IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study On Secured Communication Using Steganographic Methods With A Special Emphasis On Image Steganography: A Review

Chethana N S [1*], Anitha Devi M D[2*]

[1*]Research Scholar, Sri Siddhartha Academy of Higher Education, Agalakote,Tumkur,Karnataka, India

[2*]Associate Professor, Department of Electronics and Communication Engineering, SSIT Tumkur

Abstract

Steganography is one of the techniques preferred for hiding secret messages. It is a method of hiding information or data within other data to conceal its existence. This research article explores the study of different methods and challenges associated with existing steganographic techniques to achieve secured communication. The various models of steganography, includes image-based steganography, audio steganography, and text-based steganography. Evaluation of most popular techniques and reviewed the performance analysis of image steganography is done in this work. So that we can understand the complexities and limitations that can be carefully considered in choosing the steganography technique for specific communication.

Key Words: Steganography, Secured Communication, Image-Based Steganography, Audio Steganography, Text-Based Steganography, Encryption, Data Security

1. INTRODUCTION

Digitization is common now a days in many fields. Safety, Security and Confidentiality are the features to be considered in good communication. The need for secure communication has become increasingly critical in todays digital era. Traditional cryptographic methods like encryption play a vital role in securing data during transmission. However, steganography offers a complementary approach to conceal sensitive information within carrier data, adding an extra layer of security to communication protocols. This article aims to provide a study of the methods and challenges associated with secured communication using steganography.

Cryptography and Steganography are the two primary ways for safeguarding, concealing and transmitting messages. without the safety of data, others can obtain secret information which might cause serious harm. Steganography is method of hiding confidential messages or data in non confidential objects. Historically people were using tattoos or invisible ink to convey steganographic information. The word steganography comes from Greek word meaning secret writing and is usually analysed to embed sensitive information in other covert form, plenty of research has been done to unveil different covert communication methods and its challenges. Steganography is an art and science of hiding secret data behind the cover medium. In new generation of computers, steganography is considered a sub branch of data communicating security. Hence new ways based on steganographic methods are emerging. Concealed medium can be any multimedia content like digital images, audios files or video files. Applying steganography into communication protocols, security measures can be enhanced, ensuring that

sensitive information remains confidential during transmission [1]. Attempts should be made to enhance the capacity of data lodging and keep up covertness. In this procedure, the covert text file can be accommodated to the size of the image. We can endeavour strategic procedures to backstair text files with larger size than image size. The private keys have to be illustrious to sender and receiver. Keys will be dispensed separately but weren't not shipped in cover images. A blueprint can be developed to generate and distribute the keys secretly [2]. New approaches in steganographic methods are being proposed by several researchers and new steganalysis processes are also found. Hence, research to create inured steganographic and steganalysis technique is a nonstop activity [3]. In this paper an insight is being done into vibrant covert communication methods and challenges associated with them to examine the merits and demerits of these techniques to assure safe communication. Various covert communications discussed in this paper include different types.

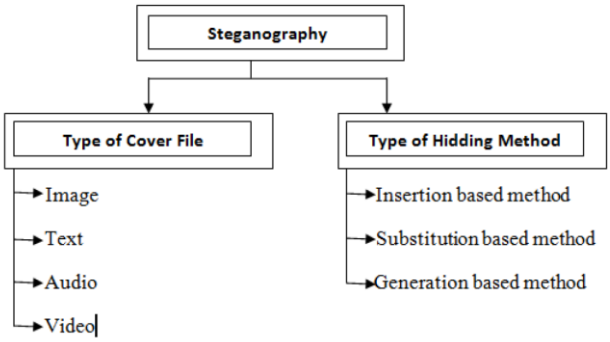

Figure 1: Different Types of Steganography

1. Image stegnography
2. Text stegnography
3. Audio stegnography
4. Video stegnography
5. Insertion based method
6. Substitution method
7. Generation based method

1. Image-Based Steganography: This model focuses on hiding information within digital images. It involves imperceptibly altering the pixels of an image to encode a hidden message. Techniques like Least Significant Bit (LSB) insertion and masking are commonly used in image-based steganography. The altered image can then be transmitted and the hidden message extracted by the intended recipient using appropriate decoding techniques.

2. Text-Based Steganography: Text-based steganography conceals secret messages within seemingly innocuous text. Techniques such as modifying whitespace characters, altering word or letter frequencies, or employing special encoding schemes can be used to embed information within plain text. This model offers a discreet way to transfer sensitive data through written or digital communication channels.

3. Audio Steganography is the term used to describe the process of using audio as a carrier for the purpose of concealing information. It has become a highly major media as a result of the popularity of voice over internet protocol (VOIP). For the purpose of steganography, digital audio formats like MPEG, WAVE, AVI, MIDI, and others are utilized for audio steganography. The audio steganography techniques that are most frequently utilized are as follows: Parity coding, Spread coding, LSB coding, Phase coding and Echo concealment method. ICMP, IP, UDP or TCP are some of the network protocols are used in network protocol Steganography.

4.Video Steganography: Steganography as it pertains to video is a method that may be utilized to conceal some kind of documents or information within a digital video format. Hidden information is transmitted through the medium of video, which is a blend of still images. In general, discrete cosine

transforms (DCT) are used to change values (for example, from 5.668 to 6), [4] which are then utilized to conceal information in every images in the movie that is invisible to naked eye. A variety of video codecs, including AVI H.264, MPEG and MP4 are utilized in video steganography.

5.The Insertion-Based Steganography: This is a technique that involves locating specific regions inside cover files that are typically disregarded by apps that read the cover file. Subsequently, the covert data is embedded within these specified regions. Owing the fact that this method incorporates the concealment data into the cover file. It is expected that the stego file size will be more than the cover file size. Because this method is dependent on the accumulation or addition of the secret data to the cover file. Cover file contents should not be altered after the embedding because, the cover file already contains the secret data.

6. The Substitution-Based Steganography: This method differs from insertion-based method by ways that it will not include secret data in cover file. This method is dependent on locating certain irrelevant information in the cover file. Later, this irrelevant data will be replaced by the secret data. As a result, some of the cover data is only updated or replaced without adding more data. Hence, the cover file quality, may suffer after the embedding procedure has been completed. Additionally, the extent of the secret data that may be concealed is limited due to the limited number of irrelevant information that is contained within the cover file.

7. Generation-Based Method: This method does not require a cover file in contrast to the two methods described above. Here, Appropriate stego files is generated by utilizing secret data. cover files and stego files are compared to detect steganography. The fact that only stego files are accessible and cover files are not utilized is one of the reasons why generation-based steganography is advantageous. This is because it eliminates the possibility of detection of this kind. The fact that this approach can only generate a limited number of stego files is the most significant drawback it has. Furthermore, the created stego files may be files that end users find to be unrealistic (for example, a picture may contain a variety of forms and colors that make no sense, or a word may contain no meaning at all). As a result, the primary media for such a technique are images that appear to be random and English text file. Another Latest method apart from the above list is **Steganography of a network protocol** is employed when the protocol is utilized as a carrier. Covert channels are available in the OSI network layer architecture, and they allow for the implementation of steganography in the header bits of TCP/IP fields that are not being used. Regardless of the sort of cover that is being utilized to conceal the data. One way to categorize steganography is according to the approach that is utilized to conceal confidential information. Therefore, there are three different techniques to conceal confidential information within cover files.

By employing these steganographic techniques, secure communication can be achieved without drawing attention to the existence of the hidden information. When combined with encryption and other security measures,

steganography enhances the confidentiality and integrity of transmitted data, making it a valuable component in information security protocols.

Image steganography algorithms:

Image steganography algorithms include Spatial domain and Transform domain.

Spatial domain: this method involves selection of bits from the cover picture and substituting them by the secret data.

Spatial domain steganography techniques: 1) LSB based approach (Least Significant Bit) 2) PVD based system (Pixel Value differencing) 3) EMD based system (Exploiting Modification Direction) based approaches.

Transform domain steganography techniques: 1) Discrete Wavelet Transform (DWT) 2) Discrete Cosine Transformation (DCT) 3) Contourlet Transform 4) Wavelet Transform and 5) Fourier Transform

Performance is reviewed in terms of Embedding capacity, Robustness, Security and PSNR.

Embedding capacity: It is the quantity of information that may be hidden inside a cover picture.

Robustness: It is the ability of recovering stego original image's confidential information when subjected to transformations.

Security: It refers to safeguard the data while maintaining the user's privacy by preventing unwanted access.

PSNR: it is used to determine efficiency of techniques for concealing one picture inside another. It is a metric that quantifies the noise ratio between the stego picture and the original image.

2. AVAILABLE STATE OF THE ART LITERATURE:

2.1 Steganography in Spatial Domain:

The study by MamtaJuneja et al., [4] presents a secure and strong approach to data security. This proposal introduces two component-based methods for embedding LSB (Least Significant Bit). Secret information will be hidden within the least significant bits of blue pixels and some of the green pixels placed at the peripheries of image. They also proposed an adaptive LSB-based steganography technique incorporating data from the MSB's of red, green, and blue components Selected pixels scattered throughout even surfaces. It is stronger because of its integration with an Advanced Encryption Standard (AES).

Thiyagarajan et.al.,[5] introduced a Steganographic scheme with high-capacity by using 3D geometric model. This procedure re-triangulates a section of triangular mesh. It incorporates confidential data into the triangular mesh which is recently inserted location. This algorithm opposes uniform affine transformations like scaling, cropping and rotation. The stego key is derived from the data intended for embedding. The triangle's vertices are utilized for incorporating.

Shamim Ahmed Laskar et.al's [6] approach involves embedding data into the red plane of the image. A random number generator is used to select the pixel. It's nearly undetectable modifications to image. Utilizing a stego key to initialize the Pseudo Random Number using a Generator (PRNG) to choose location of pixel. This paper delves into enhancing the message security and minimizing the distortion rate.

S.Shanmuga Priya et al., [7] in their article, introduced a new LSB based method. Information concealing is done by using a unit pixels pair, with least significant bit of the first pixel. A small data with a function map two-pixel values to other piece of data. The method demonstrates superior performance with respect to resistance and distortion.

B.Sharmila et. al., [8], the authors present an algorithm that operates on colour picture files in JPEG format. Edges will be selected to hide secret data which increases robustness capability. Sharper edges exhibit many regions with complex statistical features and relay highly on the contents of the image. Observing changes at sharper edges is more challenging compared to smooth surfaces. During embedding process, components of RGB are separated and they are influenced by a common secret data to enhance the quality of the image. Security is assured by a specific stego key.

2.2 Steganography in Transform Domain:

Hemalatha.S et.al's paper [9] introduces a method that utilizes two grayscale images sized 128 × 128 as secret images. These images are embedding them in YCbCr and RGB domains. The steganographic image quality is high in RGB domain when refer to PSNR values. The authors utilized IWT (Integer Wavelet Transform) to conceal stego images within the colour cover image. Authors also examined values of PSNR and quality of image concealed in the YCbCr and RGB domains.

Hemalatha.S et.al.,[10] proposed using IWT (Integer Wavelet Transform) for concealing numerous stego images and keys under colour cover image for more effect. The envelop image is depicted in color system of YCbCr. Two stego keys are acquired, coded, and concealed within the cover image using Integer Wavelet Transform.

Keith L. Haynes' paper [11] examines the utilization of image steganographic technique to infiltrate an organization's cyber and physical defences. The technique uses machine learning and computer vision to generate undetected messages which can't be deciphered unless the stego key is compromised. DWT (Discrete Wavelet Transform) is utilized to prevent detection. A computer vision system aims at enable machines to determine and evaluate information within an image. Different classifications of Computer vision are Model-based and Appearance-based approaches, which utilize sample images and machine learning methods for recognizing crucial regions or features in images which are essential for distinguishing entities or objects in an image. Computer must determine the presence of a face by analyzing the values within 2D matrix. Haar feature selection method is used to detect the image feature. The objective is to determine group of attributes which differentiates different photos of various classifications most effectively. In this method, the cover image does not conceal the secret message. Instead, concealed information is revealed through the image's classification. The system uses regular, unaltered photos, thus there are no built-in signs of hidden.

In the work that was done by S.Arivazhagan and colleagues [12], they offer a method which operates in the transform domain and makes an effort to retrieve the secret in a manner that is practically identical to the one that is embedded. This is accomplished by utilizing techniques such as median maintenance, offset, and quantization. In order to circumvent the constraints that are associated with embedding, an improved method for shielding color images inside color images has been developed. Increasing the robustness of the secret image is accomplished by applying a transform to it. After that, the altered image is divided into three color planes, viz R, G, and B. Each of these color planes is then exposed to discrete wavelet transform (DWT) independently, reformed in to bit stream. Finally, it is integrated to be included within the cover image.

The authors of the study [13] by Anindya Sarkar and colleagues present a ME-RA (Matrix Embedding with Repeat Accumulate) based steganography. Here, the host coefficients are altered minimally in a way that the sent bits lie inside a coset of a linear code, and the pattern is responsible for communicating the hidden bits. Pseudo-random selection is used to select the hidden blocks. When it comes to error repair, a powerful repeat accumulate code is often utilized. Both the Quantization Index Modulation (QIM) and the ME-RA approaches have been taken into consideration by the writers. There is also a tabulation of the comparisons that were made with little alterations of the MERA (non-shrinkage and puncture) procedures along with other decoding methods. They emphasize the utilization of matrix embedding rather than QIM in the Yet Another Steganographic Scheme results in enhanced steganographic analysis performance; however, the complexity of the software is increased.

A appropriate encryption methodology that uses a symmetric key cryptographic algorithm which is presented by authors of the paper [14] written by Prosanta Gope and colleagues. Additionally, the authors present an improved JPEG steganography. The JPEG cover image is divided into pixel blocks that are 8 by 8 pixels in size. A new encryption approach that makes use of CRC checking is utilized, and DCT is used to every block. Quantization is also performed and the encryption of data is done by using this novel method.

M.D Anitha Devi et.al.,[19] proposed a new image steganography method for online transaction securely using discrete wavelet transformation along with visual cryptography proposed by and K B ShivaKumar [19] These authors have proved that better PSNR and MSE values were obtained using DWT and visual cryptography combination than using only DCT. MSE and PSNR are the parameters used to determine the effectiveness. This procedure provides very minimal information required for online shopping and it also provides maximal security to customer's information. Hence increase the security during online transactions.

2.3 Steganography using Statistical Method:

Tomas Filler et. al.'s study [16] presents a practical procedure using a normal embedding operation that offers greater flexibility and simplicity for reduction of additive distortion in steganography. Enhancing system security is the primary goal of Syndrome-Trellis Codes (STC). STC categorizes the samples into various bins, a widely used technique for addressing information-theoretic and data-hiding challenges. This method is applicable in both spatial and transform domains. Choosing an appropriate distortion function can complicate statistical detection. After the distortion function is specified by the stenographer, the framework offers all the necessary tools to create practical concealing schemes. The the embedding operations or distortion function need not have to known for recipient.

Jessica Fridrich et.al.,[17] proposed a scheme using reversible embedding for VQ-compressed images based on side matching and relocation in their research paper. This new procedure achieves reversibility by not relying on location map. though a slight alteration of the original content is not suitable for certain crucial applications like medical, military data. Hence, significance of reversible steganography techniques is important. Vector Quantization (VQ) has gained popularity due to its straight forward encoding and decoding processes. In order to enhance imperceptibility, the codebook is divided into multiple clusters before embedding data. The required input includes a VQ compressed image, multiple hit maps, a sequence of secret bits, clusters of the super codebook SC, and a super codebook SC. The outcome will be a VQ stego image. When X matches the ith code word of Go, the embedding process is triggered. When X equals the ith code word of G1, embedding a secret bit is not possible and a compensation procedure must be implemented to prevent conflicts with case 1. If X is not a member of

G0 U G1, then no secret bit can be embedded, and X will be skipped. Secret information can only be embedded in case 1.

The article by Chin-Chen Chang et.al., [15] introduces a novel method using random linear codes of small co-dimension for wet paper codes to increase the efficiency. To prevent attacks, it is important to ensure that the selection channel is not accessible to the public in any way. One potential solution is based on additional data that the attacker does not have access to, such as randomness or information that is difficult to estimate from the stego image. Utilizing steganography techniques that do not involve shared selection channels involves utilizing memory codes containing defective cells, which are also known as wet paper codes. This article introduces a novel steganographic tool, an encoding method that allows the steganographer to utilize various selection channels and reduce the number of embedding changes significantly. This method integrates wet paper codes with matrix embedding, allowing for arbitrary selection channels and enhanced efficiency of embedding through the use of random linear codes with small co-dimension.

The authors in Zhicheng Ni et.al.'s article [18] introduce a lossless data hiding method which will be resistant to JPEG / JPEG 2000 compression. The image is divided into 8 x 8 blocks, with each block further divided into two subsets (A, B). Calculating the value of difference for each block involves finding the arithmetic average of differences of pixel pairs within the block. This quantity is chosen for embedding the information bit due to its robustness. Every fragment of the confidential message corresponds to a set of pixels. When a pixel is within a certain range, to encode a specific bit, adjust the pixel value by adding or subtracting a fixed number within a subset. When embedding 0, the block remains intact. When the value is outside the threshold, it is recommended to embed 1 to shift the value beyond the threshold. Next, error correction code is implemented.

3. CONCLUSIONS AND POSSIBLE FUTURE WORK:

Recent trends in secret communication through steganography reveal a dynamic landscape marked by advancements in both techniques and applications. Steganography, the art of concealing messages within seemingly innocuous cover media, has seen notable developments driven by the increasing need for covert communication in various fields, including cyber security, intelligence, and privacy preservation.

One prominent trend is the integration of steganography with emerging technologies such as deep learning and artificial intelligence. These advancements have led to more sophisticated algorithms capable of embedding and extracting hidden information with greater efficiency and resilience against detection. Moreover, the adoption of steganographic techniques in multimedia formats like images, audio, and video continues to expand, offering diverse channels for covert communication.

Additionally, there has been a growing emphasis on robustness and security in steganographic systems. Researchers are exploring novel approaches to enhance the imperceptibility of hidden data while minimizing the risk of detection by adversaries. This includes techniques like adaptive embedding, which adjusts the hiding strategy based on the characteristics of the cover media, and cryptographic enhancements to assure the privacy and integrity of hidden messages. Furthermore, the proliferation of digital platforms and communication channels has fuelled the demand for steganography as a means of privacy protection. Individuals and organizations are increasingly leveraging steganographic tools to safeguard sensitive information during transmission and storage, particularly in contexts where traditional encryption methods may attract unwanted attention or suspicion.

Despite these advancements, challenges persist in the field of steganography, including the ongoing arms race between concealment techniques and detection methods. As adversaries develop more sophisticated detection algorithms, steganographic systems must continually evolve to maintain their effectiveness and reliability.

In conclusion, recent trends in secret communication using steganography reflect a dynamic interplay between technological innovation, security requirements, and practical applications. While the field continues to advance, the pursuit of robust, efficient, and undetectable steganographic solutions remains a central focus, driven by the imperative to secure sensitive information in an increasingly digital and interconnected world.

REFERENCE:

[1] Fabien A.P.Petitcolas, Ross J.Anderson and Markus G.Kuhn, (2023) "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078. (PAPER1)

[2] R. Suryawanshi, Suresh N. (2018) "Analysis of Effect of Spatial Domain Steganography Technique on DCT Domain" international Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, pp. 634-640

[3] Gunjan, Er. Madan Lal (2016) "Investigation of Various Image Steganography Techniques in Spatial Domain" Volume 3, Issue 6, June-2016, pp. 347-351 ISSN (O): 2349-7084 International Journal of Computer Engineering In Research Trends (MADAM)

[4] MamtaJuneja and Parvinder Singh Sandhu (2023) "A New Approach for Information security usingan Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.

[5] P.Thiyagarajan, V.Natarajan, G.Aghila, V.PrannaVenkatesan, R.Anitha, (2013) "Pattern Based 3DImage Steganography", 3D Research center, Kwangwoon University and Springer 2013, 3DRExpress., pp.1-8.

[6] Shamim Ahmed Laskar and Kattamanchi Hemachandran, (2022) "Steganography Based OnRandom Pixel Selection For Efficient Data Hiding", International Journal of Computer Engineeringand Technology, Vol.4, Issue 2, pp.31-44.

[7] S.ShanmugaPriya, K.Mahesh and Dr.K.Kuppusamy, (2020) "Efficient Steganography Method toImplement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.

[8] B. Sharmila and R.Shanthakumari, (2021) "Efficient Adaptive Steganography For Colour Images Based on LSBMR Algorithm", ICTACT Journal on Image and Video Processing, Vol. 2, Issue:03,pp.387-392.

[9] Hemalatha.S, U.Dinesh Acharya and Renuka.A, (2013) "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains", International Journal of Advanced Information Technology, Vol.3, No.3, pp.1-9.

[10] Hemalatha.S, U.Dinesh Acharya and Renuka.A, Priya R Kamnath, (2013) "A Secure and High Capacity Image Steganography Technique", Signal & Image Processing – An International Journal,Vol.4, No.1, pp.83-89.

[11] Keith L.Haynes, (2021) "Using Image Steganography to Establish Covert Communication Channels", International Journal of Computer Science and Information Security, Vol 9, No.9, pp. 1-7.

[12] S.Arivazhagan, W.Sylvia Lilly Jebarani, and S.Bagavath (2011) "Colour Image Steganography Using Median Maintenance", ICTACT Journal on Image and Video Processing, Vol. 2, Iss:01,pp.246-253.

[13] Anindya Sarkar, B.S.Manjunath (2010) "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography", IEEE Transactions on Information Forensics and Security,Vol.5.No.2, pp.225-239.

[14] Prosanta Gope, Anil Kumar and Gaurav Luthra, (2010) "An Enhanced JPEG Steganography Scheme with Encryption Technique", International Journal of Computer and Electrical Engineering, Vol.2.No.5, pp924-930.

[15]Chin Chen Chang, Piyu Tsai & Min-Hui Lin (2004) "An Adaptive Steganography for Index-Based Images using Codeword Grouping", Springer-Verlag Berlin Heidelberg 2004, pp.731- 738.

[16] Tomas Filler, Jan Judas (2010)"Minimizing Additive Distortion in Steganography using Syndrome Trellis Codes", IEEE Article,pp.1-17.

[17] Jessica Fridrich, Miroslav Goljan, David Soukal (2006) "Wet Paper Codes With Improved Embedding Efficiency ", IEEE Transactions on Information Forensics and Security, Vol 1. No.1, pp102-110.

[18] Zhicheng Ni, Yun Q.Shi, Nirwan Ansari, Wei Su, Qibin Sun & Xiao Lin (2004) "Robust Lossless Image Data Hiding", IEEE Article.

[19] M.D Anitha Devi, K B ShivaKumar (2017) "A Novel Image Steganography Technique for Secured Online Transaction Using DWT and Visual Cryptography" article: 2017 IOP Conf. Ser.: Mater. Sci. Eng. 225