

Secure Data Transfer Over Internet Using Image Steganography.

Chapter 1: introduction

Background

Transfer of information through the Internet creates many challenges related to data security and receipt, especially when sensitive information is at stake. Encryption is generally considered a correct method to protect confidential data, providing it inaccessible to unauthorized parties. Nevertheless, the use may unconsciously indicate that valuable information is protected, potentially attention or targeted attacks on drawing. As a result, researchers have discovered alternative methods. Steganography, which involves hiding information in others, appears to be an important approach in this context [1]. Steganography and the transition between the encryption lie in the subtlety: encryption strolls data, it makes it unreadable, but also emphasizes itself as preserved information. Steganography, on the other hand, is aimed at existing the existence of a message hidden from any unexpected audience. In short, the information hides so well within regular media that its presence is not noticed by anyone, and provides an extra layer of discretionary [2].

Throughout history, humans have always found clever ways to conceal information—think invisible ink or encoded tattoos, pretty much straight out of a spy novel. In the digital age, though, things have gotten way more sophisticated. These days, people often hide information inside digital images because, let's face it, there's a ton of extra data buried in most pictures that no one ever notices. Here's the trick: by making tiny changes to things like the least significant bits in a pixel (the sort of detail even a hawk-eyed viewer won't catch), confidential info can be tucked away without messing up how the image looks at all. So, you get a perfectly normal-looking photo that quietly carries a hidden message—practically invisible, but definitely there.

When steganography is combined with encryption, the security of hidden messages takes a significant leap forward. Even if an adversary identifies the presence of concealed information within a digital medium, the data itself remains protected by encryption, rendering it inaccessible without the appropriate cryptographic key.

Given the rapid growth of cyber threats, not only provides to rely on traditional encryption methods enough insurance for secure transfer of sensitive data. In light of these challenges, this research introduces an online steganography system that uses minimum important bits (LSB) techniques to encrypt data in digital images. The primary goal is to install a strong and secure channel for broadcasting confidential information on the Internet, which reduces the risk of risk or unauthorized access.

In short, the project wants to produce effective integration of encryption and steganography as Amin to increase privacy for data under digital communication. Growing complications today, given the dangers of cyber security, take such an approach to an approach to protect sensitive information in the electronic environment and address concerns that suppress concerns. Finally, objective and practical solutions to protect private data to develop.

Problem Statement:

Given the landscape of sometimes the landscape of cyber threats-from-Detta-cutting to unitarian-internet-have become a fast Cruel effort to promote sensitive information sent on the Internet. Although the encryption is still a basic tool for protecting data by presenting it unparalleled to outsiders, it is not without deficiencies. In fact, encrypted data often indicates topo tensive attackers that the information is of important value, the potentially targeted cutter invites you to decrypt. For this reason, further safety strategies such as steganography - who Radeta seems to appear hidden in the files - important. By adding these methods, organizations can more unclear and defend sensitive information during transmission, increasing the strength of the cyber security currency.

Research Objectives

This research picture focuses on establishing a strong and secure approach to transfer information on the Internet using actinography. The central idea is to benefit from the underlying excess indigenous images, and create confidential data built in such a way that its presence remains for external observers, while the general image quality is preserved. To further improve safety, the proposed method integrates encryption - especially asynchronoscription - which is embedded in the primary. This means that even an attacker identifies the existence of an attacker hidden data, they will still not be able to understand the material without access to the correct decrypt key. The main objectives of the project are as follows:

- Develop algorithm that is able to enter data into minimalist pieces of a digital image. Inaccessible without appropriate authority.
- Maintain the visual integrity of the visual integrity of the image so that its presence does not stimulate the presence of confidential information.

In summary, the purpose of this double -layer safety method is not only to hide the existence of sensitive data bits, and also ensure the content, leading to a significant increase in the general security of data TransferWise digital images.

Chapter 02: Literature Review:

Nanna and Krishna [6] introduce a hybrid approach that merges cryptography with image steganography, which aims to increase the safety of data transfer on the Internet. In its method, the data is first encrypted by the use of x Or - operations - a technique that is inadequate, usually as a standalone encryption method against refined attacks. Once, the data is built into an image based on a user -defined key, which is based on the layering of safety effectively by effectively by hiding and encrypting the message. The author does not address the most important assessment criteria for the quality of these images, such as top-to-NOS (PS). The Tethese matrix lapses leaves unanswered questions how well the Steganographic process preserves the native image's disciplinary integrity, which is an important idea in the assessment of SSY Systems. Alrikabi and

Hagim [7], offering an innovative approach to protect sensitive information during reciting and steganography integrates both. Their method comes out in three stages: Originally, they use discomfort Belstranda (DWT) on both hosts and secret images. Thistchnique decomposes each image in different frequency rounds, enabling selective manipulation to the more efficient built - in of the secret image in the host. The next phase includes the built -in process. The specific coefficients of the host image are set to zero and mainly clean the site of the secret image. The secret image data is then modified and inserted, which is the integrated null coefficient, which helps to hide the appearance of hidden materials. Usually common picture - now hidden information - under -crept encryption

Despite its strength, the function is not without deficiencies. The dependence on DWT and complex functions increases the calculation requirements, and potentially limits practically. In addition, changing pixel values for built -in can reduce visual objects or hostbild quality, especially if the process is not carefully controlled.

Hasballah et al. [8] A method known as HHO-IWT was introduced, which is specially designed for protection, which is ready for the Industrial Internet of Things (IIOT) environment. The approach integrates Harris Hukanhecain with Integer Wavelet transformation, which enables the built-in of confidential data integrated overlay picture pixels. This targeted selection process not only increases the payload capacity but also preserves the visual integrity of the images and strengthens security measures against stealth attacks. It is important to note, however, that the study's focus remains exclusively on IIoT-related applications. The effectiveness or adaptability of this technique for other domains was not addressed, representing a notable limitation in the scope of their research.

Shree and Swami [9] proposed a hybrid system for secure data transmission, based on encryption and image hiding techniques. The proposed method first encrypts plaintext and converts it to a ciphertext image, which is then hidden inside a cover image to create a hidden image. The study did not specify the encryption algorithm used, so the level of security depends on the quality of the encryption algorithm used. Furthermore, the study did not detail the methodology used in the data hiding process. Therefore, providing precise details on this topic would be useful to evaluate the effectiveness of the proposed system.

Alkhudaydi and Gutub [10] , presents a dual-layer security system that combines lightweight cryptography (LWC) with Arabic text steganography. The methodology consists of two main stages: 1. Light-Weighted Cryptography (LWC), where sensitive text is first encrypted using lightweight encryption algorithms such as AES, DES, or IDEA to convert it into an unreadable format. 2. Arabic Text Hiding: The encrypted data is not embedded in an image or media as is customary, but rather embedded within the Arabic text's diacritical marks. In other words, the Arabic text with diacritical marks is the encrypted text. Although the methodology aims to make hidden information difficult to detect, the cover text, when it appears with diacritics that do not conform to Arabic grammar rules, may raise suspicions among attackers that hidden data is present. Furthermore, the encryption algorithms used in the study (AES, DES, IDEA) still require computational costs.

Wani et al.[11] introduced a notably advanced approach to multi-image steganography, aiming to strengthen communication security—particularly in military applications. Their method integrates AES encryption with the least significant bit (LSB) substitution technique, a classic tactic for embedding hidden information within images. What makes their system stand out is the way it divides the encrypted message and disperses it across multiple images, significantly complicating unauthorized extraction. The reported image distortion was minimal—about 0.059%—which means the visual quality remained practically untouched. This feature is crucial when the transmission of highly sensitive data is involved.

On a related note, Oji et al[12]. proposed a hybrid system called Stagedive, which fuses RSA encryption with LSB steganography but applies it to video rather than static images. Their process involves segmenting a video into individual frames, encrypting these with RSA, and then embedding the encrypted data back into the frames using LSB. One of the main forces in the system is its capacity, which has its capacity after decrypting and data extraction, only with insignificant changes in file size (for example, 1.12 MB of video remains essentially the same). The solution also supports live streaming, making it suitable for real-time applications such as distance education and video conferences, and meets the integrity and appearance of all original videos. Writers emphasized the effectiveness of their approach, remembering its ability to transfer secure data without observable visual deformation.

Abdulmaged [13] introduced an advanced hybrid approach that merges with AES encryption, HSI color space formation and genetic algorithms to hide safety data in digital images. Cockfosters with encryption of target data through AES, and then converts the front-page image to the HSI color model, which was later divided into blocks. Subsequently, a genetic algorithm is used to identify teoptimal blockage for data admission, especially with values such as the highest signal-to-show ratio (PSNR). Encrypted information is built into pieces of randomly selected bytes in this selected block. A genetic algorithm is then employed to identify the optimal block for data embedding, specifically the one yielding the highest signal-to-noise ratio (PSNR)—with reported values reaching up to 83.85 dB. The encrypted information is embedded in the least significant bits of randomly chosen bytes within this selected block. Experimental results highlighted the

scheme's effectiveness, maintaining exceptionally high image quality, as evidenced by PSNR values ranging from 77.61 to 83.85 dB for standard 512×512 images.

Abdullah and Fadel [14] developed a method for incorporating steganography into online applications by concealing private information within digital photographs. In order to avoid visual distortion, the system used an SVM classifier to analyze image pixel priority and determine the best embedding regions based on color contrast and 8-neighbor coherence. Pixel value changes were kept to a maximum of ± 2 units. A random key was created to regulate the embedding sequence after text input was transformed into a binary stream and embedded into the least significant bit (LSB). The suggested methodology produced good results, according to the authors, with a signal-to-noise ratio (PSNR) of 89.52 dB (as opposed to 73.53 dB in traditional LSB methods).

Clearly, combining encryption and obfuscation is a promising approach to securing data transmission over the internet, especially for sensitive data requiring high security. The reviewed studies highlighted numerous methodologies that discussed different ways to protect data through the development of different techniques. For example, the hybrid systems proposed by Nona and Krishna, as well as Shri and Swami, emphasize the importance of two-layer security. However, these studies often lacked sufficient details about the encryption algorithms used.

Although the use of lightweight encryption may be effective for devices with limited capabilities, as in the studies of Al-Khaji and Ghatlab, it poses challenges related to potential vulnerabilities that could compromise data during transmission. Therefore, the reliance on the XOR algorithm in some studies may be a clear weakness, as it may not withstand sophisticated attacks. Therefore, there is an urgent need for a stronger encryption technique. The stronger the encryption algorithm, the more resilient it is to even the most powerful attacks, making data transmission more secure.

Embedding data within images inevitably impacts the quality of the original medium, as pixel-level manipulations tend to degrade visual fidelity. There's also a hard cap on how much information you can actually conceal, since the algorithm's pixel selection directly limits the message size. This not only improves capacity, but also increases the risk of detection, and allows the image to be manipulated to the attacker's advantage. Furthermore, the current methods lack

strict evaluation by using established performances - which think of PSNR and MSE - which makes it difficult to assess their efficiency. These intervals are clearly required by a stronger assessment structure in lightoffs. When combining with encryption, it is definitely a compressed approach, and running research should address these deficiencies that are really safe and reliable data transfer.

Chapter 03 : Methodology

In this section, we will explain the proposed methodology for designing the proposed system, which seeks to develop a secure data transmission system based primarily on image steganography technology. The process of encrypting the intended message, using Advanced encryption standards (AES), is a widely recognized symmetrical encryption algorithm known for its security facilities. When encrypted, the message is converted to binary form, which produces the celebration of appropriate pieces for built -in. The built -in process uses an adaptive at least significant bit (LSB) steganography algorithm. Uncontrolled LSB methods, adaptive approaches include the analysis of digital image to identify optimal-specific to identify the pixels-der data can be hidden with minimal conceptual deformation. This selection is important, as changes in these areas suggest that it is inherent. Selected pixels, steganographic dimensions are transferred to the entire network. By integrating both cryptographic encryption and adaptive steganography, this method aims to provide a safe and effective means of protecting sensitive information from sensitive and unauthorized access during online communication.

1. System workflow

System workflow for Sender Side

Figure 1 depicts the initial phase of the transmission process, specifically system initialization. At this juncture, critical parameters—such as the encryption key, connection settings, and network availability—are verified. This preliminary check is essential to ensure the subsequent transmission proceeds without disruption.

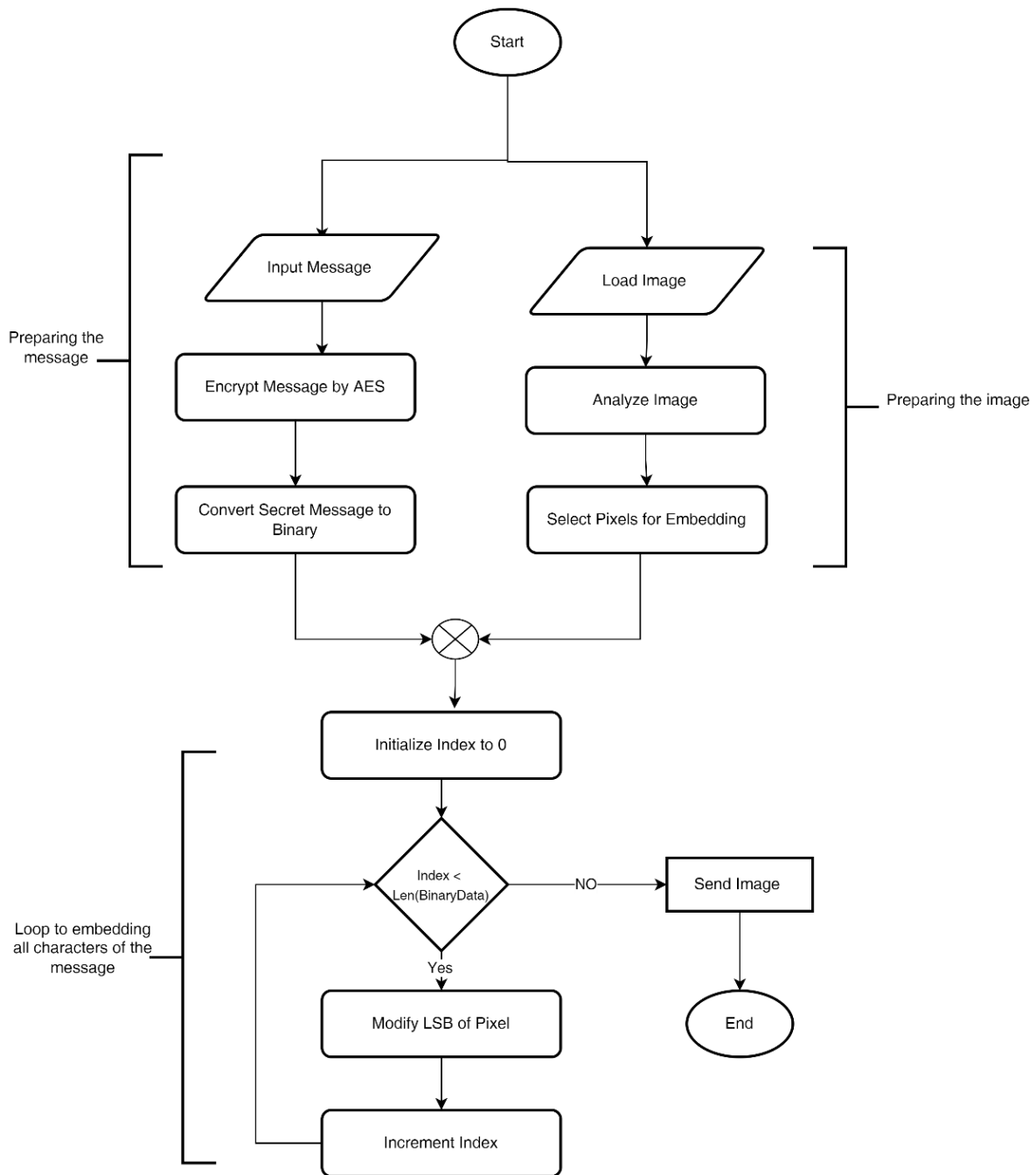


Figure 1: system workflow Sender Side (Encryption and Embedding)

The system allows the user to type the message to be sent securely. Considering this information to be critical, the system first applies AES encryption. This ensures that even if attackers are able to discover a secret message and analyze the image to extract the hidden message, they will not be able to interpret it without the decryption key.

The ciphertext is then converted to binary format, producing a series of bits (0s and 1s). These bits are what the system will ultimately embed in the image. The user then selects a cover image to use as a means of concealing the message. Before embedding, the system examines the selected image to identify areas with rich texture or edges, as these areas are more resistant to small pixel changes. Based on this analysis, appropriate pixels are selected. The embedding process begins with the first bit.

For each selected pixel, its least significant bit (LSB) is adjusted to match the current bit of the message. After the bit is included, the system moves to the next bit until the entire binary sequence is included. After all bits are included, the image containing the hidden message is ready to be transmitted to the receiver.

System workflow for Receiver Side

On the receiver side, the process begins with receiving the image transmitted over the network containing the hidden message. The system analyzes the image to identify potential pixels for inclusion. Using the same adaptation rules as the sender, the system retrieves the least significant bits from those pixels one by one. These extracted bits are reassembled into the original encrypted sequence. After the binary data is reconstructed, the system applies an AES decryption step, which restores the sender's message to its original, readable form.

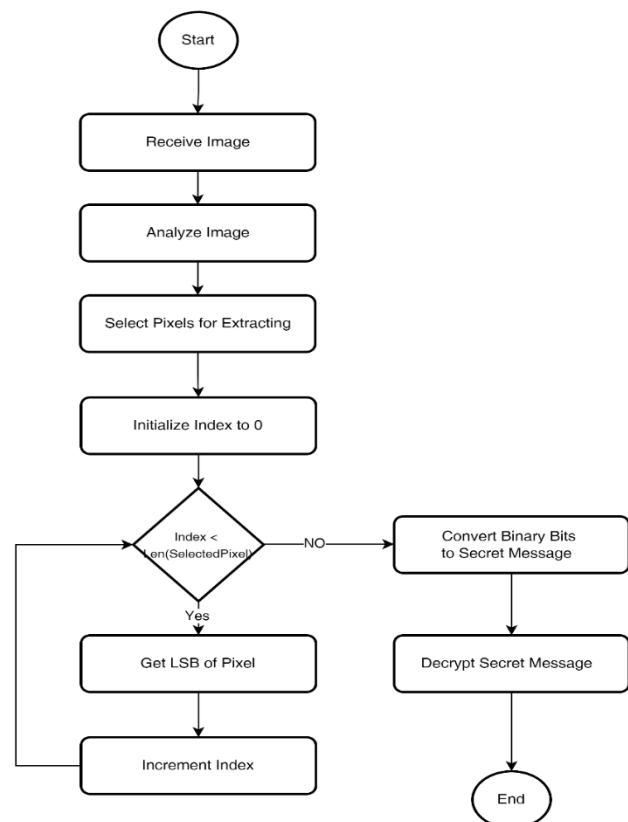


Figure 2: system workflow Receiver Side (Extraction and Decryption)

Expected output

The proposed method is expected to maintain image quality after embedding, as any distortion in the image would indicate that the image contains a hidden message. Therefore, the Peak Signal-to-Noise Ratio (PSNR) criterion should be measured, which measures the quality degradation resulting from data embedding. Image quality degradation is directly proportional to the size of the embedded message, with the degradation increasing as the embedded message size increases. The graph (Figure 3) shows the expected PSNR in decibels for different message sizes. A higher PSNR value (>40 dB) indicates minimal distortion, ensuring that the embedding image remains visually similar to the original. As the message size increases, the PSNR value decreases slightly due to further pixel modifications. However, values remain above 66 dB, confirming that the adaptive LSB embedding technique effectively preserves image quality while securely hiding data.

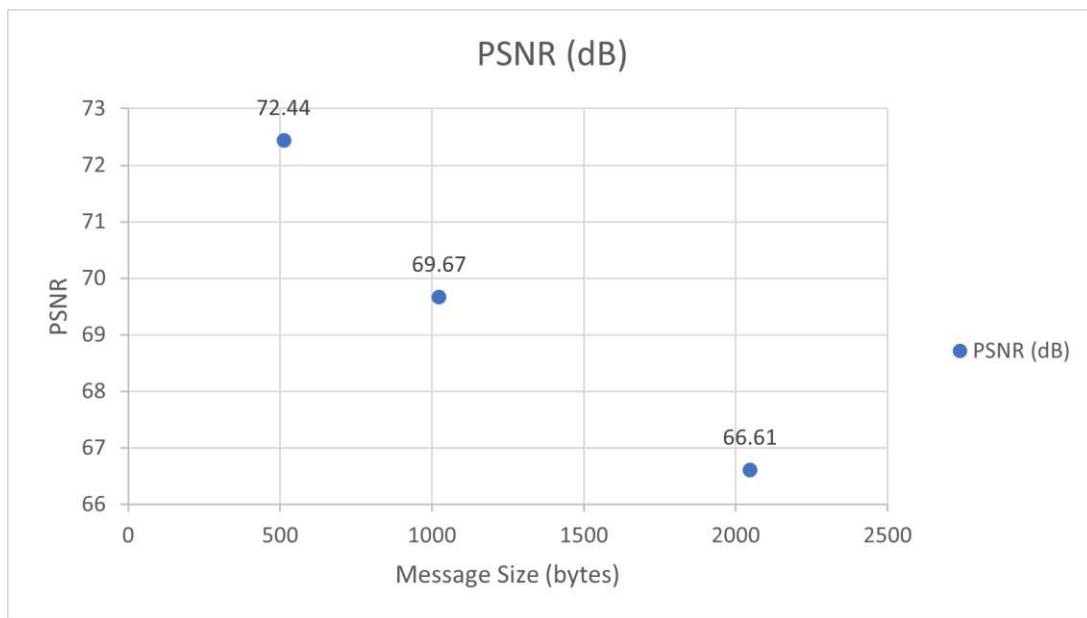


Figure 3 Peak Signal-to-Noise Ratio to message size

In addition, the Mean Square Error (MSE) criterion measures the degree of distortion resulting from the data embedding process. The graph (Figure 4) shows the expected mean square error (MSE) values for different message sizes included in the embedding image. A low MSE value indicates minimal pixel intensity modification, preserving the visual integrity of the image. The expected results show a slight increase in MSE with increasing message size, which is expected

due to increased pixel modifications. However, the values remain low (≤ 0.0142), confirming that the adaptive LSB embedding technique ensures insensitivity while securely hiding data.

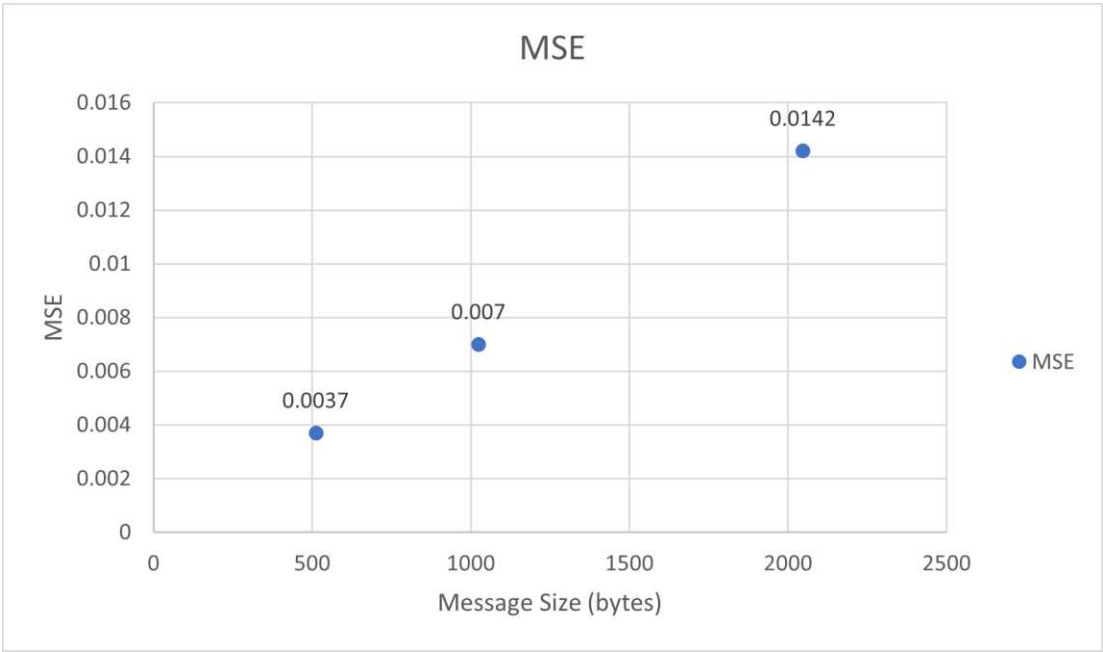
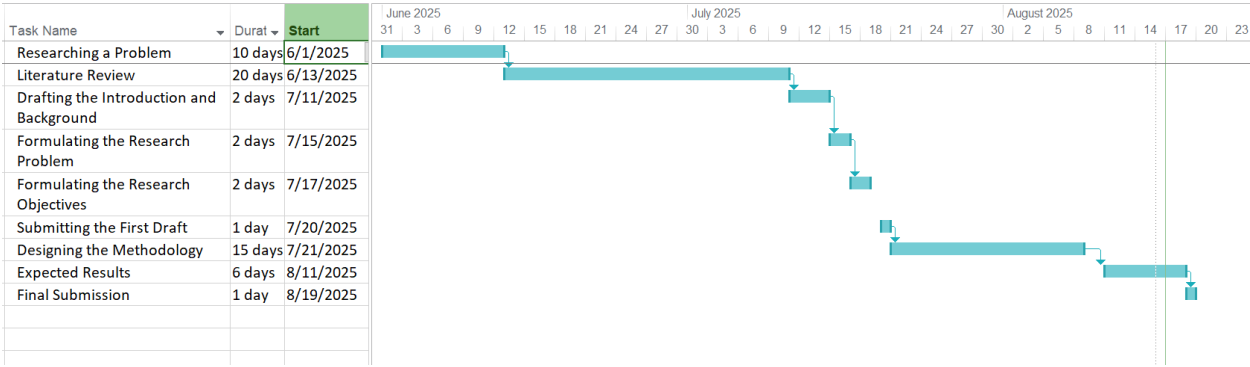


Figure 4 MSE to message size

Gantt chart



References

- [1] D. Watermarking, S. Katzenbeisser, and F. A. P Petitcolas, *Recent Titles in the Artech House Computer Security Series Rolf Oppliger, Series Editor Information Hiding Techniques for Security Technologies for the World Wide Web, Rolf Oppliger*, 1st ed., no. 112. Artech House, 2015. [Online]. Available: <http://www.ifi.unizh.ch/~oppliger/serieseditor.html>.
- [2] N. Jhonson, Z. Duric, and S. Jajodia, *Information Hiding Steganography and Watermarking : Attacks and Countermeasures, Advanced in Information Security*. New York: Springer Science-Business Media, 2001. doi: 10.1007/978-1-4615-4375-6.
- [3] J. Fridrich, *Steganography in digital media: Principles, algorithms, and applications*, vol. 9780521190. Cambridge university press, 2012. doi: 10.1017/CBO9781139192903.
- [4] M. M. Taher, A. R. B. H. J. Ahmad, R. S. Hameed, and S. S. Mokri, "a Literature Review of Various Steganography Methods," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 5, pp. 1412–1427, 2022.
- [5] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.
- [6] K. C. Nunna and R. Marapareddy, "Secure data transfer through internet using cryptography and image steganography," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2, 2020, doi: 10.1109/SoutheastCon44009.2020.9368301.
- [7] H. T. S. Alrikabi and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 16, pp. 144–157, 2021, doi: 10.3991/ijim.v15i16.24557.
- [8] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A Novel Image Steganography Method for Industrial Internet of Things Security," *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7743–7751, 2021, doi: 10.1109/TII.2021.3053595.
- [9] R. Shree and D. Swami, "Hybrid Secure Data Transfer Scheme Using Cryptography and Steganography," *Lect. Notes Networks Syst.*, vol. 166, pp. 577–583, 2021, doi: 10.1007/978-981-15-9689-6_62.
- [10] M. Alkhudaydi and A. Gutub, "Securing Data via Cryptography and Arabic Text Steganography," *SN Comput. Sci.*, vol. 2, no. 1, 2021, doi: 10.1007/s42979-020-00438-y.
- [11] P. Wani, A. Nanaware, S. Shirode, A. Suram, and P. Archana, "SECRET COMMUNICATION USING MULTI-IMAGE STEGANOGRAPHY FOR MILITARY PURPOSES.," *IJCRT*, vol. 10, no. 7, 2022.
- [12] O. Ojo, M. Kareem, I. K. OGUNDOYIN, O. Oyinloye, and O. Ikumpayi, "Stegovideo: An Efficient Mechanism for Securing Video Data Using Steganography and Cryptography Techniques," *J. Sci. Technol.*, vol. 42, no. 2, pp. 50–63, 2024, doi: 10.4314/just.v42i2.4.
- [13] N. Mohammed Abdulmaged, "Hybrid Steganography for Enhanced Information Security," *Int. J. Math. Stat. Comput. Sci.*, vol. 3, pp. 359–364, 2025, doi: 10.59543/ijmscs.v3i.11135.

- [14] Salam Khalaf Abdullah, Ammar Mohammedali Fadhil, "Enhancing Data Security: Implementing Steganography in Web Application," *Journal of Information Systems Engineering and Management*, vol. 10, no. 29s. pp. 850–857, 2025. doi: 10.52783/jisem.v10i29s.4596.