International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 174 - 180

Secured Data Communication using Steganography

Aliyu Haruna Ahmad
Department of Computer Science
Faculty of Science and Humanity, SRM University
Chennai India
aliyuharunaahmad@gmail.com

G.Kalpana
Assistant Professor
Department of Computer Science
Faculty of Science and Humanities, SRM University
Chennai, India
srmkalpana@gmail.com

***Abstract*—** Secured data communication is highly needed in today's communication media like internet due to vulnerable of confidential resource in a network which can be easily hack. This reason makes the researchers and other users to start research in order to have good techniques which will improve the security of any confidential resource in a network; one of the techniques is steganography. The main contributions of this paper are to design and implement an application that will embed the secret information in an image by using LSB. This approach is the simplest and straight forward in steganography technique. Due to the redundant pixel in image the embedding secret information in a LSB of cover image will not change the stego image in such a way that can easily detected as stego image. The copyright control is added, this will improve the security of stego image by providing stego key which will help to control in controlling copyright. The communication can be carryout with this secured technique because the small changes in LSB of image pixel will make the cover image and stego image no difference. Even if the image is detected, the copyright control prevents the unauthorized user (third party) from accessing secret information. With this method the communication security is improved.

Keywords- *Steganogaraphy, Stego-Image, Stego-Key, Cover Image, LSB, Hiding Infoemation, Secret Message, Secret File, Security, Embed, Retrieve.*

*****

I. INTRODUCTION

Internet is one of the popular channels used for communication nowadays. However, message transmissions over the Internet still have to face many problems, such as data security, copyright control, data integrity, etc [1]. Because of this there is need for secure secret communication methods for transmitting message over the Internet. The main techniques uses for securing data available are Encryption and Steganography methods. Encryption is one of the well-known methods for security protection, which refers to the process of encoding secret information in such a way that only the person with the right key can successfully decode it [6]. But this method makes the message unreadable and making message suspicious enough to attract third-party's attention. The other technique is Steganography, which is use to hide the secret information behind a cover so that it draws no special attention.

Steganography is sometimes confused with cryptography. Both are used to protect information but steganography is concerned with concealing information thereby making it unseen while cryptography is concerned with encrypting information thereby making it unreadable. [3].

Research in steganography has started growing due to lack of strength in cryptographic systems to secure information.

B. Various Methods of Digital Steganography

Most of the digital file formats can be used as a medium for steganography, but the file formats with high degree of redundancy are more suitable. Redundancy can be defined as the bits of an object that provide accuracy per greater than the necessary for the object's use and display. The redundant bits are those bits that can be altered without the alteration being detected easily in an object. The image and audio files are complied with this requirement. Figure below

Becouse of security many governments create a laws which will limited the strength of cryptographic system, some they prohibited it altogether, this reason forcing people to started research in order to find other ways to secure information transfer. Even the businesses have started understanding the important of steganography in secret trade communication and exchanging idea about new product. By using new methods of communication channels like steganography, the risk of information to be vulnerable in transmission is reduces [2]. Hiding information in a photograph of the company picnic is less suspicious then communicating an encrypted file.

II. STEGANOGRAPHY

Steganography is a technique use to hide information in a media in such a way that the third party cannot detect the present of information in the media. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [2, 7] defining it as "covered writing". In image steganography the information is hidden exclusively in side images.

A. Component of a Steganographic

- Secret message.
- Cover data.
- Stego message.

show the file formats available for using digital steganography..

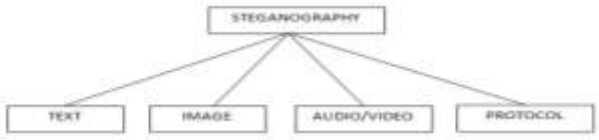

Fig 2. Various Steganography menthods

- *Text Steganography method*, in this method the text is used as a medium (cover). It used text file to hide the secret information in a text. In olden days before internet and other digital file formats become active, this method is the most popular technique to concealed data [4].
- *Image Steganograph method*, now days, this method is the most popular and widely used in secured communication using steganography. The digital image is used to hide secret information and transmitted it across the communication channels media. [4].
- *Audio Steganography method* is another type of stegaraphy medium. In this method the secret information is hidden in an audio file. The audio file is a cover file of steganography. Some format support this technique includes WAVE, MIDI, AVI, and so on [4].
- *Video Steganography method* is also another type of steganography medium. In this method the secret data is conceals in video file. Some format support this technique are AVI, H.264, Mp4, MPEG, etc. [4].
- *Protocol Steganograph*, in this type of technique, the secret data is hided in TCP/IP header packet. The TCP/IP header packet contains some optional fields which can take some information [4].

C. Steganographic Techniques

In this paper we are going to see the image steganography. Digital image steganography techniques is categories into domains, which are as follows [8]:

- Spatial Domain Techniques

  This is one of the categories of domain in steganography. In this category many different versions are available. In any version, some of the bits in digital image pixel values are charged in order to hide the data. The simplest technique used to hide the data in image file in steganography is Least significant bit (LSB), in which the pixel values of LSB are replaced with secret bits of information without introducing much perceptible distortions. The hidden secret information can be done in two ways, sequentially or randomly. In this domain there are different techniques which includes differencing, LSB replacement/substitution, LSB matching, matrix embedding and pixel value etc [4].

- Transform Domain Techniques

  This is another technique use to hide data in an image file. It is one of the complex techniques in steganography. Many algorithms are used in this domain in order to hide data behind image [5]. This technique also called as a domain of embedding techniques. The technique is the most strong technique use by steganography, because most of the strong steganographic systems are using this technique. The transform domains are more useful than the spatial because it embed data in an image pixels that will tolerate some image alteration like cropping, compression and so on [4].

- Distortion Techniques

  This is type of technique that works with principle of differences between the original image and the stego-image. To embed data in image in this technique, the encoder will add the changes in the cover image sequentially. The distortion of the difference images (cover and stego images) need to be considered. Before encode the data, the encoder will chooses the pixels in cover image in order to change their bits in a such a way that statistical properties of cover image will not be effected. However, these techniques are very powerful, because they kept track both cover and stego images, but there are some disadvantages: Can't support nested cover image and can easily attack by tempering the stego-image by cropping, scaling or rotating the stego-image [4].

- Masking and Filtering

  This technique is similar with paper watermark technique. In this technique information is get hidden by marking an image for that purpose it uses the noise levels of the cover images [4].

D. Problem Definition

The aim of steganography is to avoid drawing suspicion to the existence of a hidden data. This approach of data hiding technique has recently become important in a many application areas. One of the popular technique uses in steganography is LSB because it is simple and straightforward [6]. Below is one of the mathematical algorithm uses in LSB.

Let Z be M_z x N_z pixels of the cover-image file which is represented as:

$$Z = X_{ij} \mid 0 \le i \le M_z, 0 \le i \le N_z, \quad X_{ij} \in \{0, 1, 2, \dots, 255\}$$

The n-bit of secret data (*T*) is represented as:

$$T = \{t_i \mid 0 \le i \le n, t \in \{0,1\}\}$$

Assuming that *T* is to be fixed into the k-rightmost LSBs of *Z*. Firstly, T is rearranged in order to form abstractly k-bit virtual image *T'* as [9]

$$T' = \{t_i' \mid 0 \le i < n', t_i \in \{0,1,\dots,2^k - 1\}\}$$

Where n' < M_z x N_z the mapping between T = $\{t_i\}$ and the embedded message M' = $\{m_i'\}$ which can be defined as:

$$t_i' = \sum_{j=0}^{k-1} t_{ixjxk} \times 2^{k-1-j}$$

The pixels subset of n' $\{x_1, x_2, \dots, x_{in}\}$ are selected from Z in a predefined sequence. The embedding process will be completed when the k LSBs of *xi* is replaced by t*i'*. Mathematically, some of the pixel values (xli) are selected for strong t*i*' is customized to get stego-pixel *xi'* as:

$$x_i^{'} = x_i^{'} - x_i^{'} mod 2^k + t_i$$

In the recovery process, when the stego-image *S* is available, the hided secret data can be ready to recover without referring to the cover-image. The reverse of embedding secret data will be used to recover from stego-image to get secret data. The selected K LSBs pixels will be extracted and reconstruct the bits to get secret data back. Mathematically, the secret data bits (t*i*') are recovered as [9]

$$t_i' = x_i' mod 2^k$$

E. *Disadvantages*

- Loss of perceptual quality of the cover.
- Loss of data with key
- Once the file is detected as stego file or looking suspicions, the hided data or file can easily seen or discover

III. PROPOSED SYSTEM

The "Data Hiding in image Files" mainly developed to embed or extract the messages into image files. This project basically deals with two important network security concepts namely steganography and encryption. For encryption AES algorithm is used. The plaintext is given as input. The plaintext is encrypted using AES algorithm. The cipher text is given as output. The output cipher text is hidden into the image files using Steganography. For steganography, LSB algorithm is used and the image file is used as a medium to conceal and transmit the secret information. The contents of secret text/file are also converted to the bit stream. The encrypted file is now embedded behind the image file by mixing the contents together using LSB algorithm. At the other end, the encrypted file is separated from image file. The encrypted file is then decrypted and the original text file contents are then viewed.

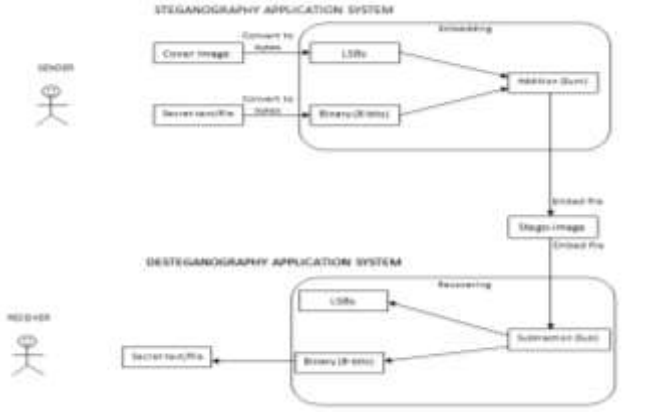

Fig 3. Proposed Methodology

A. *List of Modules and there Functions*

1) Sender Module

Sender is a User that interacts with the application in order to embed the secret data in image file and send the file to the Receiver. The function of this module is to accept the original image and the secret data from the user and hide the secret data in the image file and produce stego image.

2) Receiver Module

Receiver is a User that interacts with the application in order to recover the secret data in image file. The function of this module is to accept the stego image from the user and recover the secret data hided in the file.

3) Encryption Module

The Encryption module is a module that will help the data to be secured, which will allow the user to provide the secret key for retrieving the secrets data in the receiver side?

4) Decryption Module

The Decryption module is a module that will authenticate the receiver by requesting the receiver to enter the secret key before haven access to secret data.

B. *Development Environment*

We used the following software for the development of the system.

- Programming Language Java
- Framework Swing
- IDE Eclipse
- Database server MY SQL

IV. RESULT

Now having the Steganography application and ready to use after following the working steps and gathering the benefits from it

Sender

- The user will open the application and provide valid username and password. After the user login into the application, the home page for application will be

 ISSN: 2321-8169
174 - 180

displayed as shows in figure (4). If the user want send the secret data will click on Embed button, else the user will click on Retrieve button for recover the secret message.

- If the user click on Embed, the new window will show the type of data want to embed (text or image file) as shows in figure (5). After press Embed Message, window appear to the sender to select Master file(cover image) as shows in figure (6) in where you store in your computer. After selecting cover image, new window will appear to name the new stago-image as output file as shows in figure (7).
- Window will appear to sender after selecting cover image and set stego image name. This window will allow sender to compose the text and provide stego-key then embed the message, send stego-image and close the application as shows in figure (8).
- If the user click press Embed file, window appear to the sender to select Master file (cover image) and secret file in where you store in your computer and set the stego-image name as output file as show in figures (9-10-11).
- The window will appear to sender which will allow the sender to provide stego-key then embed the file, send the stego-image and close the application as shows in figure (12).

Fig 4. Home Page

Fig 5. Optional window for Sender

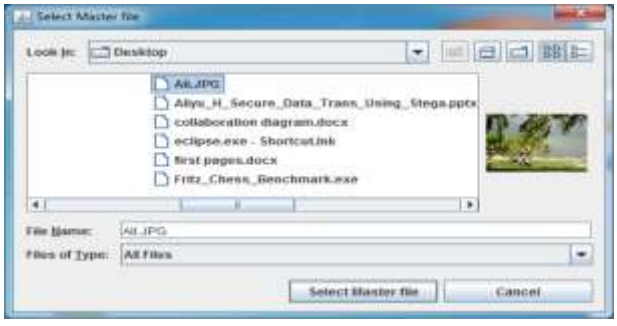

Fig 6. Opening file window for Cover Image of embedding message

Fig 7. Window for Stego Image name

Fig 8. Embed Message Window

Fig 9. Opening file window for Cover Image for embedding file

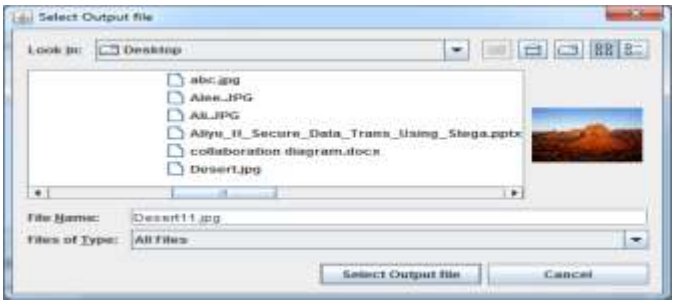

Fig 10. Window for Stego Image name

 ISSN: 2321-8169
174 - 180

Fig 11. Opening file for Data file

Fig 12. Embed File Window

Receiver

- If the user clicks on Retrieve, the new window will show the window that will allow user to select type of data want to Recover (text or image file) as shows in figure (13). After press Retrieve Message, window appears to the receiver to select stego-file in where you store in your computer as shows in figure (14).
- After selecting stego-image, new window will appear to user which contain the details about the stego-file and ask if user want to recover the secret message as shows in figure (15).
- If the receiver want recover, window will appear to ask for stego-key shows in figure (16-17).
- If the user press Retrieve file, in where you store in your computer as shows in figure (18).
- After selecting stego-image, new window will appear to user which contain the details about the stego-file and ask if user want to recover the secret message as show in figures (19-20-21).
- Lastly with valid stego-key application will display the secret file to user

Fig 13. Optional window for Receiver

Fig 14. Opening file window for stego image to retrieve message

Fig 15. Stego image details window

Fig 16. Stego-key window

Fig 17. Secret message window

Fig 18. Opening file window for stego Image to retrieve file

Fig 19. Stego image details window

Fig 20. stego-key window

Fig 21. Successful stego-key window

V. COPYRIGHT FORMS AND REPRINT ORDERS

In this part, we are going to analyze the securety of secure steganography application we developed by comparing the original image and stego-image. From the figure (22-23) (a) cover image and (b) stego-image all they look same, which is difficult to differentiate cover-images from steno images.

(a) Original image

(b) Stego image

Fig 22. Comparison of cover and stego images for secret message

(a) Original image

(b) Stego image

Fig 23. Comparison of cover and stego images for secret file

VI. FUTURE ENHENCEMENTS

The knowledge of information technology is still limited to mainly the research individual and academia, however the understanding the technology to used wisely is growing every day. A plan is made to continue to carry out more research in the field of information hiding. In future, the system will be extending to become more efficient and secure. The research will include the enhancement of the algorithm that will utilize the entire image for embedding the message. The research will see how possible is the system can automatically generate the secret key for recovering the secret data and attach the secret key to receiver account for automatic recovery by detecting the receiver account when the receiver try to recover any stego image.

REFERENCES

[1] H.-W. T. Chin-Chen Chang, "A steganographic method for digital images using side match," Pattern Recognition Letters, p. 1431–1437, 2004.

[2] J. a. M. O. T Morkel, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, 2005..

[3] L. McGill, "Steganography: The Right Way," SANS Institute InfoSec Reading Room, pp. 1-29, 2005.

[4] P. N. L. B. Mr. Swapnil S. Thakare, "Data Embedding using Secured Adaptive Pixel Pair Matching," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, no. 5, pp. 176-184, 2014.

[5] T. a. G. C.P.Sumathi, "A Study of Various Steganographic Techniques Used for Information Hiding," International Journal of Computer Science and Engineering Survey (IJCSES), pp. 9-25, 2013.

[6] V. B. Deepesh Rawat, "A Steganography technique for hiding image in an image in an image using LSB method for 24-bit color image, "International Journal of Computer Applications , p. 0975 – 8887, 2013.

[7] S. I. M. S. a. M. R. K. Muhalim Mohamed Amin, "Information Hiding Using Steganography," UNIVERSITI TEKNOLOGI, Malaysia, 2003.

[8] B. N. Hamidreza Rashidy Kanan, "A novel image steganography scheme with high embedding capacity and," Expert Systems with Applications, p. 6123–6130, 2014.

[9] L. M. C. K. Chan, "Hiding Data in Images by Simple LSB Substitution," Pattern Recognition, pp. 469-474, 2004