IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 14, May 2023

Steganography: Concealing Information within Images using GUI-based Application

Bhavesh Jha[1], Vibhav Kumar Dubey[2], Ajay Rai[3]

Students, Department of Computer Science and Engineering[1,2,3]

Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh, India

Abstract: *Steganography is a captivating method used to conceal sensitive data within seemingly harmless information, like images, audio files, or videos. This research paper introduces a Java-based graphical user interface (GUI) application for steganography, implemented using the Swing framework. The application enables users to hide messages or files within images and retrieve them later, offering a seamless and user-friendly experience. The paper delves into the underlying technology and algorithms employed in steganography, as well as the notable features and functionality of the developed GUI application. Experimental results effectively demonstrate the application's efficiency and effectiveness in concealing and retrieving information while preserving the integrity of the carrier image. The research emphasizes the practical applications of steganography and the importance of user-centric interfaces in enhancing the accessibility and usability of cryptographic techniques.*

Keywords*:* Steganography, Cryptography, Invisibility, Undetectability, Confidentiality

I. INTRODUCTION

Steganography is an approach employed to conceal confidential information within seemingly ordinary files, such as images or audio. It enables individuals to transmit messages discreetly, without arousing suspicion. Unlike encryption, which alters the content to render it incomprehensible, steganography conceals the actual message itself.

The following are the objectives of the project:

- Images: Image formats like JPEG, PNG, or BMP are frequently utilized in steganography. Due to the substantial presence of redundant data in images, they are well-suited for concealing supplementary information without significantly compromising the visual quality.
- Cover objects: Cover objects are the media files used as carriers for concealed data in steganography. Steganography can be applied to different digital media formats, including images, audio files, videos, and text documents. Each type of cover object presents unique strengths and challenges regarding embedding capacity, robustness, and perceptual transparency. The selection of a cover object depends on the specific needs and goals of the steganographic application.Audio files: Audio steganography involves hiding secret messages within audio signals. Techniques like modifying the least significant bits of audio samples or exploiting inaudible frequency ranges can be used for embedding.
- Videos: Video steganography involves using video frames as cover objects. Similar to images, videos possess a substantial amount of redundant data, which can be leveraged to conceal confidential information.
- Text documents: Text files can also be subjected to steganography by modifying specific elements or employing encoding techniques to conceal information within the text itself

Work Related Steganography

Steganography, derived from the Greek term "covered writing," refers to the practice of concealing information within other forms of data, such as text, images, or audio files, in a manner that remains imperceptible to casual observation. Various steganographic techniques exist for hiding data, depending on the chosen carriers.

DOI: 10.48175/568

Both steganography and cryptography serve the purpose of secure data transmission. Steganography shares similarities with cryptography, employing concepts like encryption, decryption, and secret keys. However, unlike cryptography, steganography maintains the original content of the message without altering it throughout the process.

Steganography supports multiple digital formats that can be used as carriers for hiding data. These formats are commonly referred to as carriers, and the selection depends on the redundancy of the chosen object. Redundancy involves using additional bits to enhance the accuracy of the displayed object.

The primary file formats employed in steganography include text, images, audio, video, and protocol files. Various types of steganographic techniques are available, including pure steganography, public key steganography, and secret key steganography. The different types of steganographic techniques that is available are

- Puresteganography
- Public key steganography
- Secret key steganography

II. LITERATURE SURVEY

Information Security - Security generally refers to the quality or state of being protected from danger. In the context of information security, different layers are defined based on the type of content to be secured:

1. Physical security: This layer focuses on protecting physical data or objects from unauthorized intrusion.
2. Personal security: It pertains to the security of individuals who are officially authorized to access information about the company and its operations.
3. Operational security: This layer emphasizes the protection of information related to specific operations within a chain of activities.
4. Communication security: It encompasses security issues concerning an organization's communication media, technology, and content.
5. Network security: This layer is responsible for safeguarding information related to networking components, connections, and content.

Information security, as a whole, entails the protection of information, as well as the systems and hardware that utilize, store, and transmit that information. It encompasses measures adopted to prevent unauthorized use, modification, or access to data or capabilities.

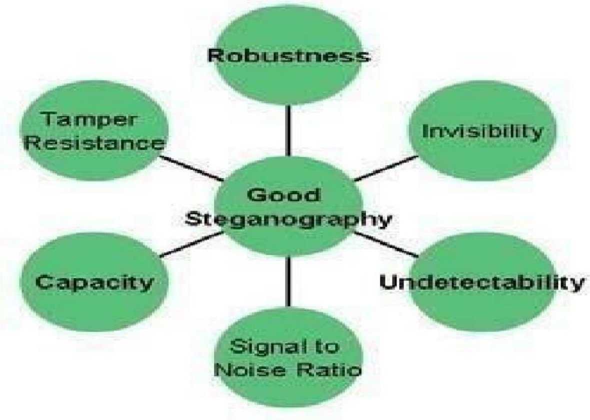
The main objective of this project is to propose a method and critically discuss the properties that facilitate the transmission of data or information over a network without any modifications. The critical characteristics of information include:

1. Availability: Ensuring that authorized users have uninterrupted access to information in the required format. It involves verifying user access rights to prevent unauthorized disclosure.
2. Accuracy: Referring to the absence of mistakes or errors in the information. Accurate information meets the expectations of end users and avoids intentional or unintentional modifications.
3. Authenticity: Signifying the genuineness or originality of information, not a reproduction or fabrication of previously known data. Authenticity ensures that information remains unmodified and retains its original state.
4. Confidentiality: Protecting information from unauthorized disclosure or exposure to individuals or systems. Confidentiality ensures privacy and secrecy of personal or organizational data, limiting access to those with proper rights and privileges.
5. Integrity: The quality of being whole, complete, and uncorrupted. Information integrity is compromised when it suffers from corruption, damage, destruction, or disruptions to its authentic state caused by intended or unintended sources.

By addressing these properties, information security aims to safeguard data and maintain its confidentiality, availability, accuracy, authenticity, and integrity.

Security Attacks: Data is typically transmitted from a source to a destination in its normal flow, as depicted in the figure. However, hackers may attempt to breach the network to gain unauthorized access or modify the original data. These malicious activities are referred to as security attacks. Various approaches exist to prevent such security attacks, with the most commonly used ones being. The most useful approaches are

- Cryptography
- Steganography
- Digital watermarking



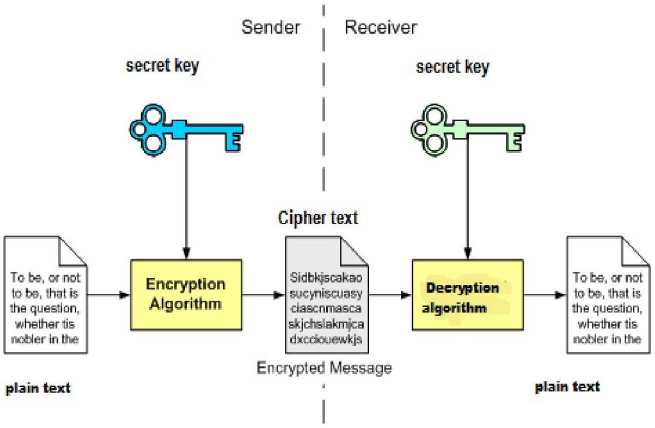
The term "cryptography" originates from two Greek words that mean "secret writing." Cryptography involves the process of scrambling the original text through rearrangement and substitution, transforming it into a seemingly unreadable format for unauthorized individuals. It serves as an effective method to protect transmitted information within network communications.

Cryptology, on the other hand, is the scientific field that encompasses both cryptography and cryptanalysis. Cryptography focuses on securely and confidentially sending messages to their intended destinations, while cryptanalysis involves the methods used to decipher hidden messages within original texts.

In general, cryptography involves the alteration of data from its source to its destination through the use of a secret code. Cryptosystems utilize plaintext as input and generate ciphertext using encryption algorithms, which require a secret key as input.

The important elements in cryptosystems are

- Plaintext(input)
- Encryption algorithm
- Secret key
- Ciphertext
- Decryption


Sender
Receiver
secret key
secret key
Cipher text
To be, or not to be, that is the question, whether tis nobler in the
Encryption Algorithm
Sidbkjscakao sucyniscuasy ciascnmasca skjchslakmjca dxcciouewkjs
Decryption algorithm
To be, or not to be, that is the question, whether tis nobler in the
Encrypted Message
plain text
plain text

DOI: 10.48175/568

Steganography, derived from the Greek term "covered writing," refers to the practice of concealing information within other forms of data, such as text, images, or audio files, in a manner that remains imperceptible to casual observation. Various steganographic techniques exist for hiding data, depending on the chosen carriers.

Steganography and cryptography are both employed for secure data transmission. They share similar approaches, including encryption, decryption, and the use of secret keys. However, in steganography, the message is kept secret without any visible changes, while cryptography involves altering the original content of the message through encryption and decryption stages.

Steganography supports different digital formats that can be used as carriers for hiding data. These formats are known as carriers, and the choice depends on the redundancy of the selected object. Redundancy involves using additional bits to enhance the accuracy of the displayed object.

The main file formats used in steganography include text, images, audio, video, and protocol files. These formats provide different levels of redundancy and suitability for steganographic techniques.

The different types of steganographic techniques that is available are

- Puresteganography
- Public key steganography
- Secret key steganography

Digital watermarking is the practice of fitting information into a digital signal, similar as an image, videotape, or audio train. Its primary ideal is to guard the integrity and authenticity of digital media. Through digital watermarking, a unique identifier or watermark, associated with the proprietor, is directly bedded into the host signal. The purpose of bedding the watermark in such a way is to make it challenging for hackers to remove it without significantly demeaning the quality of the signal or image. By using digital watermarks, power of specific means, similar as images, vids, and audio lines, can be demonstrated and vindicated. They serve as a form of evidence of authorization and act as a hand to indicate power.

III. RESULTS AND DISCUSSION

All approaches to steganography have a fundamental similarity: they involve hiding a secret message within a physical object that is being transmitted. The process of steganography can be illustrated through the depicted figure, which shows the cover image being inputted into the embedding function along with the message to be encoded. This results in a steganography image that contains the hidden message. To protect the hidden message, a key is often utilized. This key, typically in the form of a password, is used to both encrypt and decrypt the message before and after embedding it.

IV. CONCLUSION

The Java-based project "Steganography" successfully fulfills the organization's requirements. Its primary objective is to protect data resources and programs from accidental or intentional destruction, modification, or unauthorized disclosure. The system prioritizes user-friendliness, providing a convenient and interactive interface that simplifies the data security process for authorized users.

Developing this software has been a valuable learning experience for me, allowing me to expand my knowledge in the software field. I am pleased with the system's ability to meet all the specified requirements. The project has been thoroughly developed and deployed, adhering to the user's requirements and maintaining a bug-free status based on implemented testing standards.

Any errors or issues that may arise and go unnoticed will be addressed in future versions of the software, which are planned for development in the near future. Currently, the system does not incorporate lower-level check constraints for accessing file types in distributed environments. This aspect will be considered and addressed in future upgrades.

In its present state, the developed project is well-equipped to handle the central file system of an organization on a server, granting user access with varying privileges as specified in the password file by higher

REFERENCES

[1]. Chan,C.K.Cheng,L.M.,2004.Hidingdatainimagesbysimplelsbsubstitution:patternrecognition.vol37. Pergamon.

[2]. Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the DiscreteWavelets Transform and Singular Value Decomposition, European Journal Of ScientificResearch,vol39(1), pp 231-239

[3]. Amirthanjan,R.Akila,R&Deepikachowdavarapu,P.,2010.AComparativeAnalysisofImageSteganography,InternationalJournalofComputerApplication,2(3),pp.2-10.

[4]. Arnold,M.2000.Audiowatermarking:Features,applicationsandalgorithms,ProceedingoftheIEEEInternationalConferenceonMultimediaandExpo,pp1013-1016.

[5]. Bandyopadhyay,S.K.,2010.AnAlternativeApproachofSteganographyUsingReferenceImage.InternationalJournalofAdvancementsinTechnology,1(1),pp.05-11.

[6]. Bloom,J. A. et al.,2008. Digital watermarking and Steganography. 2nd ed. MorganKaufmann.

[7]. Bishop,M.,2005.Introductiontocomputersecurity.1sted.Pearsonpublications.Cachin, C., 2004. Information: Theoretic model for steganography. Work shop on informationhiding,USA.

[8]. Cox, I. Miller, M. Bloom, J. Fridrich, J & Kalker, T. 2008. Digital watermarking andSteganography. 2nd Ed. Elsevier. David, W. (2004) Managing information:IT for Businesspurpose.3rd edn, pgno. 215,Elsevier.

[9]. Hellman, M.E., 2002. An overview of public key cryptography. IEEE communicationmagazine.

[10]. JeffreyA,Bloometal.,2008.Digitalwatermarkingandsteganography,2ndedn,MorganKaufmannpublications.