography; it has evolved recently as a way of improving payload, reducing distortion, and making a dynamic decision on special data during steganographic processes. However, this type of steganography needs more time to mature in the face of modern steganalysis [4].

Conclusion

In this paper, a literature survey of digital image steganography information hiding techniques is presented. first, a classification of watermarking algorithms based on embedding domain is shown. These domains are spatial domain, transform domain. All these algorithms try to satisfy three most important factors of steganographic design i.e. un-detectability, robustness, and capacity. then, some hybrid techniques are discussed. Finally, a comparative study between the different methods is introduced. It is clearly observed that the embedding procedure is easy in spatial domain techniques compared to complex transform domain techniques. Also, Spatial domain techniques are simple and have high stego visual quality, but transform domain techniques are more robust and less exposure to image processing attacks. From the paper, it can be concluded that every technique has advantages and disadvantages if compared with other techniques of steganography. Which mean that it is not fair to call any method 'the best or the worst of all'. So, determining the suitable method is chosen based on the wanted purpose.

References

[1] Random, Steganography Scheme Using Two. "An Effective and Secure Digital image Steganography Scheme using Two Random Function and Chaotic Map." Journal of Theoretical and Applied Information Technology 98.01 (2020).

[2] ALRikabi, Haider TH, and Hussein Tuama Hazim. "Enhanced Data Security of Communication System Using Combined Encryption and

Steganography." International Journal of Interactive Mobile Technologies 15.16 (2021).

[3] Dhawan, Sachin, and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." Information Security Journal: A Global Perspective 30.2 (2021): 63- 87.

[4] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trendsin future research. Neurocomputing, 335, 299-326.

[5] Yang, Peng, Yingjie Lao, and Ping Li. "Robust Watermarking for Deep Neural Networks via Bi-Level Optimization." Proceedings of the IEEE/CVF International Conference on Computer Vision. 2021.

[6] Pirandola, Stefano, et al. "Advances in quantum cryptography." Advances in Optics and Photonics 12.4 (2020): 1012-1236.

[7] Saini, Ravi, Kamaldeep Joshi, and Rainu Nandal. "An Adapted Approach of Image Steganography Using Pixel Mutation and Bit Augmentation." Smart Computing Techniques and Applications. Springer, Singapore, 2021. 217-224.

[8] Mushenko, Alexey, Alexander Zolkin, and Aleksandr Yatsumira. "Steganography Analysis of Chaotic Carrier Signal Transmission with Non-linear Parametric Modulation." 2021 International Russian Automation Conference (RusAutoCon). IEEE, 2021.

[9] Alsaawy, Yazed, et al. "Double Steganography- New Algorithm for More Security." 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2021.

[10] Taha, Mustafa Sabah, et al. "A Steganography Embedding Method Based on P single/P double and Huffman Coding." 2021 3rd International Cyber Resilience Conference (CRC). IEEE, 2021.

[11] Al-Halabi, Yahia Sabri. "A Symmetric Key Based Steganography Calculation For Anchored Information." Journal of Theoretical and Applied Information Technology 98.01 (2020).

[12] Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66.

[13] Taha, Mustafa Sabah, et al. "Information Hiding: A Tools for Securing Biometric Information." Technology Reports of Kansai University 62.04 (2020): 1383-1394.

[14] Wahab, Osama Fouad Abdel, et al. "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques." IEEE Access 9 (2021): 31805- 31815.

[15] ALRikabi, H. T., & Hazim, H. T. (2021). Enhanced Data Security of Communication System Using Combined Encryption and Steganography. International Journal of Interactive Mobile Technologies, 15(16).

[16] AbdelWahab, Osama F., et al. "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data." Procedia Computer Science 182 (2021): 5-12.

[17] Al-Nofaie, Safia, Adnan Gutub, and Manal Al- Ghamdi. "Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces." Journal of King Saud University- Computer and Information Sciences (2019).

[18] Al-Nofaie, Safia Meteb, Manal Mohammed Fattani, and Adnan Gutub. "Merging two steganography techniques adjusted to improve arabic text data security." Journal of Computer Science & Computational Mathematics (JCSCM) 6.3 (2016): 59-65.

[19] Ala'a, M., and Odeh Alnihoud. "AMeliorated Kashida-Based Approach For Arabic Text Steganography." Int. J. Comput. Sci. Inf. Technol.(IJCSIT) 9.2 (2017).

[20] Abbasi, Aliya Tabassum, et al. "Urdu text steganography: Utilizing isolated letters." Australian Information Security Management Conference. Australia (2015).

[21] Yang, Yang, Weiming Zhang, and Nenghai Yu. "Improving visual quality of reversible data hiding in medical image with texture area contrast enhancement." 2015 international conference on intelligent information hiding and multimedia signal processing (IIH-MSP). IEEE, 2015.

[22] Punidha, R. "Integer wavelet transform based approach for high robustness of audio signal transmission." International Journal of Pure and Applied Mathematics 116.23 (2017): 295- 304.

[23] Vardhan, M. Vishnu, B. Rama Krishna, and V. Thanikaiselvan. "IWT Based Data Hiding in Encrypted Images." 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2018.

[24] Yin, Bangxu, et al. "Separable reversible data hiding in encrypted image with classification permutation." 2017 IEEE Third International Conference on Multimedia Big Data (BigMM). IEEE, 2017.

[25] Manikandan, Vazhora Malayil, and Vedhanayagam Masilamani. "An improved reversible data hiding scheme through novel encryption." 2019 Conference on Next Generation Computing Applications (NextComp). IEEE, 2019.

[26] Dhande, Krutika, and Rutuja Channe. "A Brief Review on Reversible Data Hiding in Encrypted Image." 2019 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2019.

[27] Marella, Pranay, Jeremy Straub, and Benjamin Bernard. "Development of a Facial Feature Based Image Steganography Technology." 2019 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2019.

[28] Benedict, Arnold Gabriel. "Improved file security system using multiple image steganography." 2019 International Conference on Data Science and Communication (IconDSC). IEEE, 2019

[29] Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. "An image steganography approach based on k-least significant bits (k-LSB)." 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.

[30] Rafiqi, Abdul Yabar. "Features Analysis and Extraction Techniques for the Image Steganography." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.8 (2021): 2103-2109.

[31] Indrayani, Rini, Hanung Adi Nugroho, and Risanuri Hidayat. "An evaluation of MP3 steganography based on modified LSB method." 2017 International Conference on Information Technology Systems and Innovation (ICITSI). IEEE, 2017.

[32] Datta, Biswajita, Prithwish Kumar Pal, and Samir Kumar Bandyopadhyay. "Multi-bit data hiding in randomly chosen LSB layers of an audio." 2016 International Conference on Information Technology (ICIT). IEEE, 2016.

[33] Al-Bayati, Marwa Tariq, and Mudhafar M. Al- Jarrah. "DuoHide: A Secure System for Hiding Multimedia Files in Dual Cover Images." 2016 9th International Conference on Developments in eSystems Engineering (DeSE). IEEE, 2016.

[34] Sharma, Vipul, and Ravinder Thakur. "LSB modification based audio steganography using trusted third party key indexing method." 2015 Third International Conference On Image Information Processing (ICIIP). IEEE, 2015.

[35] Abdelsatir, El-Tigani B., Narayan C. Debnath, and Hisham Abushama. "A multilayered scheme for transparent audio data hiding." 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2015.