International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012

http://www.ijcsjournal.com Volume 10, Issue 1, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-418 PAGE NO: 2820-2822

Secure Data Transfer Over Internet using Image Steganography

Pavithra N[#1], Mr. N. Ganapathiram[*2]

[#]*Student, B.Sc Computer Science, Rathinam College of Arts and Science,*
Coimbatore, Tamil Nadu, India -641021
pavithra6025@gmail.com

[*]*Assistant Professor, Department of Computer Science,*
Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021
ganapathiram.cs@rathinam.in

***Abstract* -** Steganography is the technique of hiding private or sensitive information within something that appears to be nothing is a usual image. Steganography involves hiding Text so it appears that to be a normal image or other file. If a person views that object which has hidden information inside, he or she will have no idea that there is any secret information. What steganography essentially does is exploit human perception; human senses are not trained to look for files that have information inside of them. What this system does is, it lets user to send text as secrete message inside an image file, user uploads the image and enters the text to send secretly, and gives a key or a pass word to lock the text, what this key does is it encrypts the text, so that even if it is hacked by hacker, he will not be able to read the text. You will need the key to decrypt the hidden text. User then sends the image and key to the receiver and receiver first opens the image, and then he enters the key or password for decryption of text, he then presses decrypt key to get secret text of the sender. By using this method, you can double ensure that your secret message is sent secretly without outside interference of hackers or crackers. If sender sends this image in public others will not know, what is it, and it will be received by receiver.

***Index Terms* –** Steganography, Private, Public key, Secret Text, Hackers.

I. INTRODUCTION

Steganography comes from the Greek Steganography (covered or secret) and -graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds. The first steganography technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography which involved: shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, and sending the slave on his way to deliver the message.

II. SYSTEM DEVELOPMENT

LIMITATIONS:

There are various approaches for information and data security to achieve secret communication. There are many existing works related to steganography, which includes audio steganography. The existing methods were used LSB (Least Significant Bit) technique for hiding secret data. But the least bit stganography is always can be detected and not much protected. Due to this problem, image steganogaphy failed in many applications. Another problem of the existing technique is the quality of the image can leak the hidden information in the image.

TRUMP CARD:

In the proposed system a fresh unique scheme of data hiding images is presented with random bit selection, where the application select image as a carrier medium and select random pixels RBS which is abbreviated as random block steganography to hide the data rather than the sequence least bit. Using the proposed system, the secret data can be embedded in the image without quality degrades. The data owner selects the original text content and embeds the data into the images using standard randomized ciphers with hash keys to produce the stego images.

INGREDIENT:

Modules are units of code written in access basic language. We can write and use module to automate and customize the database in very sophisticated ways.

1. Image selection and frame extraction
2. Encryption
3. Data embedding module:
4. Extraction of original data and decryption process
5. Image selection and frame extraction

Initially the user should select a image file format, after the selection the image will be converted into set of frames using frame grabber technique. After the frame extraction the data will be embedded into the frames. Image compression uses modern coding techniques to reduce redundancy in image data.

Encryption

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Original message is hidden within a carrier such that the changes occurred in the carrier are not observable. The information about the private key is used to encrypt the text. The text message will be encrypted and embedded into the frames.

Data Embedding Module

The Image steganography composed of two main phases namely extraction of image files and embedding of secret message, as the secret message is already encrypted using AES it can be easily embedded into carrier image randomly using RBS.The extraction of all frame again convert into image making this file more robust The steganography file generated is then transmitted over the communication channel which remains intact as a result of this complex data hiding method.

Extraction of original data and decryption process

Decryption is the process of converting encrypted data back into its original form, so it can be understood. When the user inputs the correct key that is used at the decryption process, this will extract the original message that is encrypted and embedded.

III. EVALUATION METHODS

The different types of testing are:-

1. Unit Testing
2. Integration Testing
3. Validation Testing
4. Output Testing
5. User Acceptance Testing

Unit Testing

Unit testing focuses verification efforts on the smallest unit of software design, the module. This is also known as "Module Testing" The modules are tested separately this testing is carried out during programming stage itself. In this step each module is found to be working satisfaction as regard to the expected output from the module.

Integration Testing

Integration testing focuses on the design and construction of the software architecture. Data can be lost across an interface, one module can have adverse effect on another sub functions and show on. Thus integration testing is a systematic technique for constructing test to uncover errors associated with in the interface. In this project, all the modules are companied and then the entire program is tested as a whole.

Validation Testing

Validation testing is the requirement established as a part of software requirement analysis is validated against the software that has been constructed. This test provides the final assurance whether the software needs all functional, behavioral and performance requirements. Thus the proposed system under consideration has been tested by using validation testing and found to be working satisfactory.

Output Testing

After performing the validation testing, the next step is the output testing of the proposed system, since no system could be useful if it does not produce required output in the specific format. Tested asking the users about the format required by them, the output is considered into two ways: one is on the screen and the other is printed format.

The output format on the screen is found to be correct as the format designed according to the user needs, for the hard copy also, the output comes as specified by the user. Hence output testing does not result in correction in the system.

Whitebox Testing

White box Testing is done with the project which drive test cases that do the following

1. Guarantee that all the independent paths with in modules have been exercise at least once.
2. Exercise all logical decision on the true and false side.
3. Execute all loops at the boundaries and within their operation bounds.
4. Exercise internal data structures to ensure the validity
5. It is aimed at ensuring that the system works accurately and efficiently before live operation command.

Blackbox Testing

Black box System methods focus on the functional requirement of the software. Using the black box testing method the following errors are identified and rectified in the package.

1. Incorrect or Missing functions
2. Interface Errors
3. Errors in data Structures or external database access.

User Acceptance Testing

User acceptance testing of a system is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keep in touch with the prospective system user at time of developing and making changes wherever required.

IV. SYSTEM IMPLEMENTATION

In this project, propose virtualizing Harvard architecture on top of the existing memory architecture of modern computers, including those without non-executable memory page support, so as to prevent the injection of malicious code entirely. Harvard architecture is simply one wherein code and data are stored separately. Data cannot be loaded as code and vice-versa. In essence, we create an environment where in any code injected by an attacker into a process' address space cannot even be addressed by the processor for execution. In this way, we are attacking the code injection problem at its root by regarding the injected malicious code as data and making it un addressable to the processor during an instruction fetch. Split memory architecture produces an address space where data cannot be fetched by the processor for execution. For an attacker attempting a code injection, this will prevent him from fetching and executing any injected code.

V. CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Image file Steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at Steganography to circumvent such policies and pass messages covertly. Although the algorithm presented is a simple one and not without its drawbacks, it represents a significant improvement over simplistic steganography algorithms that do not use keys. By using this algorithm, two parties can be communicated with a fairly high level of confidence about the communication not being detected. In designing the "Steganography" utmost care was taken to meet user requirements as much as possible. The analysis and design phase was reviewed. Care was taken strictly to follow the software engineering concepts. And principles so as to maintain good quality in the developed system as per the user requirements.

REFEERENCES

[1] Rajendran S, Doraipandian M. "Chaotic map based random image steganography using lsb technique," IJ Network Security. 2017;19:593-598.

[2] Ismael HR, Ameen SY, Kak SF, Yasin HM, Ibrahim IM, Ahmed AM, et al. "Reliable Communications for Vehicular Networks," Asian Journal of Research in Computer Science. 2021;33-49.

[3] A. Khaldi, "Steganographic Techniques Classification According to Image Format," International Annals of Science. 2020;8: 143-149.

[4] Abdullah RM, Ameen SY, Ahmed DM, Kak SF, Yasin HM, Ibrahim IM. et al. "Paralinguistic Speech Processing: An Overview," Asian Journal of Research in Computer Science. 2021;34-46.

[5] Haref QM, Taha MS, M. Rahim MS, Hashim MM, Ahmad AMB. Rifa'i, Categorization of spatial domain techniques in image steganography: A revisit," Journal of Advanced Research in Dynamical and Control Systems. 2021;10: 1538-1551.