IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁒ Peer-reviewed & Refereed journal ⁒ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13668

IMAGE STEGANOGRAPHY IN ORDER TO AVOID TO CYBER CRIME USING LSB TECHNIQUE

Tejaswini M

Guest Lecturer, Department of CSE, Govt. Home Science College Hassan, Karnataka, India

Abstract: Image steganography is a sophisticated method of hiding information within digital images to prevent unauthorized access and protect sensitive data. This abstract explores the use of the Least Significant Bit (LSB) technique in image steganography as a means to combat cybercrime by ensuring data confidentiality and security.

Cybercrime presents a significant threat to information security, with increasing instances of data breaches, identity theft, and unauthorized access to sensitive information. Image steganography offers a promising solution by embedding hidden messages within digital images, thereby obscuring the presence of the information from potential attackers. The LSB technique is one of the most effective and widely used methods for this purpose.

Keywords: LSB, Terror, al-Qaida, HTML, CSS**.**

I. INTRODUCTION

This is a Software Project developed to provide the transfer of secret message embedded in the image data, to obtain new data , practically indistinguishable from the data by people, in such a way that an eavesdropper cannot detect the presence of hidden information. In this modern era, technology has played an important role in advancing communication. The rise of smart phones, internet, cloud, and other advanced technologies has kept people more connected. Consequently, this also imposes threat on the security of data being sent over networks. Keeping data secure has become a major concern. Cryptography and steganography are well-known methods of data security. Steganography is generally known as the art of hiding information. It is the science of hiding information in seemingly innocent objects in a way that the hidden information is imperceptible to human eyes. Steganography is used to protect the privacy and authenticity of hidden data in concealed communication Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether forcing people to study other methods of secure information transfer. Businesses have also started to realise the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit . After the overview it briefly reflects on the suitability of various image steganography techniques for various applications. This reflection is based on a set of criteria that we have identified for image steganography. The remainder of the paper is structured as follows: Section 2 gives the reader an overview of steganography in general and differentiates between different kinds of steganography. In section 3 the most popular algorithms for image steganography are discussed and compared in section 4. In Section 5 a conclusion is reached.

II. PROJECT DESCRIPTION

Purpose:

The aim of the project is to hide information in undetectable way both perceptually and statistically and also to provide security, prevent extraction of the hidden information

MOTIVATION

The primary reason for selecting steganography among the list of possible project topics was due to the unfamiliarity of the word that twigged an interest in the subject. Another motivation for researching the topic was after reading an online article in the USA Today titled “Terror groups hide behind Web encryption” that claims terrorists and, in particular, Osama bin Laden and the al-Qaida network, may be using steganography to communicate with each other in planning terrorist attacks.

DOI: 10.17148/IJARCCE.2024.13668

OBJECTIVE

In this project we primarily concentrated on the data security issues when sending the data over the network using steganographic techniques. The main objectives of our project are to product security tool based on steganography techniques to hided message carried by stego-media which should not be sensible to human beings and avoid drawing suspicion to the existence of hidden message. and to avoid the cybercrime and to maintain the sensitive information in an image.

HTML Hypertext Markup Language (HTML) is the standard markup language for creating web pages and web applications. With Cascading Style Sheets (CSS) and JavaScript, it forms a triad of cornerstone technologies for the World Wide Web. Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document. HTML elements are the building blocks of HTML pages. With HTML constructs, images and other objects such as interactive forms may be embedded into the rendered page. HTML provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. HTML elements are delineated by tags, written using angle brackets. Tags such as directly introduce content into the page. Other tags such as surround and provide information about document text and may include other tags as sub-elements. Browsers do not display the HTML tags, but use them to interpret the content of the page.

CSS Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a mark up language like HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript. CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple web pages to share formatting by specifying the relevant CSS in a separate .css file, and reduce complexity and repetition in the structural content. Separation of formatting and content also makes it feasible to present the same markup page in different styles for different rendering methods, such as on-screen, in print, by voice (via speech based browser or screen reader), and on Braille-based tactile devices. CSS also has rules for alternate formatting if the content is accessed on a mobile device.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

There are many approaches to hide the secret data and exchange between two authorised persons.

➢ The one among the common practice is cryptography.

➢ The cryptography is technique where a normal text is encoded or a normal text is converted to a non readable format which also uses some key technique to encrypt and decrypt.

➢ This encrypted data or non readable format data is exchanged over a network between two authorised persons.

➢ Meanwhile when the data is sent over the network it makes the sense that a secret message is being transferred, hence which invokes the data hackers to capture the data and try to decrypt which is a crime.

➢ The data hackers can easily understand that the secret message is being shared and the hackers try to predict the key and the secret message is exposed on successful decryption.

➢ Many encryption techniques are used to make data more secure and un hack able.

PROPOSED SYSTEM

The purpose of Steganography is to maintain secret communication between two parties. Unlike cryptography, which conceals the contents of a secret message, steganography conceals the very fact that a message is communicated. Although steganography differs from cryptography, there are many analogies between the two, and some authors classify steganography as a form of cryptography since hidden communication is a type of secret message. The data is hidden in the image and the data is also encrypted hence exchanging the stegnography picture makes casual feel the its an normal image exchange. The system reduces the risk of data explosion and maintains the data secret. Steganography works have been carried out on different transmission media like images, video, text, or audio.

Input Image

Output Image

ADVANTAGES:

Up to now, cryptography has always had its ultimate role in protecting the secrecy between the sender and the intended receiver. However, nowadays steganography techniques are used increasingly besides cryptography to add more protective layers to the hidden data. The advantage of using steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

IV. REQUIREMENTS

SOFTWARE REQUIREMENT SPECIFICATION

Software Requirement Specification is the starting point of the software development activity. It includes an introduction that gives the purpose, scope and an overview of the system. This needs requirement by talking to the people and understanding their needs. It also includes a general description of the product perspective, product function and certain user characteristics of the system. It also specifies the overall functional requirements, performance requirements and design constraints. The SRS is a means of translating the idea in the mind of the clients (the input), into a formal document (the output of the requirement phase). The Software Requirement Specification document is organized in such a manner it aids validation and system design.

SOFTWARE REQUIREMENTS

- Operating system
- Programming language
- IDE

HARDWARE REQUIREMENT

- Hard disk
- Ram
- Monitor

V. SYSTEM DESIGN

System design is concerned with how the system functionality is to be provided by different components of the system. The design process establishes overall system architecture. Software design involves representing the software system functions in a form that may be transformed into one or more programs. The requirement specified by the end user has to be put in a systematical way.

Any design problem must be tackled in three stages:

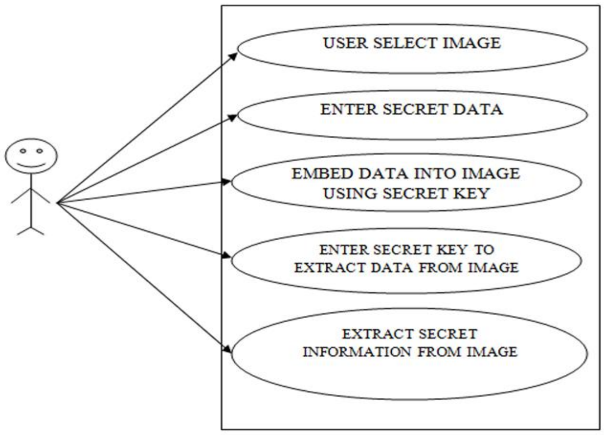
DOI: 10.17148/IJARCCE.2024.13668

• Study and understand the problem: The problem should be examined from a number of viewpoints as these provide different insights into design requirements.
• Identify the gross features of at least one possible solution: It is often used to identify a number of solutions and to evaluate them all. The choice of solution depends upon the designer's experience, the availability of reusable components and simplicity of derived solutions.
• Describe each abstraction used in the solution: Before creating formal documentation an informal design description may be analyzed by developing it in detail.

SYSTEM ARCHITECTURE:

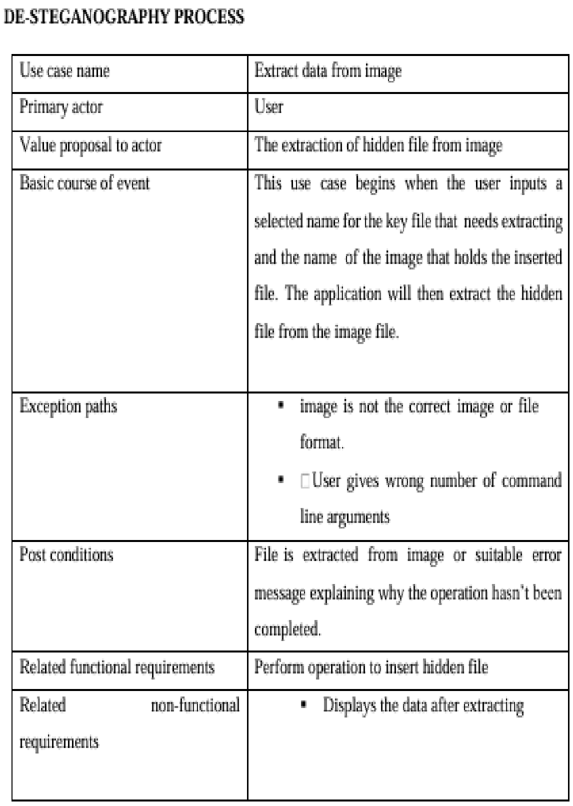
The activities in this process are:
• Partition requirements: During this phase, the requirements are analyzed and collected into related groups.
• Identify sub-system: This activity is concerned with identifying different sub-systems that can, individually
• Assign requirements to sub-systems: In this requirements are assigned to sub-systems. In principle, this should be Straight forward if the requirement partitioning is used to drive the sub-system identification.
• Specify sub-system functionality: This may be seen a part of the system design phase or, if the sub-system is a software system part of requirements specification activity for that system.
• Define sub-system interfaces: This critical activity involves defining the interfaces that are provided and expected by each sub-system. Once these interfaces have been agreed, parallel development of the sub-systems becomes possible.

VI. USE CASE DIAGRAM


USER SELECT IMAGE
ENTER SECRET DATA
EMBED DATA INTO IMAGE USING SECRET KEY
ENTER SECRET KEY TO EXTRACT DATA FROM IMAGE
EXTRACT SECRET INFORMATION FROM IMAGE

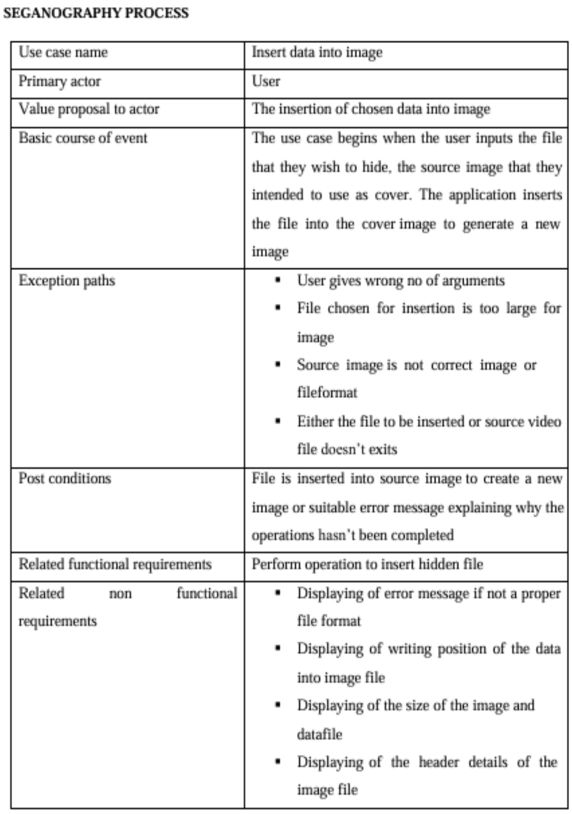
It is that a third person watching the communication between the sender and the receiver will not be able to find out whether the sender has been active, and when, in the sense that he really embedded a message in the cover-text. In other words, stego texts should be indistinguishable from cove texts. System Feasibility The proposed system can be developed using the present hardware and software technologies. The project requires following requirements. Hardware and software architecture with minimum requirements, which supports an operating system on which Java toolkit and Media player applications can be developed and deployed. The estimated time given to different phases in the project such as Analysis, Design, implementation and testing all sum up to make a total time required to complete the project as approximately equal to 2 months (Excluding future Enhancement).

VII. PROCESS



DE-STEGANOGRAPHY PROCESS

Use case name	Extract data from image
Primary actor	User
Value proposal to actor	The extraction of hidden file from image
Basic course of event	This use case begins when the user inputs a selected name for the key file that needs extracting and the name of the image that holds the inserted file. The application will then extract the hidden file from the image file.
Exception paths	▪ image is not the correct image or file format. ▪ User gives wrong number of command line arguments
Post conditions	File is extracted from image or suitable error message explaining why the operation hasn't been completed.
Related functional requirements	Perform operation to insert hidden file
Related non-functional requirements	▪ Displays the data after extracting



SEGANOGRAPHY PROCESS

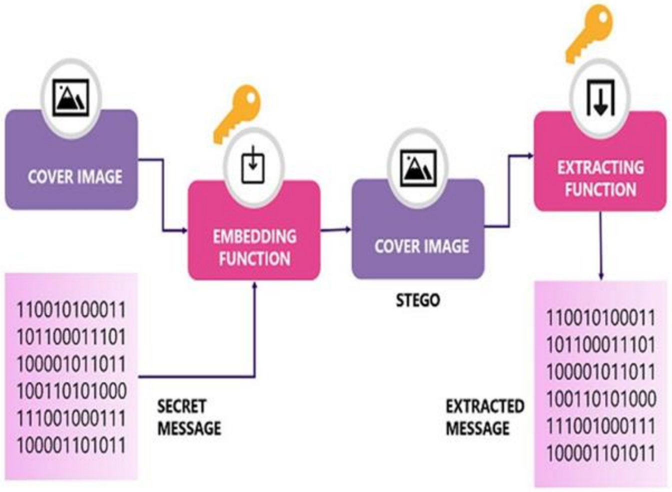
Use case name	Insert data into image
Primary actor	User
Value proposal to actor	The insertion of chosen data into image
Basic course of event	The use case begins when the user inputs the file that they wish to hide, the source image that they intended to use as cover. The application inserts the file into the cover image to generate a new image
Exception paths	▪ User gives wrong no of arguments ▪ File chosen for insertion is too large for image ▪ Source image is not correct image or fileformat ▪ Either the file to be inserted or source video file doesn't exits
Post conditions	File is inserted into source image to create a new image or suitable error message explaining why the operations hasn't been completed
Related functional requirements	Perform operation to insert hidden file
Related non functional requirements	▪ Displaying of error message if not a proper file format ▪ Displaying of writing position of the data into image file ▪ Displaying of the size of the image and datafile ▪ Displaying of the header details of the image file

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product.

It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

Steganography Activity Diagram



DOI: 10.17148/IJARCCE.2024.13668

VIII. IMPLEMENTATION

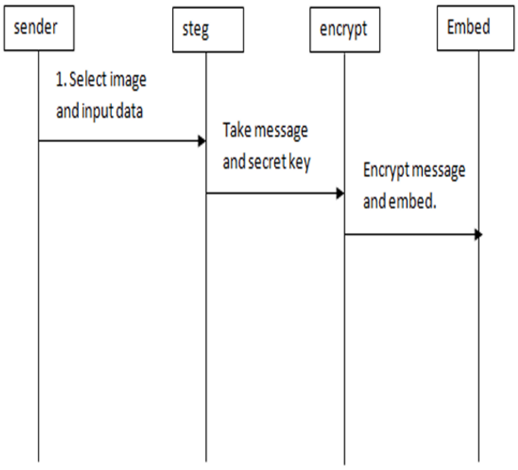
Steganography The basic algorithm and the functional flowchart for the steganography process are shown below. Algorithm for steganography

Step 1: Create separate classes for the image file headers, for example RIFF(Resource Interchange File Format), image main header, image stream header, audio, bitmap.
Step 2: Get the input files through the graphical user interface.
Step 3: Check the number of argument if it is not equal to 2 display error and exit else go to step 4.
Step 4: Assign the image file name to image and text file name to txt. (image & txt are constructor variables)
Step 5: Open the image file using File Input stream and get the size of the imagefile
Step 6: If (size of image file < (size of text file *8)) print "cannot continue" and exit else step 7.
Step 7: Read the file in terms of bytes corresponding to the size of the headers and check first 4 bytes for RIFF and next 4 bytes for chunk ID and next 4 bytes for image. If RIFF and image not found, display not a valid image file and exit else continue.

To do list the check parameters

Step 8: Read the RIFF, image main header, image Stream header, Bitmap Info header, Wave format Header and image Index structures through the class object from the video file and display them.
Step 9: Using do-while loop find the starting part of the data in the image file. For example after reading all the header information read the file by, byte by byte up to finding the letter ‘L’ and read the next 3 bytes then compare with “LIST” if it is equal do the same operation for finding “movi”. After finding movi skip 8 bytes to find the starting position of data.
Step10: Create a key file using Output DataStream and write the content of the image file starting from the data to the end.
Step 11: Close all the files. Step 12: Open the text file using Random Access File and read the file then get the size of the file.
Step 13: Read the text file through byte by byte and convert every single byte into corresponding binary number.
Step 14: Convert each bit of the binary equivalent into a separate byte and store it in a separate array named var. temp [], as 1 is 1 and zero is 2.
Step 15: close the text file.
Step 16: Again open the image file and a new file named temp file text in read Write mode using Random Access File.
Step 17: Place the file pointer to the starting point if the data using seek ().
Step 18: Read the data content of the image file and also the data stored in the var. temp[] array in byte by byte.
Step 19: If (b [0]==255 || b [0]==254) minus the data stored in var. temp[] array with data content of the image file otherwise add the data. Do this up to the last byte of the var. temp[] array.
Step 20: Result of the step 16 is over writed to the data part of the image file as well writted into the newly created file temp_file.txt.
Step 21: Close all the files that are opened .
Step 22: Exit

Flow chart for function Steganography


sender
steg
encrypt
Embed
1. Select image and input data
Take message and secret key
Encrypt message and embed.

DOI: 10.17148/IJARCCE.2024.13668

IX. CONCLUSION

Steganography process can be used for hide a secret message within a image file. Steganography process is done by using the Least Significant Bit Algorithm using an AVI file and the text file. In the de-steganography process the reverse Least Significant Bit algorithm is done to extract the data from the AVI file and the keyfile. This is useful method since intruder won’t be having any knowledge about the data hidden in the image and even though he finds then he needs the key file to regenerate the data which is embedded in the image file. The image file can be chosen which has less color in it preferably grayscale, since the human eye can’t make out the change in the image. The steganography process is useful when exchanging data between two parties in a peaceful and personal conversation. This is useful to exchange the key in different protocols in the network between the user and the server. The main disadvantage of this process is that it can also be misused by the terrorist for doing their illegal business and trading.

REFERENCES

[1]. INFOSYSSEC. Cryptography, Encryption and Stenography.
[2]. [Online] 2000. Available at http://www.infosyssec.org/infosyssec/cry2.htm;
[3]. Wikipedia - The Free Encyclopedia. Steganography. [Online] 2004 June.
[4]. Available at http://en.wikipedia.org/wiki/Steganography; Wikipedia - The Free Encyclopedia. Stego text. [Online] 2004 June.
[5]. Available at http://en.wikipedia.org/wiki/Stegotext; Plunt. Steganography (hide and seek) Tutorial. [online] Astalavista Group. 2004 January. Available at http://www.astalavista.com//data/hide_and_seek.txt; Johnson, N. F., Duric, Z., Jajodia, S.
[6]. Information Hiding: Steganography and Watermarking - Attacks and Countermeasures. Kluwer Academic Press. Norwell, MA, New York, The Hague, London, 2000. Johnson, N. F., Jajodia, S.
[7]. Exploring Steganography: Seeing the Unseen. [online] 1998 February. Available at http://www.jjtc.com/pub/r2026.pdf; Accessed on 24 June 2004. Rude, T. J.
[8]. Steganography - Disappearing Cryptography. [online] CRAZYTRAIN.COM 2000. Available at http://www.crazytrain.com/rudedude.pps; 8. Haldar, V. Steganography and Audio. [online] Available at http://www.ics.uci.edu/~lopes/teaching/280ubicompW03/students%20presentations/v ivek%20haldar.pdf;