



A SECURE DATA TRANSFER OVER INTERNET USING STEGANOGRAPHY

¹Tejashwini K, ²Dr Jithendra, ³Prof. Rakesh Sharma

¹PG Student, ²PG coordinator, ³Associate Professor of CSE Dept.

¹Department of Computer Science and Engineering,

¹Srinivas Institute of Technology, Valachil, Mangalore, India

Abstract: In Today's world Sensitive data is increasingly used in communication over the internet. Thus, Security of data is the biggest concern of internet users. Best solution is use of some Steganography algorithm which encrypts data in Images it over the internet and again decrypted to original data. Secure information transmission is the focus of the fields of cryptography and steganography. Allowing the intended recipients to correctly receive a message while preventing eavesdroppers from comprehending it is the aim. IT comprises a collection of methods for jumbling or hiding data so that only the person who can transform it back into its original form may access it. In modern computer systems, steganography offers a solid, cost-effective foundation for maintaining data confidentiality and confirming data integrity. Thus, to address many of the issues with traditional cryptography, lightweight steganography techniques are suggested. This project sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new way of encryption of plaintext as a message into Images.

Index Terms- Steganography, Secure Communication, Data Hiding, LSB, Digital Image Security

I. INTRODUCTION

Information security can be summed up to info, a group of steps, procedures, and strategies that are used to stop and observe illegal access, trouble- shooting, revelation, and adjustment of computer network sources. It takes a lot of work to increase the privacy, eligibility, and reliability of the work by strengthening the existing techniques by ongoing tries to break them and creating new methods that are resistant to most, if not all, types of assaults. As the number of internet users continues to rise, more complicated issues have emerged regarding the methods for safely storing and/or sending such vast amounts of user data. These issues include the need to store and send data over the internet, such as passwords, account numbers, and bank verification numbers (BVNs). Therefore, in addition to the encryption-decryption methodology, this project work suggested a data hiding method called steganography to provide a superior security mechanism.

Steganography is the art and science of concealing information in various carrier files, including text, audio, pictures, video, and so on. Discussions on the necessity of sending messages as safely and securely as possible have been going on for a while. Any association's most valuable asset is its information. This means that for an organization that handles confidential data, security concerns are the top priority. The primary concern is the level of security, regardless of the process we employ for the security point. The ability to write in a way that is hidden or covered is known as steganography.

Steganography is a term that comes from the Greek words "stegos," which means "cover," and "grafia," which means "writing." Steganography refers to the technique of concealing a message, picture, or video inside another message, picture, file, or video. Through the use of steganography, information hidden in audio or video files can be revealed. The hiding process is controlled by a stego-key to reduce the likelihood of fixed data being discovered or recovered. A number of individuals accused Osama Bin Laden of utilizing eBay photos he uploaded that year to transmit covert signals to different terrorist groups.

The message, cover object, embedding method, and Stego key make up the fundamental steganography model. In Figure 1, the steganography model is displayed. A cover object, sometimes referred to as a carrier, conceals the message and disguises its existence. Covers or carriers for hidden data might be digital photos, movies, sound files, and other PC files that include redundant or perceptually irrelevant information. Once the cover-object has been embedded with a secret data, a so-called stego-object is produced.

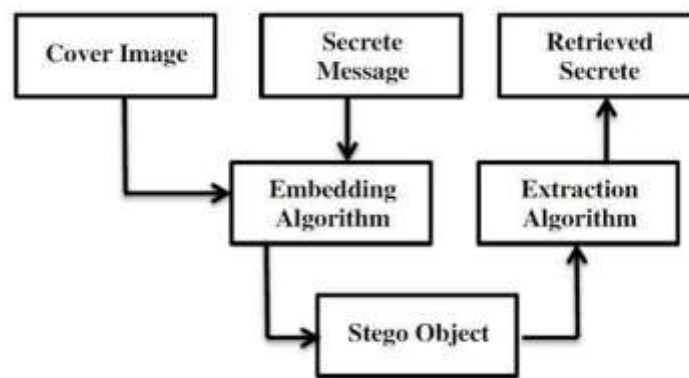


Figure 1.1 Basic Steganography Model

We can get the secret message from the Stego object at the recipient end by using an extraction method. The visibility, quality, and clarity of the image are unaffected by the project's use of the technique of concealing data within an image file. The duration of the hidden data may vary. When the image is previewed, the hacker will just see the image and not any indication of the hidden data. Since the information is kept in a binary encryption form, it will also not be visible if the picture file is opened in a text editor. This makes it challenging for the enclosure to distinguish between the data and the image file.

1.1 PROBLEM STATEMENT

Since utilizing cryptography to conceal messages appears to be vulnerable to "ease" of cryptanalysis, it is crucial that we use a more secure method that conceals texts in carriers like images. Using the Least Significant Bit (LSB) approach, image steganography is used in this study to provide a more secure data transport, particularly over the internet. The implementation of picture steganography using this approach is seen to be a practical solution to the security issues that cryptography presents.

2.2 AIM AND OBJECTIVES

The goal of this project is to create a system that uses images to accomplish steganography, which is a security mechanism that conceals a message from a third party. The objectives of the study are highlighted as below:

- To carry out a critical review of the concept of information security
- To carry out a thorough survey of the various steganography types we have
- To carry out an elaborate investigation into image steganography

II. LITERATURE SURVEY

TITLE: Steganography Techniques—A Review Paper, Jasleen Kour, Deepankar Verma, 2020

DESCRIPTION: Steganography is the process of concealing sensitive data in an apparently innocuous carrier media, like a text message, audio file, or picture. Steganography attempts to make the concealed data nearly imperceptible by encoding the secret message into the carrier media. Steganography is essential for secret communication because it makes it possible to send private data securely and without raising red flags. This study examines many steganography methods and how well they work to achieve undetectability. According to coding theory, steganography techniques use a variety of approaches to embed and encode hidden data while preserving the carrier medium's original properties. These approaches include spread spectrum, least significant bit embedding, and transform domain methods like wavelet and discrete cosine transforms. The development of steganalysis methods, which are employed to find and retrieve concealed data from carrier media, is also covered in this work. Additionally, the study emphasizes how crucial capacity and resilience are to steganography methods as they have a direct effect on the carrier medium's quality and the transmission of hidden information (Koptyra & Ogiela, 2020). By enclosing sensitive data in harmless carrier media, steganography techniques provide a useful way to communicate secretly. They not only offer an extra degree of protection, but they also make it possible to send private information without causing suspicion.

TITLE: Social Steganography: Privacy in Networked Public, Danah boyd, Alice Marwick, 2011

DESCRIPTION: Boyd and Marwick address the changes in privacy behaviors and views brought about by social media in the introduction of their study on social steganography (Sarwatay et al., 2021). They provide a networked privacy model that reflects the many ways in which people negotiate their privacy in online environments and stress the importance of understanding how people control their privacy in networked publics. This method acknowledges that protecting privacy entails more than just restricting access to personal information; it also considers things like social context, visibility, and information exchange practices. The authors argue that in order to create a fair and responsible "algorithmic sovereignty," social media platforms should give users more control over customizing algorithms. They also argue that public institutions and civil society should be involved in the creation and research of public algorithms. In their study, Boyd and Marwick emphasize how social media has fundamentally changed the dynamics of privacy and visibility, calling for a nuanced understanding of privacy in networked publics. They note that self-esteem is correlated with both virtual and in-person interactions, and that young people in particular often do not differentiate between their online and offline lives. The authors also note that most teenagers are not overly concerned about other parties seeing their data, even when they choose secret settings and distribute them carefully.

TITLE: Overview: Main Fundamentals for Steganography, Zaidoon Kh. AL-Ani, A.A. Zaidan, B.B. Zaidan and Hamdan.O. Alanazi,2010

DESCRIPTION: Steganography is a method for concealing confidential information beneath a cover that appears benign. This method guarantees that anyone who is not aware of the secret message's existence won't notice it. But as technology has advanced and steganography has become more popular, there is also a growing need for efficient steganalysis methods. The practice of employing steganography to find concealed communications is called steganalysis. Because of its great quality and small file size, JPEG is a popular picture format for steganography (Kose et al., 2020). It's crucial to remember that steganography and cryptography have different uses. Steganography seeks to completely conceal the presence of hidden communications, whereas cryptography concentrates on encrypting data to render it unintelligible. Imperceptibility, which guarantees that the concealed data is not observable by humans, is one of the essential conditions of steganography. This prerequisite is essential to preserve the stego-image's quality and prevent distortion in the reconstructed cover picture following the extraction of the sensitive data. It is impossible to overestimate the importance of precise weather forecasts in the quickly evolving world of today. It is impossible to overestimate the importance of precise weather forecasts in the quickly evolving world of today. "This attribute differentiates it from cryptography- when information is encrypted, it cannot be read, but everyone knows of its existence."

TITLE: Reversible Data Embedding in Golomb Rice Code, Awais M, Müller H, Tang T.B, Meriaudeau F,2011

DESCRIPTION: In addition to outlining the usage of Golomb Rice codes for reversible data embedding, the introduction of the work "Reversible Data Embedding in Golomb Rice Code" also discusses the significance of data embedding techniques. This method may be used in a variety of situations since it enables data to be embedded in any bitstream (Solano, 2020). The notion of "reversible steganography," which seeks to accomplish both reversibility and moderate undetectability, is also covered by the paper's authors. This work proposes a method for achieving reversible data embedding by altering the histogram using Golomb Rice codes. Based on histogram shifting, this double-layer embedding method concentrates changes in intricate regions of the pictures (Tang et al., 2020). Reversible data embedding in color pictures is the aim of the suggested double-layer embedding method based on histogram shifting employing Golomb Rice codes. This technique is intended to conceal data in a way that is easily undone without resulting in noticeable distortion or discovery. This method is crucial because it enables the secret storing of data, allowing for the restoration of the original content and the undoing of any data alterations. A useful addition to the field is the suggested reversible data embedding approach, which is based on Golomb Rice codes and histogram shifting in color pictures.

TITLE: RNN-Stega: Linguistic Steganography based on Recurrent Neural Networks, Yang Z.L, Guo X, ChenZ.M, Huang Y, F. Zhang,2018

DESCRIPTION: The process of concealing confidential information inside non-secret material, including text, audio, or pictures, is known as steganography. Steganography techniques can be used to obscure the secret message in a way that makes it impossible for an observer to detect. This makes it possible to communicate covertly because the hidden message cannot be detected. Recurrent neural networks may be used to do linguistic steganography with the RNN-Stega technique put forth by Yang et al. The RNN-Stega technique embeds hidden messages in text by harnessing the power of recurrent neural networks. This technique efficiently encodes and decodes secret information by utilizing RNNs and capitalizing on the sequential pattern of text data. Linguistic steganography is made more effective and efficient by employing RNN-Stega. The RNN-Stega technique of linguistic steganography, which is based on recurrent neural networks, provides a practical and efficient way to conceal confidential communications in text. Because the secret message is imperceptible to an observer, this approach enables clandestine communication. Two primary approaches are used in the field of steganography to safeguard the copyrights of digital information. The first tactic is to conceal copyright information in non-secret data by using steganography techniques, as the RNN-Stega approach (Fkirin et al., 2022). The second tactic is embedding information into the original digital work via digital watermarking to protect copyright.

III. ANALYSIS OF THE EXISTING SYSTEM

Security has always been the cornerstone of human transactions and life protection. Prior to the development of artificial intelligence, people learned to trust one another and the safety of information, with the exception of a few instances in which security was threatened by betrayal or breach of trust by individuals, which frequently resulted in severe crises. There was a method of security for every system and circumstance. For example, in ancient times, before modern technology advanced, kings used spies and allies to convey very confidential messages within and around the village, birds were sent on errands to neighboring villages or towns to announce the birth or death of a royal blood, and aroko—a material used primarily in western Nigeria, particularly among the Yoruba—was a symbol of information that can only be interpreted by the intended receiver even if it is received by someone else. New and creative approaches were developed as more and more circumstances demanded ever-tougher security measures. The banking industry provides a real-world example, since forms with security questions were utilized to disburse cash. This method was used for a while until banks started inventing passcodes that only the legitimate owners understood, enabling them to access their money, because fraud had become too hard to prevent. The banks demanded that their client's complete paperwork and provide truthful responses to personal questions that, presumably, only the legitimate owners were aware of. To reduce risk and offer the best protection, banks have implemented these and a number of other state-of-the-art security measures.

Before artificial intelligence, there were several other ways to ensure security, such as oaths and vowed secrecy. These security methods and techniques have a number of flaws that reduced their effectiveness. People have always wanted to keep their words and thoughts private, hidden from prying eyes. As a result, the options available to keep secrets safe are either unsatisfactory or draw unwanted attention to the presence of a locked secret. Therefore, they introduced an approach for securi

ng and safely hiding things in an unsuspecting manner. For example, if an attacker were to guess the random selection of numbers or letters used in the password, they could defeat the security and take away confidential information.

Thus, the development of steganography Using the Least Significant bit (LSB) for masking, filtering, and transformations on the cover picture is one of the most popular ways to make changes. LSB is the art and science of rendering communication incomprehensible to everyone but the intended receiver.

IV. ANALYSIS OF THE PROPOSED SYSTEM

The proposed system deals with information and a means of securing it. It uses one of the methods of information security; Steganography. The rapid development in the transfer of data through internet made it easier to transfer data accurate and faster to the destination.

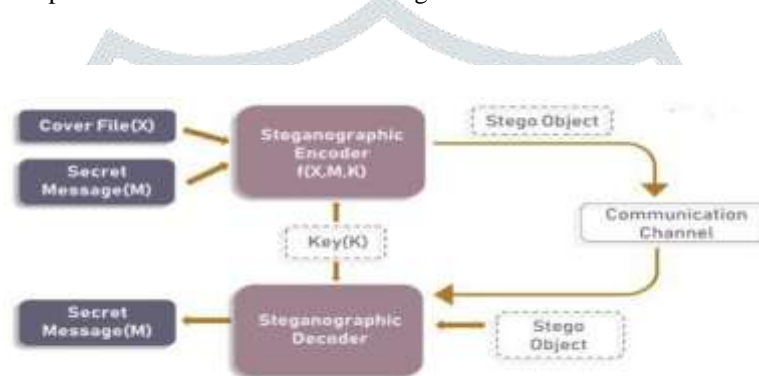


Figure 4.1 Graphical Representation of Steganography

Security of information is one of the important factors of information technology and communication. Steganography is art and science of invisible communication. Steganography is the method through which existence of the message can be kept secret. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information.

The Least Significant Bit (LSB) algorithm is used for this project job, and it modifies the image's least significant bit pixels, which in this case are the carrier file. The number of bits in the image determines how many bits are inserted in this technique. For example, in an 8-bit image, the bit of the secret message will be substituted for the LSB of each byte. The RGB (Red, Green, Blue) color components are appropriately replaced in a 24bit image using the secret data's MSB (Most Significant Bit). The lossless nature of JPEG images makes the LSB technique highly effective when applied to them.

ALGORITHM TO EMBED TEXT MESSAGE:

- Step 1: Examine the cover picture and the text message that will be concealed within it.
- Step 2: Convert the text message to binary format in step two.
- Step 3: Determine the LSB of each cover picture pixel.
- Step 4: Substitute each secret message bit one at a time for the cover image's LSB.
- Step 5: The Stego picture is shown.

TEXT MESSAGE RETRIEVAL ALGORITHM:

- Step 1: Examine the image of Stego.
- Step 2: Determine the LSB for every stego picture pixel.
- Step 3: Extract the bits, then turn each 8-bit bit into a character.
- Step 4: Presents the initial notification.

V. RESEARCH METHODOLOGY

5.1 AN OVERVIEW OF MODERN STEGANOGRAPHY

Steganography techniques have changed from ancient times to modern times due to technological advancements. Instead of changing the data into a different format, steganography conceals the data being transmitted by hiding it in a cover object, such as text, audio/video, images, or a protocol. The most desirable digital file formats are those with high redundancy, or the parts of an item that give accuracy considerably larger than the need for the object's usage and presentation, yet many of them can act as cover objects for concealed data (Morkel, Eloff, & Olivier, 2005).

The redundant bits can be defined as the number of bits that can be altered without the alteration being detected easily, an example is image and audio file formats.

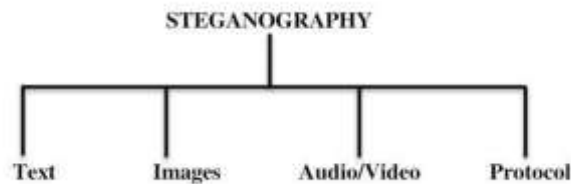


Figure 5.1 Cover object for Steganography

There are four primary file types that may be used as cover objects for concealed data, as shown above.

- a. picture Steganography: This approach involves hiding data within a picture without altering the original image.
- b. Audio Steganography: This technique can be used to conceal data in audio files. It should be impossible to detect the audio file.
- c. Video Steganography: Information in video files can be concealed using video steganography. The attacker should not be able to detect the video files.
- d. Text file steganography: Information in text files can be concealed using text steganography. Steganography is the broad technique of creating a stego object using text as a source that will not differ from the original item.

5.2 STEGANOGRAPHY ALGORITHM

5.2.1 SUBSTITUTION ALGORITHM

The usage of digital photos for steganography has increased as a result of the proliferation of digital images on the internet and the enormous amount of redundant data they carry. In the field of picture steganography, there are essentially two major types of replacement algorithms that are used to improve images:

1. Techniques in the Spatial Domain
2. Techniques for Transforming Domains

SPATIAL DOMAIN TECHNIQUES (IMAGE DOMAIN)

In this method, there is direct manipulation of the image pixel. This method conceals the secret information by substituting the bit value of the secret message for the selected portions of the cover image. This means that unless the secret data is converted into its matching bit value, it cannot be utilized in the cover image.

According to Mustafa, ElGamal, ElAimi, and Ahmed (2011), the Least Significant Bit (LSB) method is the most well-known steganography algorithm. It functions by substituting a representation of the secret message—which is imperceptible to the human eye as long as the image quality isn't appreciably diminished—for the Least Significant Bit of an image pixel.

Several spatial domain algorithms can randomly alter the carrier image's LSB, whereas others accomplish this via altering the pixel value (Wilson & Bryon, 1992). Pixel Value Differencing (PVD), Random Pixel Embedding Method, Texture Based Method, Histogram Shifting Method, and others are examples of such algorithms.

TRANSFORM DOMAIN TECHNIQUES

The secret information is concealed in regions that are less vulnerable to manipulation, like as compression and cropping, making this technique more complex than the spatial domain technique. Some mathematical functions, such as the sine/cosine function, conceal the data. The discrete cosine transformation (DCT), which affects the cover image's discrete cosine transformation, is one of the most widely used transform domain techniques. In essence, it finds any value below a specific value called the threshold after obtaining the image's corresponding DCT coefficient. The stego image is then created by substituting the secret bits for the returning value. Other forms of transform domain techniques include: Discrete Fourier Transformation (DFT), Discrete Wavelet Transformation techniques and Lossless DCT Method.

5.3 LEAST SIGNIFICANT BIT (LSB) ALGORITHM

The carrier file, which is the image's least significant bit pixels, is adjusted via the Least Significant Bit (LSB) algorithm. The bit insertion in this approach is contingent on the image's bit count. For example, the bit of the secret message will be substituted for the LSB of each byte in an 8-bit picture. In a 24bit image, the MSB (Most Significant Bit) of the secret data is used to replace the RGB (Red, Green, Blue) color components appropriately. The LSB technique works particularly well with JPEG images because of their lossless nature.

5.4 HIDING A TEXT WITHIN A PICTURE

Least Significant Bit (LSB):

- One of most common techniques.
- Alters LSB of each pixel (1 bit out of 24 or 1 out of 8 for gray scale)
- Uses the concept of parity, i.e., even numbers in binary end in 0, odd one end in 1
- Easiest to implement: hiding bitmaps in a color picture
- Hiding ASCII code, one letter at a time

Example: To hide letter C, which ASCII code is 67 and binary equivalent number is 1000111 in a grayscale file:

Original:

```
01001101 01001110 01001110 01001111 01010000 01010000
      1      0      0      0      0      0      1
01001111
      1
```

Encoded:

```
01001101 01001110 01001110 01001111 01010000 01010001
01001111
```

Encoding a message

The function encode() creates an image with message written in big black letters across it; it then invokes encode Picture() to hide the image with the message in the given picture.

5.5 SYSTEM DESIGN

This is the process of designing a new system, such as one to replace or enhance an existing one, but before we can do so, we must fully comprehend the old system and ascertain how computers might be utilized to improve its functionality.

VI. RESULTS AND DISCUSSION

This result and discussion offer the analysis and design for the implementation of the suggested system. A system is an arrangement of connected components and processes that cooperate well to accomplish certain objectives. Analysis, on the other hand, is a thorough investigation of the many components that make up the system in order to gain a deeper understanding of it. Thus, system analysis is the process of gathering, arranging, and examining information about current processes, systems, and activities in order to fully understand the current state of affairs and to plan and implement an efficient computerization program. The many components of the steganography technology are covered in this section. There are several methods for system analysis, which would include the following phases. I investigate the sets of algorithms, text, key, and interacting entities that comprise the system.

- The creation of a feasibility study, which entails figuring out if a project is possible from an organizational, social, and economic standpoint.
- Performing fact-finding procedures intended to determine the end users' needs for the system.
- Assessing how the system would be utilized by the end user, what it would be used for, and so on. The suggested system is analyzed using a structural and interaction model of the system.





VII. CONCLUSION AND FUTURE ENCHANCEMENT

The most widely used method for data security is steganography. It will function as a mechanism to conceal written text by blending it into images or by hiding it as plain text. To overcome the obstacles caused by image signaling breakdown. We suggested an improved version of steganography that is far more resistant to Friedman and Kasiski attacks. Because many tables are used for encryption, the suggested approach is also significantly more difficult to crack using cryptanalysis, frequency analysis, pattern prediction, and brute assault. The algorithm that creates the improved form of steganography now has a high proportion of confusion and diffusion, making it an extremely robust system that is challenging to crack. Even with the abundance of steganography and cryptographic techniques, this field still needs serious study network attention to increase data security. Our goal going forward is to validate the suggested strategy through security and performance study.

VIII. Acknowledgment

I, Prof. Rakesh Sharma, Dr. Jithendra, would like to express our heartfelt gratitude to the Department of Computer Science and Engineering, SIT, Valchil, Mangalore, for their continuous support, guidance, and for providing the infrastructure that made this research possible. I also thankful to our friends, mentors, and families for their constant encouragement and motivation throughout the project. Additionally, I acknowledge the open-source communities, whose contributions played a vital role in enabling the development of our real-time, AI-powered meeting summarization system.

REFERENCES

- [1] Steganography Techniques–A Review Paper, Jasleen Kour, Deepankar Verma, 2020.
- [2] Social Steganography: Privacy in Networked Public, Danah boyd, Alice Marwick, 2011
- [3] Overview: Main Fundamentals for Steganography, Zaidoon Kh. AL-Ani, A.A. Zaidan, B.B. Zaidan and Hamdan.O. Alanazi, 2010
- [4] Reversible Data Embedding in Golomb Rice Code, Awais M, Müller H, Tang T.B, Meriaudeau F, 2011
- [5] RNN-Stega: Linguistic Steganography based on Recurrent Neural Networks, Yang Z.L, Guo X, ChenZ.M, Huang Y, F. Zhang, 2018
- [6] Secure Data Transmission Through Steganography with Blowfish Algorithm, K. Vengatesan, Tusar Sanjay Subandh, Saiprasad Machhindra Wani, Abhishek Kumar, Achintya Singhal, Rajiv Vincent, Samee Sayyad, 2019.
- [7] Secure Data Transfer via Internet Cryptography and Image Steganography in Wireless Sensor Networks, Dr. P. Kavitha, P. Elamaran, 2024.
- [8] A Novel Technique for Secure Data Transmission using Distributed Steganography and Cryptographic Techniques, Smt. K. Venkata Ramana, Smt. S. J. R. K. Padminivalli V, Ms. V. Vijaya Lakshmi, 2015.
- [9] Steganography Techniques: A Review, Mr. Pravin R. Kamble, Mr. Prakash S. Waghmode, Mr. Vilas S. Gaikwad, Mr. Ganesh B. Hogade, 2013.
- [10] Securing Data Communication of Internet of Things in 5G Using Network Steganography, Yixiang Fang, Kai Tu, Kai Wu, Yi Peng, Junxiang Wang, Changlong Lu, 2020.

- [11] A Review on Image Steganography Techniques, Neha Gupta, Rakesh Kumar, 2015.
- [12] Secure Data Transfer through Internet Using Cryptography and Image Steganography, Krishna Chaitanya Nunna, Ramakalavathi Marapreddy, 2020.
- [13] Improved Secure Data Transfer Using Video Steganographic Technique, V. Lokeswara Reddy, 2020.
- [14] A Comparative Study of Steganography Techniques: A Review, Sahil Raj, Harsh Tyagi, Devansh Mishra, 2023.
- [15] C.Sanchez-Avila and R. Sanchez-Reillo, "The Rijndael block cipher (AES proposal): a comparison with DES," in Security Technology, 2001 IEEE 35th International Carnahan Conference on, 2001, pp. 229-234.
- [16] Bio-Inspired Algorithms for Secure Image Steganography: Enhancing Data Security and Quality in Data Transmission, Samira Rezaei, Amir Javadpour, 2024.
- [17] A Secure Multimedia Steganography Scheme Using Hybrid Transform and Support Vector Machine for Cloud-Based Storage, Arunkumar Sukumar, V. Subramaniaswamy, V. Vijayakumar, Logesh Ravi, 2020.
- [18] Secure Data Hiding Techniques: A Survey, Laxmanika Singh, A.K. Singh, P.K. Singh, 2020.
- [19] Ensuring Security of Data Through Transformation-Based Encryption Algorithm in Image Steganography, Sushil Kumar Narang, Vandana Mohindru Sood, Vaibhav, Vania Gupta, 2024.
- [20] Secure and Efficient Data Transmission by Video Steganography in Medical Imaging System, S. Balu, K. Amudha, C. Nelson Kennedy Babu, 2018.
- [21] A Review on Various Steganography Techniques, Priyanka Sharma, Rakesh Kumar, 2014.
- [22]] https://www.researchgate.net/publication/278329938_A_Review_on_the_Various_Recent_Steganography_Techniques
- [23] Puneet Kumar, Shashi B. Rana, Development of modified AES algorithm for data security, Optik- International Journal for Light and Electron Optics, Volume 127, Issue 4, 2016, Pages 2341-2345, ISSN 0030-4026, <http://dx.doi.org/10.1016/j.ijleo.2015.11.188>. (<http://www.sciencedirect.com/science/article/pii/S0030402615018215>)
- [24] Steganography: A Secure Way for Transmission in Wireless Sensor Networks, Khan Muhammad, 2015.
- [25] Blockchain for Steganography: Advantages, New Algorithms and Open Challenges, Omid Torki, Maede Ashouri-Talouki, Mojtaba Mahdavi, 2021.
- [26] Secured Data Transfer through Images by Using Data Hiding and Encryption, Siddhant Saka, M Manish, Debopam Dey, Thanikaiselvan V, Amirtharajan R, 2020.
- [27] Secure Image Steganography using Cryptography and Image Transposition, Khan Muhammad, Jamil Ahmad, Muhammad Sajjad, Muhammad Zubair, 2015.
- [28] Android Application Development for Secure Data Transmission using Steganography, Vineet Ramesh Jeswani, Savita Kulkarni, Manisha Ingle, 2015.
- [29] Secure Data Transfer over Internet Using Image Steganography: Review, Dakhaz Mustafa Abdullah, Siddeeq Y. Ameen, Naaman Omar, Azar Abid Salih, Dindar Mikaeel Ahmed, Shakir Fattah Kak, Hajar Maseeh Yasin, Ibrahim Mahmood Ibrahim, Awder Mohammed Ahmed, Zryan Najat Rashid, 2021.
- [30] Enhanced Security of Symmetric Encryption Using Combination of Steganography with Visual Cryptography, Sherief H. Murad, Amr M. Gody, Tamer M. Barakat, 2019.
- [31] https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
- [32] https://en.wikipedia.org/wiki/Polybius_square
- [33] Classical cipher, Transposition ciphers, Retrieved from http://en.wikipedia.org/wiki/Classical_cipher
- [34] Transposition ciphers, columnar transposition Retrieved from http://en.wikipedia.org/wiki/Transposition_cipher
- [35] <https://www.geeksforgeeks.org/difference-between-steganography-and-cryptography>