

# Steganographic Metadata Embedding to Trace the Footprint of ChatApp Images

Vaibhav Dobe, Komal Dumbare, Dhudhbahte Priyanka, Riya Dhomne, Dr. Suresh Mali

Dr. D. Y. Patil College of Engineering and Innovation, Pune

**Abstract:** This research paper proposes a method to trace the footprint of senders while forwarding of images on ChatApp by embedding metadata (such as mobile numbers) using Least Significant Bit (LSB) steganography. The technique ensures that the hidden information is imperceptible to users and remains intact even after ChatApp's image compression. The method allows for tracking the digital footprint of images, providing traceability to combat misinformation, piracy, and privacy concerns. The system is robust, enabling metadata recovery after multiple shares, with applications in digital forensics, media integrity, and monitoring the spread of viral content

**Keywords:** LSB, Steganography, Metadata, Imperceptibility, Data-Hiding, Cryptography

## I. INTRODUCTION

In today's digital age, messaging applications like WhatsApp, Telegram, and others have become integral to personal and professional communication. While these platforms offer convenience and speed, they also introduce challenges related to the spread of misinformation, offensive content, and privacy violations. One critical problem is the inability to trace the origin and modifications of forwarded messages, which can lead to serious reputational damage, misinformation, and legal consequences.[5] Metadata is a set of data that describes and gives information about other data. The technique used to address this problem is 'Steganography'. The term "steganography" comes from Greek words: "stegos," meaning cover, "grafia," meaning writing.[1] It's all about hiding one piece of data inside another one—kind of like a secret! Today, we see steganography in different ways. Think about digital watermarks or Quick Response (QR) codes. Sometimes, messages are even hidden in audio files—like when you hear backward masking. It's even found in modern cyberattacks, like malvertising!

Steganography, the practice of hiding data within other seemingly innocuous information, can be categorized into the following key types:

- Text Steganography: Hides metadata by altering text formats, replacing words, or generating random strings, though Unicode limits unprintable characters.
- Image Steganography: Embeds metadata within digital images by making small, imperceptible changes to redundant pixels.
- Audio Steganography: Conceals metadata within audio files by modifying sound waves, often using ultrasonic or infrasonic frequencies.
- Video Steganography: Embeds metadata in video frames, applying similar techniques to image steganography.
- Network Steganography: Hides metadata in network protocols by embedding it in packet headers or payloads. [4]

## II. MOTIVATION AND OBJECTIVES

### 2.1 Motivation

The LSB Steganography technique offers a potential solution by embedding traceable information, such as sender metadata or modification history, into images shared through these platforms. This can help identify the source of controversial content and trace any unauthorized changes, ensuring accountability and promoting transparency in digital communication. Key motivations behind this project are:



1. Combating Misinformation
2. Tracking Content Modifications
3. Enhancing Privacy and Security
4. Legal and Ethical Implications
5. Minimizing Impact on User

## 2.2 Objectives

1. To develop an algorithm for embedding Meta- data bits into the image before forwarding.
2. To make sure that the original image will not get detorate drastically.
3. To develop an algorithm for extraction of Meta- data to track the people who have forwarded the message.
4. Security of Metadata by using an effective steganographic algorithm and randomization tech- nique with password protection against variation attacks.

## III. LITERATURE SURVEY

1. Utilizing Imaging Steganographic Improve- ment using LSB Image Decoder: This pa- per by Ashish Kumar Verma, Shruti, and Tiyas Sarkar introduces an enhancement to the LSB image steganography technique by incorporating an image decoder. The proposed method improves the security and robustness of hidden data while maintaining the image's visual quality, offering a more secure approach to embedding secret data in digital images.[1]

2. LSB Steganography Mechanism to Hide Texts Within Images Backed with Layers of Encryp- tion : In this paper, Shukla, A. Joshi, and S. Girmé present a method for enhancing image steganography using the LSB technique combined with multiple layers of encryption. The approach ensures that hidden text within images is more secure by encrypting the data before embedding it using the LSB method. The added encryption lay- ers enhance protection against unauthorized ac- cess, making this method more robust for secure communication. The paper highlights the impor- tance of combining encryption with steganography for improved data security.[2]

3. Information Hiding using Least significant bit Steganography and cryptography: In this study, Shailender Gupta, Ankur Goyal, and Bharat Bhushan introduce an integrated method that combines LSB steganography with cryptography to enhance secure data-hiding. This approach en-

tails encrypting the confidential information before its insertion into an image using the LSB tech- nique, thereby creating a dual layer of security for the hidden data. This method ensures that the un- derlying encrypted information remains protected even if the steganographic layer is compromised.[3]

4. Cryptography and Digital Image Steganog- raphy Techniques: In this paper, Dipti Kapoor Sarmah and colleagues explore the integration of cryptography with digital image steganography to enhance secure communication. The authors discuss various steganographic techniques, focus- ing on optimizing the process using metaheuris- tic approaches. By combining cryptography and steganography, the paper demonstrates improved data protection, ensuring that sensitive informa- tion is encrypted and securely embedded within digital images. The optimization methods pre- sented aim to improve the efficiency and security of steganographic processes in digital media appli- cations.[4]

5. A Novel Approach of Image Steganography for Secure Communication Based on LSB Sub- stitution Technique: In this research, Shahid Rahman and his collaborators introduce a distinc- tive method for image steganography that leverages the LSB substitution technique. The focus of this approach is on securely embedding sensitive in- formation within digital images while preserving the original image's quality. By enhancing the tra- ditional LSB technique, this method significantly increases the protection of the hidden informa- tion, making it more challenging for unautho- rized users to detect or extract the concealed data. This innovative technique proves to be particu- larly beneficial for secure communication, where safeguarding data integrity and confidentiality is essential.[5]



6. A New Combinational Technique in Image Steganography: In this paper, Sabyasachi Pra- manik and his colleagues introduce a novel com- binational technique for image steganography that aims to enhance the security and efficiency of hidden data. Their approach integrates multi- ple steganographic methods to improve data con- cealment within digital images while maintaining image quality. By using this combination of tech- niques, the authors present a more secure and robust method for embedding sensitive informa- tion, making it more difficult to detect or extract the hidden data. This combined approach offers improved reliability for secure communication and protects information privacy.[6]

7. GAN-Based Encoding Model for Reversible Image Steganography: In this paper, Afolashade Kuyoro and colleagues propose a novel encoding model for image steganography based on Generative Adversarial Networks (GANs). Their ap- proach emphasizes reversible steganography, en- abling both the embedded secret data and the original image to be perfectly recovered. By uti- lizing GANs, the encoding process generates high- quality stego-images that are resistant to detec- tion while preserving the integrity of the original image. This method offers an advanced solution for secure data-hiding, striking a balance between concealment effectiveness and reversibility, mak- ing it suitable for secure communication applica- tions.[7] 8.Traceback for End-to-End Encrypted Messaging: In this paper, Nirvan Tyagi, Ian Miers, and Thomas Ristenpart examine techniques for tracing the origins of messages in end-to-end en- crypted messaging systems. The authors tackle the challenge of ensuring accountability and secu- rity in these systems, where traditional traceback methods often fall short due to encryption. They propose a new framework that facilitates effective traceback without compromising user privacy or the integrity of the encryption. By utilizing cryp- tographic methods, the paper illustrates how to maintain security while allowing for the identifi- cation of malicious actors within encrypted com- munication channels. This work contributes to the overall security and robustness of messaging applications.[8]

9. Security and Imperceptibility Improving of Image Steganography Using Pixel Allocation and Random Function Techniques: In this pa- per, Noor Alhuda Fet Abbas and colleagues present a new approach to enhance the security and imper- ceptibility of image steganography by using pixel allocation and random function techniques. The authors aim to improve data-hiding methods to ensure that secret information embedded within images remains undetectable while still maintain- ing high visual quality. By employing pixel alloca- tion strategies and randomization, their proposed method reduces the likelihood of detection and increases resistance to steganalysis. The results show that this combination of techniques signifi- cantly enhances both the security of hidden data and the imperceptibility of stego- images across various applications.[9]

10. Development of LSB Based Steganography Method for Video and Image Hiding: In this pa- per, N. Kumar, V. Lakhani, K. Singh, M. Bhardwaj, and S. Raj present a novel steganography method based on the LSB technique for hiding informa- tion in both videos and images. The authors focus on enhancing the traditional LSB approach to im- prove the capacity and security of data embedding while preserving the quality of the host media. The proposed method enables effective and efficient data concealment, making it suitable for secure communication applications. The results demon- strate the method's effectiveness in achieving high imperceptibility and robustness against detection, highlighting its potential for practical use in mul- timedia data protection.[10]

11. Autoencoder-Based Image Steganography With Least Significant Bit Replacement: In this paper, Mariam Ibrahim, Ruba Elhafiz, and Haneen Okasha introduce a novel image steganog- raphy method that integrates autoencoders with the LSB replacement technique. This approach uses autoencoders to improve the efficiency of data hiding while preserving the quality of the result- ing stego-image. By embedding secret information through LSB replacement, the method offers a secure and effective way to conceal data within digital images. The incorporation of autoencoders optimizes the steganography process, enhancing both imperceptibility and security, making it suit- able for secure communication across various ap- plications.[11]



#### IV METHODOLOGY

##### LSB Steganography For Cover Images:

In today's world, where everyone is chatting on-line and sharing information constantly, keeping sensitive data safe is extremely important. Digital content is everywhere, and with so many platforms available, ensuring the security of our media files can be quite challenging. However, there's an interesting technique called steganography, which allows us to hide messages in plain sight. This means we can embed information within images or videos without anyone noticing.

**Traceability:** Messaging systems are often used to share misinformation and harmful content, leading to serious issues. While end-to-end encryption protects user privacy, it poses a challenge for effective content moderation and obscures the origins of harmful information. We propose a concept called traceback. This cryptographic approach enables platforms to maintain end-to-end encryption while identifying the sources of harmful content that users report. We define the goals for functionality and security in message traceback. Additionally, we describe two methods: one that reveals a sequence of forwarded messages (known as path traceback) and another that displays the entire forwarding structure (referred to as tree traceback).[8] For a clear understanding of the embedding algorithm, refer to Figure 1.

The system consists of the following components: **Input Image:** The system processes the input image and converts it into an RGB pixel matrix. The text is transformed into binary format, making it suitable for embedding in the LSB of the image.

**LSB Embedding:** The binary text is embedded in the LSB of the RGB pixel values. This process uses a password to securely determine the embedding message.[3][9]

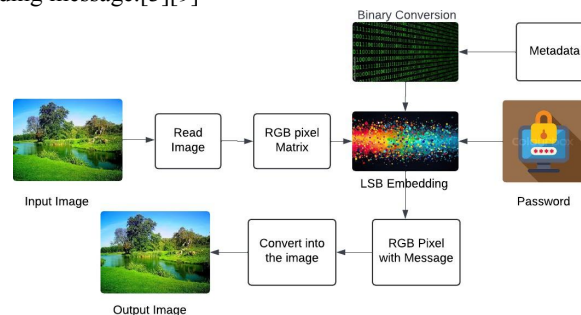


Figure 1: Embedding Algorithm

**Image with Embedded Message:** After embedding the binary message, a new image is created that appears visually identical to the original but contains the concealed message.

**Convert into Image:** The modified pixel matrix is converted back into an image format.[7]

**Trace Footprint:** Unique identifiers (footprints) are embedded or updated as the image is forwarded to trace the history and detect any tampering.

**Message Extraction and Footprint Verification:** The original message can be extracted by reading the password, and the tracing mechanism reveals the image's forwarding history.[2][6]

Now, let's understand the extraction algorithm. To do this, consider the figure2.

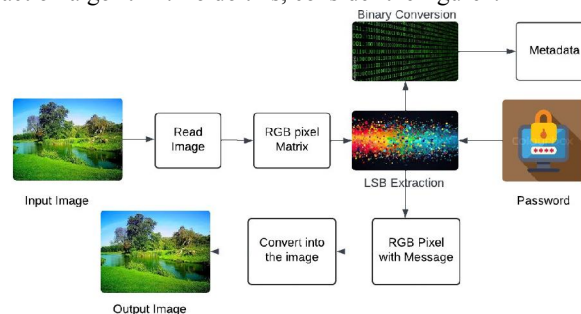


Figure 2: Extraction Algorithm



**Input Image (with Message):** The input image contains the hidden message and is fed into the system. **Read Image:** The image is read and its pixel data is extracted as an RGB pixel matrix.

**Password Input:** A password is used to decode the hidden message by determining which bits in the pixel values contain the message.[3]

**LSB Extraction:** The system extracts the least significant bits from the RGB pixel values based on the password.[3]

**Convert Binary to Text:** The binary data extracted from the LSBs is converted back into its original text form.

**Footprint Verification:** During the process, any unique identifiers (footprints) embedded in the image are checked, allowing the system to trace the image's history and determine where it has been forwarded.

**Reconstruct Image:** After extraction, the image is reconstructed to its original state (without the hidden message), ensuring the integrity of the image is maintained.[7][6]

Images are composed of countless pixels. The more pixels an image has, the higher its quality. Each pixel contributes to the intensity, which creates color in the image. Colors are represented in RGB format, which signifies the blend of red, green, and blue intensities. Each primary color can have values ranging from 0 to 255. Therefore, the color value for each pixel is denoted as a set of intensity values, noted as (R, G, B). For example, there is not much visible difference between colors represented by intensity values (0, 100, 255) and (0, 98, 253). Due to this minimal difference, manipulating the least significant bits (LSB) of the pixel values often goes unnoticed by most people.[11] LSB steganography takes advantage of this principle by replacing the least significant bits of some or all pixels with bits from a secret message. This replacement can involve changing the least significant 1-bit, 2-bits, 3-bits, or even up to 4-bits at a time. However, altering more bits than this may make the differences in the image more apparent compared to the original.[1]

## V. OUTPUT

Step 1 : Login to the app using the app created by us.

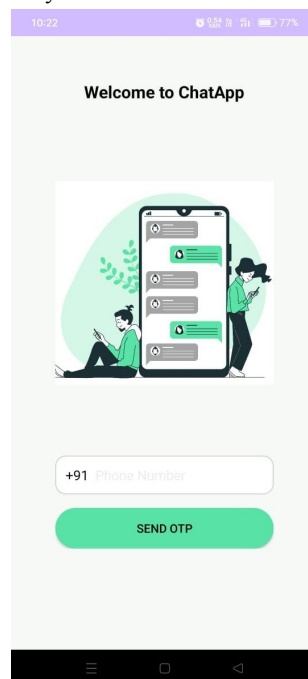


Figure 3: Login Page



**Step 2 :** Verifying the account using an OTP

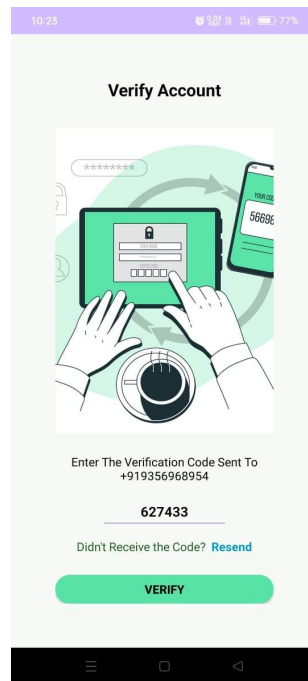


Figure 4: Verification Page Using OTP

**Step 3 :** User interface after log-in

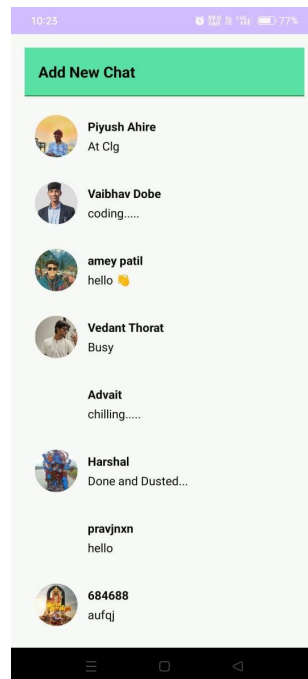


Figure 5: User chat Interface





Step 4 : Sender's interface Page to send the mes- sage

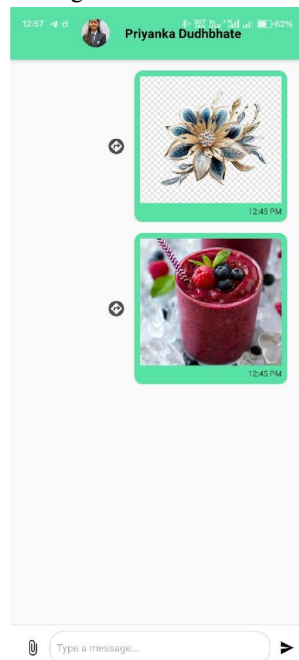


Figure 6: Sender's chat Interface

Step 5 : The receiver's chat interface received the message from the sender.

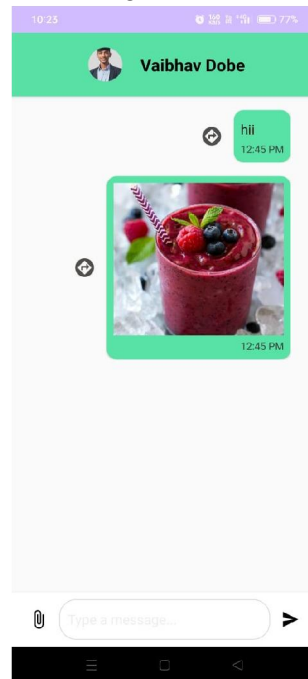


Figure 7: Receiver's chat Interface



Step 6 : To get a detailed analysis of the forwarded image, we need to tap on the image so that it shows us two options:

1) Investigate 2) Delete

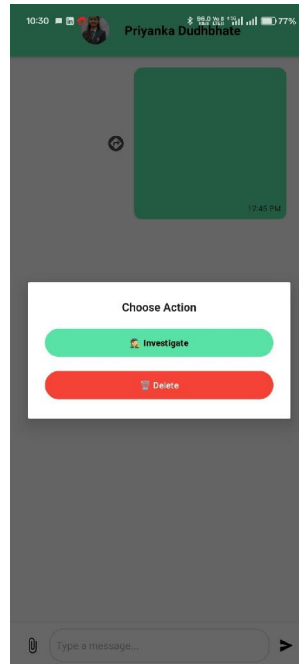


Figure 8: Investigate Image

Step 7 : Here, we need to log in using an OTP that is sent to the database administrator's mobile.

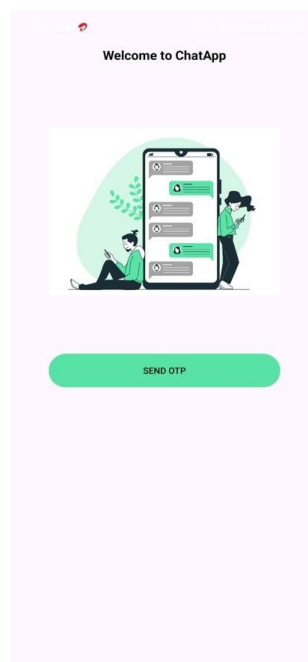


Figure 9: Database Admin Interface





Step 8 : After requesting the users to access the data from the database to check the image origin and who forwarded it. First, it shows database administrator Information.



Figure 10: Database Administrator's Information

Step 9 : After clicking on Investigate, it opens the message in the database and shows all the data of the forwarded message from the origin to the last receiver. Here, all the authorization of the database is handled by the database administrator so that no one can access the data easily or without the user's permission.

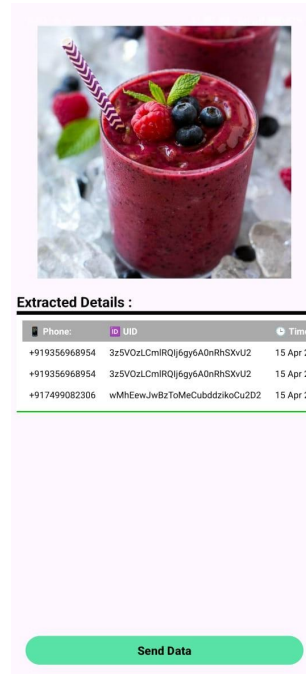


Figure 11: Receiver's Information

DOI: 10.48175/IJAR SCT-27539



## **VI. FEASIBILITY OF ALGORITHM AND SCOPE OF ALGORITHM**

### **6.1 Feasibility of algorithm**

The feasibility of implementing a steganographic metadata embedding technique to trace the origins of images shared on WhatsApp presents both opportunities and challenges. WhatsApp is a widely-used messaging platform that allows users to share images, making it an ideal medium for embedding metadata to track the dissemination and origins of these images. Steganography, which involves hiding information within digital files, could be effectively utilized to embed traceable metadata directly into images shared via WhatsApp, without visibly altering the image quality or raising suspicion. This method could aid in identifying the source of images, tracking distribution patterns, and ensuring authenticity—an approach particularly beneficial for digital forensics, copyright protection, and combating misinformation. However, there are significant challenges to consider. WhatsApp compresses and resizes images during transmission, which may strip or distort any embedded metadata. To address this issue, the steganographic technique would need to be highly robust, specifically designed to withstand the compression algorithms and other transformations applied by the platform.

### **6.2 Scope of Algorithm**

- 1) **Mobile Communication** : Mobile communication involves the transfer of data over wireless networks between mobile devices. This project focuses on how images shared through messaging platforms like WhatsApp, a popular mobile application, can be traced using steganographic techniques. It will explore the embedding of metadata within images sent via WhatsApp to track their origin and distribution path across mobile communication channels. The steganographic method ensures that the tracking data remains hidden and imperceptible to users, thus maintaining privacy while enabling traceability.
- 2) **Social Communication**: Social communication encompasses interactions on platforms like WhatsApp, Facebook, and Instagram. Images play a vital role in communication on these platforms; tracing their distribution can help monitor misuse or unauthorized sharing. This project will investigate how steganography can embed metadata within images shared in social communication to track their journey across different users and groups, facilitating the identification of the source or original sender of an image when necessary.
- 3) **Email Communication**: Images are frequently sent via email for various purposes—professional, personal, or promotional. In this project, embedding metadata steganographically into images sent via email will allow the recipient or other authorized entities to verify the source and ownership of the images. This will help with copyright management, and detecting unauthorized distribution, and tracing the chain of communication from the sender to the recipient, thereby securing email-based image exchanges.
- 4) **Copyright**: Copyright concerns the legal protection of original works such as images, ensuring that only the owner or those with permission can distribute or modify them. In this project, steganographic techniques can be used to embed copyright information (such as ownership details, timestamps, or usage rights) into the image itself. This hidden metadata helps prove ownership, preventing unauthorized usage, and providing evidence in case of disputes related to intellectual property theft or infringement.
- 5) **Ownership**: Ownership involves ensuring that the rightful owner of an image retains control over its distribution and usage. In this project, the steganographically embedded metadata can contain the name or identification of the owner, creation date, or other relevant ownership details. This allows the owner to prove the image's authenticity and origin in case of unauthorized use or distribution, as well as trace the image back to them if it is shared or forwarded without consent.
- 6) **Private Communication**: Private communication involves the exchange of sensitive or personal information that must be kept confidential. WhatsApp images frequently contain such information, making it essential to protect user privacy while also allowing for some level of traceability. In this project, steganography can help ensure that images remain confidential and unaltered, while hidden metadata allows for tracking their movement across private communication channels. This approach strikes a balance between privacy and accountability[5]
- 7) **Discrete Cosine Transform (DCT)**: The Discrete Cosine Transform (DCT) is a mathematical technique commonly used in image compression, particularly in JPEG formats. It divides an image into segments of varying importance. In



steganography, DCT can be utilized to conceal information in the less significant parts of an image, making the embedded metadata, such as traceability information, imperceptible to the human eye while still being extractable when necessary. This project aims to leverage DCT to embed tracking metadata in WhatsApp images, ensuring that the image quality remains intact while allowing the hidden metadata to trace the image's origin and distribution path.

## **VII. ADVANTAGES**

1. **Improved Traceability:** Embedding metadata steganographically into WhatsApp images allows tracking the origin and distribution of an image. This method is beneficial for monitoring the unauthorized spread of sensitive information or copyrighted material.
2. **Preservation of Image Quality:** The steganographic technique, particularly when employing methods like DCT, conceals metadata without significantly degrading the image quality. The human eye is unable to detect the embedded data, preserving the original appearance of the image.
3. **Enhanced Privacy:** The image appears normal to all users while containing important information about its source or ownership. This metadata is concealed, ensuring that user privacy is not compromised and can be accessed when needed.[4]
4. **Digital Rights Management (DRM):** Including copyright and ownership information in images helps protect intellectual property rights. This prevents unauthorized distribution and ensures rightful ownership can be demonstrated if disputes arise.
5. **Increased Accountability:** This system helps identify the origin of images, reducing misinformation and malicious content. It promotes accountability by allowing users or authorities to trace the source of an image.
6. **Supports Multiple Communication Channels:** This method is not exclusive to WhatsApp; it can be adapted for other communication platforms like social media and email, making it versatile for various types of image transmission.
7. **Non-Intrusive Method:** The process of embedding metadata through steganography does not disrupt regular communication for users. It functions in the background without altering user behavior, unlike watermarking, which can be more visually noticeable.

## **VIII. DISADVANTAGES**

1. **Complexity in Extraction:** Embedding metadata is relatively straightforward, but extracting it from images can require specialized tools and software. This limitation can hinder practical usage, especially for non-technical users.
2. **Vulnerability to Image Compression:** When an image is compressed, such as when shared on certain platforms that reduce file size, there's a risk that hidden metadata may be lost or corrupted. Many social media and messaging apps, including WhatsApp, use compression, which can compromise the effectiveness of the embedded data.
3. **Data Storage Limitations:** The amount of data that can be embedded using steganography is limited. Embedding significant amounts of metadata can impact image quality or become technically challenging, which restricts how much tracking information can be concealed.
4. **Potential for Abuse:** Malicious users could employ similar techniques to conceal harmful or illegal information within images, making it challenging to detect without the appropriate tools. This raises concerns about the unethical use of steganography.
5. **Legal and Ethical Concerns:** Embedding traceability information without user consent may raise ethical concerns, especially regarding privacy. Users might be uncomfortable with metadata embedded in shared images, even if it is for tracking purposes.
6. **Platform Compatibility Issues:** The system's effectiveness may hinge on platform-specific behaviors. For example, if WhatsApp or other platforms alter their compression algorithms or image handling protocols, the embedded metadata might become unreadable or may be removed during transmission.
7. **Resource Intensive:** Maintaining a steganographic tracking system is resource-intensive, demanding substantial computational power for data embedding and extraction. Custom tools or software may also be necessary for detection and tracing.



### IX CONCLUSION

This algorithm explores steganography, LSB method to boost the tracking responsibility of messages sent through popular encrypted apps like WhatsApp. By hiding metadata in images, we tackle big problems. These include misinformation, unauthorized changes to content, privacy issues-without affecting the key benefits of end-to-end (E2E) encryption. This work highlights how important steganography is for modern digital communication challenges. By placing traceable metadata in images, we find a real way to improve accountability and fight against harmful content while still protecting privacy and security through E2E encryption. As more digital interactions happen every day, using such clever methods will be vital in creating a secure, open, trustworthy communication space.

### REFERENCES

1. Ashish Kumar Verma, Shruti and Tiyas Sarkar, "Utilizing Imaging Steganographic Improvement using LSB Image Decoder," International Conference on Communication, Computer Sciences and Engineering (IC3SE), pp. 1-7, (2024).
2. I. Shukla, A. Joshi and S. Girmé, "LSB Steganography Mechanism to Hide Texts Within Images Backed with Layers of Encryption," International Conference on Security of Information and Networks (SIN), Jaipur, India, pp. 1-6, (2023).
3. Gupta, Shailender, Ankur Goyal, and Bharat Bhushan, "Information hiding using least significant bit steganography and cryptography," International Journal of Modern Education and Computer Science (IJMECS), pp. 1-8, (2020)
4. DK Sarmah, AJ Kulkarni, A Abraham, DK Sarmah, AJ Kulkarni, A Abraham, "Cryptography and digital image steganography techniques," Optimization Models in Steganography Using Meta-heuristics (2020).
5. Rahman, Shahid, Fahad Masood, Wajid Ullah Khan, Niamat Ullah, F. Qudus Khan, Georgios Tsaramirsis, Sadeeq Jan, and Majid Ashraf, "Novel Approach of Image Steganography for Secure Communication Based on LSB Substitution technique," Computers, Materials Continua 64, no. 1, pp. 31-61, (2020).
6. S. Pramanik, D. Samanta, SK Bandyopadhyay, R. Ghosh, "A new combinational technique in image steganography," International Journal of Information Security and Privacy (IJISP) 15.3, pp.2-19 (2021).
7. Kuyoro, Afolashade, Uchenna J. Nzenwata, Oludele Awodele, Sunday Idowu, "GAN-Based Encoding Model for Reversible Image Steganography," Revue d'Intelligence Artificielle 36, no. 4, pp. 1-7 (2022).
8. Nirvan Tyagi, Ian Miers, and Thomas Ristenpart, "Traceback for End to-End Encrypted Messaging," ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1-19, (2019).
9. Noor Alhuda F. Abbas, Nida Abdulredha, Khalid Ibrahim, Adnan Hussein Ali, "Security and imperceptibility improving of image steganography using pixel allocation and random function techniques," International Journal of Electrical Computer Engineering (IJECE), pp. 1-12, (2022).
10. N. Kumar, V. Lakhani, K. Singh, M. Bhardwaj, S. Raj, "Development of LSB Based Steganography Method for Video and Image hiding," International Conference on Reliability Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 1-6, (2024).
11. Ibrahim, Mariam, Ruba Elhafiz, and Haneen Okasha, "Autoencoder-Based Image Steganography With Least Significant Bit Replacement." 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp.1-6, (2024)

