International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017
Issue 07, Volume 5 (September 2018) www.ijiris.com

ADVANCED IMAGE STEGANOGRAPHY

Pooja Chandarana
IT Dept, K J Somaiya College of Engineering Mumbai
pooja.chandarana@somaiya.edu

Prof. Purnima Ahirao
IT Dept, K J Somaiya College of Engineering Mumbai
purnimaahirao@somaiya.edu

Manuscript History
Number: **IJIRIS/RS/Vol.05/Issue07/SPIS10083**
DOI: 10.26562/IJIRAE.2018.SPIS10082
Received: 09, September 2018
Final Correction: 19, September 2018
Final Accepted: 24, October 2018
Published: **September 2018**
Citation: Pooja & Ahirao (2018).ADVANCED IMAGE STEGANOGRAPHY. IJIRIS:: International Journal of Innovative Research in Information Security, Volume V, 471-474. **doi://10.26562/IJIRIS.2018.SPIS10083**
Editor: Dr.A.Arul L.S, Chief Editor, IJIRIS, AM Publications, India

Abstract— Advanced Image Steganography is used to develop a secure path for sending or receiving secret text messages. Using Chaff and Winnow& AES (Advanced Encryption Standard) encryption technique, the text message is encrypted and sent to receiver very securely. The system uses AES encryption to encrypt the user's secret text message and key information while sending it to receiver also using Diffie-Hellman key generation for sharing secret key between sender and receiver.

Keywords— Advanced images steganography; chaff and winnow; AES, Diffie-Hellman; Encryption;

I. INTRODUCTION

In the last years the Internet has been considered as a suitable medium for transferring digital data and multimedia. Its main advantage is the availability to almost everyone and data can be received within a few seconds. The main disadvantage of using the Internet is the weak data security, because data can be monitored by any unauthorized viewers. That is why steganography should be used. Steganography is a technique for embedding a secret data into a cover image. Any unauthorized user can view the stego image but only authorized users can extract the secret data. Any steganography approach must be secure to avoid any unauthorized access. It is divided into two main steps, the first step is the embedding algorithm and the second step is the extraction algorithm.

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 Messages, so it appears that to be a normal image or other file. If a person views that image which has hidden information inside, he or she will have no idea that there is any secret information. [1][5]

II. LITERATURE REVIEW AND EXISTING SYSTEM

In recent trends of technology, the challenge of improving Information security is important need when sending and receiving data in the fields of data communication and networks. To solve these problems there are several methods used to protect data from unauthorized access during transmission. Many techniques is used to protect the user data. The most efficient technique is using cryptography and steganography. Cryptography and Steganography are the master areas which take a shot at Information Hiding and Security.

In cryptography, encryption algorithm is the technique of converting transferred data into unrecognizable form to prevent unauthorized access to data unless knowing specific information about the used key. Decryption algorithm is used to reconstruct the original data. Cryptography recently includes using advanced mathematical procedures in encryption and decryption techniques. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric. In Symmetric-key Encryption using similar cryptographic key for both encryption and decryption. The used keys must to be similar or there can be a Some changes between the two keys. In asymmetric key encryption algorithms, the keys used for encryption and decryption must be different. Steganography is the technique that deals with hiding secret data in some cover media which may be image, audio, or video. The word steganography comes from the Greek "Seganos", that mean covered or secret and "graphy" which mean writing or drawing. [2][7][8]

- Problem with current scenario [7] [8]
  - There was no such security technique used for hiding text data into image and sending it securely to the receiver.
  - Sending a text message to other party would be easily readable by anyone.
  - By applying various combinations, hacker would easily break the security of the text message.
  - No such secure path was used to send a text message securely.
- Drawbacks of the existing system
  - Maintenance of the system is very difficult.
  - There is a possibility for getting inaccurate results.
  - User friendliness is very less.
  - It consumes more time for processing the task.

The second level of obfuscation employed in addition to a onetime-pad is chaffing. Borrowing language from the farming practice of "winnowing the chaff from the wheat", the concept of chaffing and winnowing as a means to achieve confidentiality in message transmission was first proposed by MIT computer scientist Ronald Rivest. Chaffing and Winnowing introduces an approach that does not use encryption keys, but instead uses "authentication" keys. An authentication key allows for the identification of valid bits from invalid bits of data. Using this knowledge, a message can be sent with both valid and invalid parts and the receiver can remove the invalid bits from the good bits (winnow the chaff) to get the message (the wheat). Using this approach, the cipher generated by the one-time-pad can be "padded" with additional characters, resulting in every string returned having the same number of characters [9].

There is no such existing application present for securely data transferring the data using all the algorithms proposed in this project. For additional security Diffie-Hellman key exchange algorithm is used for key exchange.

Also due to the information security background the web application security assessment of the application is be done and the application is secured completely. For the application security assessment, the Owasp testing guide was used.

III. PROPOSED SYSTEM

Considering the anomalies in the existing system computerization of the whole activity is being suggested after initial analysis. The project is developed using Visual Studio with C# .Net as programming language. There is only one entity that will have the access to the system which is user. Users first need to login using its login credentials and then only he/she can access the system. 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 where, user uploads the image and enters the text to send secretly, and gives a key or a password to lock the text, what this key does is, it encrypts the text, so that even if it is hacked by hacker it will not be able to read the text.

Receiver will need the key to decrypt the hidden text. User then sends the process id, Secret key and decryption key to the receiver where, receiver first opens the image, and then he/she enters the public key of sender of the respective id. Once the secret key is accepted by the system, then it allows receiver to decryption key for decryption of cipher-text, he/she then presses decrypt key to get secret text from 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. The system uses online database to store all related information.

Sender's Part:

- Sender loads an image which he wants to send
- Then he enters the text
- He sets the password for text and finally encrypts it.
- He saves the image and sends it across to receiver (Through email or any other way).

Receiver's Part:

- Receiver opens the image in the application.
- Enter password which was used for encrypting (Password can be pre-decided or shared)
- After typing the password press Decrypt.
- Text will be shown as it was sent by the Sender.

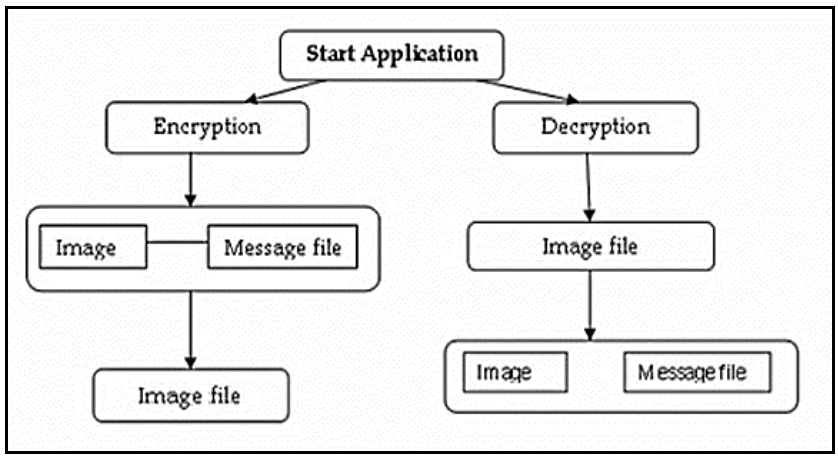

Fig 1. Block diagram of proposed System

Strings using standard string-similarity functions when the strings must be obfuscated in some secure manner (e.g. hash, encrypt, cipher). Two separate processes are elaborated within. The first, using a one-time-pad to create cipher for each string, provides for a type of obfuscation that is both theoretically unbreakable and not vulnerable to frequency analysis. The second process enhances the first by employing the method of chaffing and winnowing which involves the addition to the cipher of fake characters ("chaff") to the valid characters ("wheat") so as to result in all encoded strings being the same length.[9]

As an example, let's say that we want to encrypt the string "AARON" from data set *S*. Using a cryptographically secure random key generator we feed in the alpha-numeric seed:

"ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

And are returned the pad-key

"DO88Z0DLE7SZZI6ABAD4CHIJJ6PTYZUYZYKT".

This system comprises of 5 Modules as follows:

- **Image Selection:**
  Here, User selects an image for sending a secret message.
- **Encrypting the Data:**
  Here, User enter/inputs the text that is to be hidden in the image. User sets a key and uses the encryption technique to encrypt the data.
- **Downloading the Image:**
  After hiding the text with the encryption technique, user can save the encrypted image file and store it into local system.
- **Send Email:**
  Here, user can share the secret message with one or more people by sending them the process id, required key details via email.
- **Decrypting the Data:**
  Once, the receiver receives the image, he/she can decrypt the image and the original secret message will be displayed

IV. CONCLUSIONS

A cryptography and steganography algorithms proposed to increase security and authentication of data transmitted in a network environment. The proposed system is one of the best ways of hiding the secret of data transferred between sender and receiver from intruders in unsecured networks. The growth of modern communication needs a special means of security especially on computer network. As there appears a risk that the sensitive information transmitted might be intercepted or distorted by unintended observers for the openness of the internet. So it has resulted in an explosive growth in secure communication and information hiding. Moreover, the information hiding technique can be used extensively in applications like business, military, commercials, anti-criminal, digital forensic and so on. Steganography is the technique of secret communication which has received much attention. In this thesis image based steganography methods have been proposed to increase the performance of the data hiding techniques. This project focuses on the analysis and development of image steganography techniques that can hide data with a low detection rate and high payload.

ACKNOWLEDGMENT

I am very thankful to my guide Prof. Purnima Ahirao for her invaluable guidance and advice throughout this project.

REFERENCES

1. K. Wu and C. Wang, “Steganography using reversible texture synthesis” IEEE Transactions on Image Processing Vol.24 pp 130-139,January 2015
2. Shreyank N Gowda, “An Advanced Diffie-Hellman Approach to Image Steganography ” IEEE Transactions on advance network and telecommunication system Vol.19 pp 1-4,june 2016
3. Sherin Sugathan, “An Improved LSB Embedding Technique for Image Steganography ” International conference on applied and theoretical computing and communication technology Vol.33 pp 609-612,2016
4. S. Singh and V. K. Attri Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 8, No. 5 , pp. 259-266 ,2015
5. Utsav Sheth and Shiva Saxena, “Image Steganography Using AES Encryption and Least Significant Nibble ” International conference on communication and signal processing Vol.11 pp 0876-0879,2016
6. Radu Pietraru, “Secure communication method based on encryption and steganography” International conference on control system and computer science Vol.31 pp 453-458,2017
7. Y Manjula and K B Shivakumar ,”Enhanced Secured Image Steganography using Double Encryption Algorithm” International Conference on Computing for Sustainable Global Development (IndiaCom),2016
8. Tanushree Shelare and Varsha Powar,”A secure transmission approach using B-Trees in steganography”International Conference on Automatic Control and Dynamic Optimization Techniques,2016
9. https://www.sans.org/reading-room/whitepapers/vpns/review-chaffing-winnowing-876
10. http://www.asp.net/: This is the official Microsoft ASP.NET web site. It has a lot of: tutorials, training videos, and sample projects.
11. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6850714&queryText%3Dimage+steganography
12. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6658020&queryText%3Dimage+steganography

