Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY
Full Length Article

Image Steganography

Dr.V.R.Sadasivam [a], R.Abishake[b], R.Tamilarasan[b]

[a] *Professor, Department of Information Technology, K.S. Rangasamy College of Technology, Nammakal, Tamilnadu, India*
[b] *Student, Department of Information Technology, K.S. Rangasamy College of Technology, Nammakal, Tamilnadu, India*

***Corresponding Author**

(Dr.V.R.Sadasivam)
Tel.: +91

ABSTRACT: Steganography is the process of hiding users secret message within a cover image that someone cannot know the presence or contents of the encoded message. The purpose of Steganography is to provide secret communication between two users. This paper will explain how Image Steganography is used in today's world and provide practical or realtime understanding of what Steganography is and how to use it. Image Steganography is mostly used in securing high tech informations and user privacy. Private security and anonymity is a concern for most people on the internet. Image Steganography allows for two users to communicate secretly and covertly. It is difficult to find secret message and methods used to hide data.It allows for copyright protection on media files using the secret message as a digital watermark.The other main uses for Image Steganography is for the transportation of top secret or high level documents and files between international governments. While Image Steganography has many other uses.Image Stegangography can be used to send viruses and trojans by hackers or terrorists to compromise machinesand other organizations data that rely on covert operations to communicate safely and secretly.

Keywords: Image Stegnography, DES Cryptography, LSB Algorithm.

1 Introduction

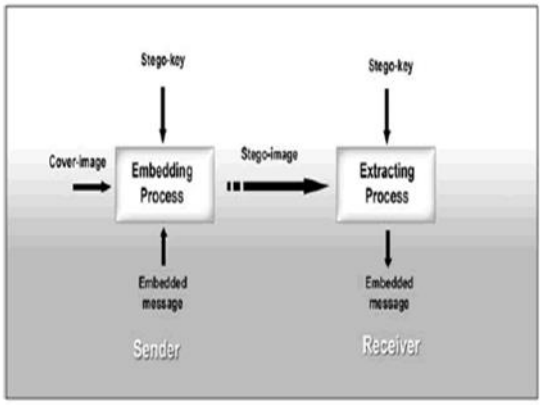
The rapid development of modern technology provides high-speed and economic communication worldwide. With innovation of new technologies security threats are also growing rapidly. Security is the primary requirement of a communication from international communication to personal communication. A technique which only secures the content of messages like cryptography increases the chanceof compromising the security. But Steganography is the process to hide the fact that communication is taking place. It is the simplest way to encode the communicating messages because if attacker is unaware about the communication the chances of attacks are automatically decreased.

The term used in Steganography are: stego image, cover image, secure message and stegonalysis. Encrypted message is the message which we want to keep secure. Cover image is the carrier image which contains encrypted message. So the stego image is that cover image which is going to be transferred with a encrypted message. Web based Image Steganography application enables secret communication between sender and receiver to send message or share data anywhere at any time. It is a platform independent and more dynamic. Sender encrypts the message with private key before sending. Receiver decrypts the message with sender's private key.The private which is used for encryption is shared between sender and receiver only. Third party or any intruders cannot access the private key.

2. Steganography& Cryptography

Steganography differs from cryptography

- **Steganography** Hide the messages inside the Cover medium,many Carrier formats.
- Breaking of steganography is known as Steganalysis.
- **Cryptography** Encrypt the message before sending to the destination no need of carrier/cover medium.
- Breaking of cryptography is known as Cryptanalysis.



3. Objectives of the Project

The project is carried out with the following objectives

- To hide the message or a secret data into an image which acts as a cover medium using LSB technique and pseudo random technique.
- The primary motivation of my current work is to increase PSNR of the stego image(peak signal to noise ratio).

4. Scope of the Work

- Scope of this project is to create a web application which would help to create a secure transmission of data between sender and receiver through a web domain.
- Steganography is the technique of hiding private or sensitive information within something that appears to be nothing be 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 press 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

5. Literature Review and Related Work

Mustafa Cem Kasapbasi & Wisam Elmasry (April 2018), Steganography is the technique for hiding information within a carrier file so that it is imperceptible for unauthorized parties. In this study, it is intended to combine many techniques to gather a new method for colour image steganography to obtain enhanced efficiency, attain increased payload capacity, posses integrity check and security with cryptography at the same time. Proposed work supports many different formats as payload. In the proposed method, the codeword is firstly formed with secret data and its CRC-32 checksum, then the codeword is compressed by Gzip just before encrypting it by AES, and it is finally added to encrypted header information for further process and then embedded into the cover image. Embedding the encrypted data and header information process utilizes Fisher-Yates Shuffle algorithm for selecting next pixel location. To hide one byte, different LSB (least significant bits) of all colour channels of the selected pixel is exploited. In order to evaluate the proposed method, comparative performance tests are carried out against different spatial image steganographic techniques using some of the well-known image quality metrics. For security analysis, histogram, enhanced LSB and Chi-square analyses are carried out. The results indicate that with the proposed method has an improved payload capacity, security and integrity check for common problems of simple LSB method. Moreover, it has been shown that the proposed method increases the visual quality of the stego image when compared to other studied methods, and makes the secret message difficult to be discovered.

Mohammad Tahghighi Sharabyan, Hamid Ghorbani(January 2018) Today, with the growing expansion of information and communication technology,the world, through digital data, is moving to the digital world and communications. Meanwhile, the role of internet as a public communication channel is becoming more and more important in the world of communication

every day. In addition, maintaining security and creating confidential communications are of particular importance regarding the general structure of this communication channel. Cryptography and information steganography are two important issues in security systems. Both encryption and steganography techniques are not effective for high security information alone, but combining these two methods can greatly improve the confidentiality and security of confidential information. Recently, new hybrid algorithms have been proposed using cryptography and steganography. However, in these methods, attempts have been made to increase the security of censorship by using random factors and hidden keys, most of these methods are broken by examining the statistical components of the images. In this paper, a high-security hybrid approach is proposed to digital images steganography based on the Imperialist Competitive Algorithm and Symmetric Cryptography Algorithm. The proposed method, by considering the Imperialist Competitive Algorithm, creates a high quality, high-security image. Prior to data insertion, symmetric encryption of information takes place, and then encrypted information is embedded in the cover image. The results of the implementation of the proposed method show that in addition to enhancing the image quality of the steganography, it is more secure than other methods.

Danny Adiyan Z, Tito Waluyo Purboyo and Ratna Astuti Nugrahaeni (June 2018),Image Files are one of the most widely used file types today. This paper describes the use of JPEG image files in Steganography. Steganography is the technique of hiding a message in an image file (cover image) so as not to be known by people who do not have permission to access. This insertion utilizes the smallest bit of pixel units in an image file (Least Significant Bit). In this journal, steganography will be combined with vigenere cipher. Steganography utilizes the weakness of the human eye in viewing the image file, steganography also uses mathematical calculations in inserting messages into the image file. This type of insertion uses the binary of the ASCII code of a character. This paper also compare the size of an image file to the size of the information that can be inserted.

6. Existing Systems

Numerous Steganographic software tools are available on the internet today. The basic idea related to these different tools is the same : to create a steganographic softwarer that can hide image or text in another medium. Existing softwares namely S-Tools, VSL, OpenPuff, CryptaPix and Quick Crypto.

- S-Tools uses images or Audio files to hide datas. This has an Action Window that shows the users what steps are being carried out by the software.
- VSL uses LSB technique to apply steganography and also uses more advanced encoding techniques like Karhunen-Loeve Transform technique.
- OpenPuff makes use of carrier chains by dividing the data into carrier chains andthen hiding data.Image,Audio,Videoand PDF files can be hidden.
- CryptaPix performs image editing such asresizing,rotating,croppingand removing red eye from images.
- Quick Crypto includes encryption of files,E-mails,password.It usesAES,Triple DES and Blowfish.

6.1 Drawbacks of Existing Systems

- The main drawback of the above systems are its portability, they are created to serve two users at different computers with separate software for encryption and decryption.
- Both end users should have an application program to encrypt or decrypt.
- The system requirements should be met in order to perform the operation.
- These softwares are platform dependent and are capable of encrypting few data formats.

7. Proposed System

- In this web application a user can encrypt and decrypt the message anywhere at any time.
- For better security DES cryptography technique has also been used in the proposed method. Before applying the Steganography technique,DES cryptography will change the secret message into cipher text to ensure two layer security of the message.
- In the proposed technique, a new Steganography technique is being developed to hide large data in image. This method is an improvement of LSB method for hiding information in images.

7.1 Advantages of Proposed System

- It is web based application therefore it is platform independant.

- Provide better PSNR values as compared to other methods.
- Deciphering the text is not possible so it is more secure.
- It provide better user interface and it has private account system.
- This sytem has an additional layer of encryption for the text.

8. Module Description

Registration:

To access the core system, user first need to register themselves by providing required details.

Login:

After registration, user may login into the system.

Algorithm Selection:

Here, user will select the algorithm such as DES (Data Encryption Standard), AES (Advance Encryption Standard) or LSB (Least Significant Bit) for encrypting data into image file.

Image Selection:

Here, User selects an image for sending a secret message.

Entering Text:

Here, User enter/inputs the text that is to be hidden in the image

.

Setting Password and Encrypting the Data:

User sets a password and use the encryption technique to encrypt the data.

Sharing:

After hiding the text with the encryption technique, user saves the image then sends it to the other party i.e. Receiver.

9 Conclusions

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be more safe and secure. In future there are several directions with this method improve the capacity and PSNR value. The combination of both the technique provided secret message can be secured by two security layers. In addition to this we added the web based service hence there are many opportunities of improvement and there are many ways to improve the webpage and to create a best mode of communication through Internet.The use of image steganography will become more and more common in near future and this is an important application to create a better future.

References

[1] Islam, M. R., Siddiqa, A., Uddin, M. P., Mandal, A. K., & Hossain, M. D. (2014). An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. 2014 International Conference on Informatics, Electronics & Vision (ICIEV).

[2] Philjon, J. T., & Rao, N. V. (2011). Metamorphic cryptography — A paradox between cryptography and steganography using dynamic encryption. 2011 International Conference on Recent Trends in Information Technology (ICRTIT).

[3] Jose, J. A., & Titus, G. (2013). Data hiding using motion histogram. 2013 International Conference on Computer Communication and Informatics.

[4] Dagar, S. (2014). Highly randomized image steganography using secret keys. International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014).

[5] Rubab, S., & Younus, M. (2012). Improved Image Steganography Technique for Colored Images using Wavelet Transform. International Journal of Computer Applications.
Vol 39–No.14.