Secret communication using steganography and cryptography

1st Madhu V H
Department of Electronics and Communication Engineering
Alva's Institute of Engineering and Technology
Moodbidri, India
vhmadhu2003@gmail.com

2nd Manjunath Choori
Department of Electronics and Communication Engineering
Alva's Institute of Engineering and Technology
Moodbidri, India
manjunathchoori28@gmail.com

3rd Netra S K
Department of Electronics and Communication Engineering
Alva's Institute of Engineering and Technology
Moodbidri, India
netrakurbet22@gmail.com

4th Nireeksha G M
Department of Electronics and Communication Engineering
Alva's Institute of Engineering and Technology
Moodbidri, India
nireekshasihi25@gmail.com

5th Dr. Ganesh V N
Department of Electronics and Communication Engineering
Alva's Institute of Engineering and Technology
Moodbidri, India
ganeshvn@aietgmail.com

***Abstract*—Steganography refers to the method of hiding data of any kind in digital media in order to transmit the information in a way that only the receiver knows and hence, secure communication is maintained.**

A simple yet effective steganographic system for images based on the Least Significant Bit (LSB) method and an elementary XOR-based scrambling technique has been presented in this study. Abstract—Steganography refers to the method of hiding data of any kind in digital media in order to transmit the information in a way that only the receiver knows and hence, secure communication is maintained. The system enables both text data and image data to be embedded in a cover image and thus has broader usage in various situation communications. A numeric password is utilized to generate key-dependent scrambling operations such that only users with possession of the correct password would receive the embedded data. The experimental findings confirm that there is no alteration in the visual quality of the original cover image after embedding and that the password protection system adds an extra layer of access control.Being straightforward in approach keeps it highly computational light and amenable for implementation in real time, though limitations and directions for future work enhancing it by integrating advanced cryptography as well as machine learning are duly pointed out.

I. Introduction

A. *Introduction*

As online communication has grown at extremely high speed, privacy about sensitive data has become essential.

Though cryptography protects data by rendering them unreadable, it still indicates the passage of hidden information. Steganography never signals transmission of information by concealing it in daily media such as images, audio, or videos. Among these steganographic schemes, image steganography has been widely studied due to redundancy in images and its covert nature [23]

Least Significant Bit (LSB) method is among popular steganographic schemes owing to simplicity in

implementation and minimal visual loss. Only pixel value bits in least significance are replaced in order to hide secret data without noticeable change in the cover image. However, basic LSB schemes lack strong security since attackers would get extracted data if no other type of security is utilized. With this in mind, different schemes generally require password encryption or any other form of encryption followed by LSB embedding.

A password-based LSB-based steganographic system in Python is outlined in the work. The system supports text-in-image and image-in-image steganography. A numeric password via XOR scramble is adopted to provide maximum secrecy such that only legitimate users will uncover the covert data. The approach is lightweight, efficient, and preserves good quality of original covering image and is therefore suitable for secure communication in resource-limited settings.

B. Overview of the Project

With the help of steganography, this project offers an easy, lightweight, and unnoticeable method of concealing secret messages in pictures—a technique that hides data in images without detection by anyone. The traditional Least Significant Bit (LSB) method is used which changes the slightest details of the pixel colors in an image to conceal the data, and a password scramble is incorporated for additional security. The whole thing is done in Python with the user-friendly Pillow library, and two major functions are provided: embedding secret text in an ordinary picture or even concealing an entire image inside another.

During the process of encoding (hidden), the user selects a regular "cover" picture along with the secret like a text message or another photo. A numerical password is entered which encrypts the data using a fast XOR operation (it is like a reversible mix that can only be undone by the correct key). The resultant bits are then hidden in the pixels of the cover image that are least perceptible. What is produced? A concept has been coined as the steganogram—a digital image so well disguised that nothing about it seems to suggest that there is actually something concealed in the file.

II. LITERATURE REVIEW

Johnson et al. [1] explore the steganography technique for digital content, putting emphasis on the processes of secret data transmission and intellectual property protection. Their paper presents a comprehensive examination of various attack scenarios and their allied countermeasures aimed at raising the concealed data's toughness against being detected, corrupted, or lost.By the way of theoretical principles and practical implementations together, they are designing secure data hiding techniques that are reliable. On the whole, it is a good source for the researchers working on building algorithms that are not only security-wise strong but also performance-wise upgraded for different kinds of digital media across the board of both steganography and watermarking systems.

Gonzalez et al. [2] provide a very comprehensive account of the principles, algorithms, and applications of digital image processing. Among others, the authors present the major topics of image enhancement, restoration, segmentation, and compression that are of utmost importance for the image steganography process, keeping the same order. The book is not only aimed at mathematicians who want to see the basic principles in numbers but also at practitioners who wish to acquire the techniques. Hence, they will be able to handle the image data for the purposes of hiding and retrieving the content no matter which method is used. This paper serves as a vital reference in the quest for the design of high-performance and fast image steganography systems that would be suitable for both research and commercial use.

Paar et al. [3] present a thorough explanation of modern cryptographic techniques, which covering the symmetric and asymmetric encryption, while hashing methods, and key management protocols. The textbook describes the mathematical concepts and their applications in the field of cryptography, at the same time, providing important information on how to protect data during embedding transmission in steganography. The

authors illustrate the process of cryptographic algorithms providing confidentiality and integrity, thus, making this publication a significant source for securely combining cryptography with steganography systems.

Fridrich et al. [4] present a thorough investigation on digital media steganography, which encompasses main concepts, algorithms, and practical applications in the real world.The different methods analyzed by the authors include data entry or hiding (using watermarking techniques), detection via steganalysis, and techniques to secure against attacks and to manage attacks. The writers discuss the whole range of spatial and frequency domain techniques but mainly concentrate on three main aspects: capacity of the payload, invisibility, and resistance to statistical analysis. Thus, the work provides a fair evaluation of steganography's usage from both the defensive and offensive perspectives in various digital media formats.

Katzenbeisser et al. [5] explore the modern techniques for hiding information, focusing on steganography and watermarking. The authors' research effectively integrates theoretical notions with practical uses, pointing out security and robustness as the major defenses against different attacks. They tell the story of the designs of the algorithms, the processes of embedding and the tactics of detection, thereby providing a complete picture of how to protect digital content.. The said method allows scholars to tackle the technical and security problems in information hiding at the same time, thereby creating the possibility of even stronger and more secure methods in the area of multimedia security.

Kessler et al. [6] examines steganographic techniques from the perspective of computer forensic investigators, outlining detection and steganalysis strategies. The challenges of revealing concealed messages in digital data, the application of forensic software, and the legal aspects are all major topics of the discussion in the paper. To that end, it mentions the various ways of practicing steganalysis, such as through signature and statistical detection methods. This advisory gives practitioners the power to identify hidden messages with ease and at the same time comprehend the metamorphosing character of steganography in legal probes.

Cox et al. [7] provide a detailed study of digital watermarking for media authentication and copy protection. The authors discuss the application of spread spectrum methods and strong watermarking systems capable of defeating distortion and tampering as the major subjects of their work. Through such a combination, the book not only explores the theory of perceptual modeling and detection protocols but also reveals the potentials in practice. Therefore, it is a practical low-cost guide for the researchers working on watermarking systems that also use steganography to secure the integrity of the content in electronic communications.

Srivastava et al. [8] propose an efficient image steganography approach using LSB schemes combined with password protection for added security. The technique used by them hides the data inside the digital pictures by encrypting the payload and allowing only those who know the password to access it. The tests have shown that it combines high imperceptibility and strong resistance against the extraction of data. Moreover, it provides a proper compromise between simplicity and security, which makes it an efficient method for secure steganographic exchange of messages.

The Python Software Foundation [9] provides comprehensive documentation for the Python Imaging Library (Pillow), which makes image manipulation the techniques essential to the steganography well-detailed and accessible. The library provides methods for the creation, alteration, and transformation of images thereby allowing the effective handling and management of images in different applications of steganography. Its detailed functions aid in data hiding encoding, decoding, as well as data visualization in images. It is the resource on which developers and researchers relying on practical steganography algorithms develop applications for non-technical users.

III. CONCLUSION

The proposed system consists of a dual-mode image steganography and password protection mechanism that is secure enough to conceal both images and texts within the cover images. The method used for data security is a combination of XOR encryption with LSB substitution which leads to data confidentiality, authenticity, and imperceptibility. The system is designed for secure communication and is both practical and user-friendly since it has GUI and command-line interfaces.

Prospects for further improvement include the integration of more secure encryption schemes such as AES adaptive embedding schemes that would allow for better steganalysis resilience and higher data capability, and the extension of the system to deal with multimedia beyond images and developing software for phones, for wider portability. More reinforcement of the system could also come from the incorporation of machine learning-based resist mechanisms as well as detection mechanisms. Possible future extensions include temporal steganography for videotext for wider multimedia applications.

REFERENCES

1. Johnson, N. F., Duric, Z., & Jajodia, S., *Information Hiding: Steganography and Watermarking - Attacks and Countermeasures*, Springer, 2001.
2. Gonzalez, R. C., & Woods, R. E., *Digital Image Processing*, 4th Edition, Pearson, 2018.
3. Paar, C., & Pelzl, J., *Understanding Cryptography*, Springer, 2009.
4. Fridrich, J., *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge University Press, 2009.
5. Katzenbeisser, S., & Petitcolas, F. A., *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, 2000.
6. Kessler, G. C., "An Overview of Steganography for the Computer Forensic Examiner," *Digital Investigation*, 1(3), 1-12, 2000.
7. Cox, I. J., Miller, M. L., & Bloom, J. A., *Digital Watermarking*, Morgan Kaufmann, 2001.
8. Srivastava, A. K., & Bharti, R., "An Efficient Approach to Image Steganography Based on LSB with Password Protection," *Int. J. of Computer Sciences and Engineering*, 2025.
9. The Python Software Foundation, *Python Imaging Library (Pillow) Documentation*, https://pillow.readthedocs.io/en/stable/

Biographies

Name : Manjunath Choori
USN : 4AL22EC046
Email : manjunathchoori28@gmail.com
Mobile : 7760575047

Areas of Interest: He is currently pursuing a Bachelor's degree in Electronics and Communication Engineering at Alva's Institute of Engineering and Technology (AIET), affiliated with Visvesvaraya Technological University (VTU) in Karnataka. His academic journey reflects a strong interest in core and emerging electronics domains such as PCB Desing, Embedded Systems, VLSI Design, Digital Signal Processing (DSP), Microcontrollers and Semiconductor Devices.

Name : MADHU V H
USN : 4AL22EC039
Email : vhmadhu2003@gmail.com
Mobile : 8792300725
Areas of Interest: She is currently pursuing a Bachelor's degree in Electronics and Communication Engineering at Alva's Institute of Engineering and Technology (AIET), affiliated with Visvesvaraya Technological University (VTU) in Karnataka. Her academic journey reflects a strong interest in core and emerging electronics domains such as PCB Desing, Embedded Systems, VLSI Design, Digital Signal Processing (DSP), Microcontrollers and Semiconductor Devices.

Name : Netra S K
USN : 4AL23EC053
Email : netrakurbet22@gmail.com
Mobile : 8618881931
Areas of Interest: She is currently pursuing a Bachelor's degree in Electronics and Communication Engineering at Alva's Institute of Engineering and Technology (AIET), affiliated with Visvesvaraya Technological University (VTU) in Karnataka. Her academic journey reflects a strong interest in core and emerging electronics domains such as Embedded Systems, VLSI Design, Digital Signal Processing (DSP), Microcontrollers , Wireless Communication and Semiconductor Devices.

Name : Nireeksha G M
USN : 4AL22EC054
Email : nireekshasihi25@gmail.com
Mobile : 7411196619
Areas of Interest: She is currently pursuing a Bachelor's degree in Electronics and Communication Engineering at Alva's Institute of Engineering and Technology (AIET), affiliated with Visvesvaraya Technological University (VTU) in Karnataka. Her academic journey reflects a strong interest in core and emerging electronics domains such as Embedded Systems, VLSI Design, Digital Signal Processing (DSP), Microcontrollers ,Wireless Communication and Semiconductor Devices.

Name : Dr. Ganesha V N
Designation : Associate Professor (Project Guide)
Email ID : ganeshavn@aiet.org.in
Mobile Number : 9880101926
Areas of Interest : As a Associate professor in the Department of Electronics and Communication Engineering at Alva’s Institute of Engineering and Technology (AIET), affiliated with Visvesvaraya Technological University (VTU) in Karnataka.