International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Hybrid Approach to Text & Image Steganography using AES and LSB Technique

Vikas M[1], Yashwanth E[2], Veeresh[3], Sanath Krishna S[4], Narender .M[5]

[1234]*Student, Department of CS&E,*
THE NATIONAL INSTITUTE OF ENGINEERING (NIE), MYSURU
[5]*Assistant Professor, Dept. Of CS&E, NIE, Mysuru*

Abstract – *For communication of secret messages or information from one place/source to another for different applications we use Steganography and Cryptography. Usually in Cryptography the content of secret message is scrambled while in Steganography secret message is embedded in a cover medium. In this paper we propose a secured model developed by combining Advanced Encryption Standard (AES) and Least Significant Bit (LSB) algorithms. Here, AES is used for Cryptography and LSB technique is used for Steganography. The system proposed encrypts a text or image inside a Cover image.*

Key Words: **Cryptography, Steganography, AES encryption, LSB technique, Image Steganography.**

1. INTRODUCTION

Cryptography is the art of protecting information by encrypting it into a format which cannot be read easily and is called as cipher text. This cipher text or secret message can only be read by those who possess a secret key and can decipher (or decrypt) the message into plain text.

Steganography is the art of hiding the information which is to be communicated in another cover medium. Most commonly used file format for communication is Digital Image due its high frequency on the Internet. For hiding secret information in images, there exist a large variety of Steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the Steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. In this paper it is been shown how a text can be hidden in an image file and also how an image can be hidden in another image.

Steganography can be classified into 4 types mainly : Audio, Video, Image and Text.

1.1 Image Steganography

It is popularly used Steganography technique for hiding data since it provides a secure and simple way to send the information over the internet. Images are routinely used in diverse areas such as medical, military, science, engineering, advertising, education as well as training. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. The essential principle of Image Steganography is the replacing of bits in the image data, with bits belonging to the target message. Special care is taken to ensure that the bits of the image used to store the message bits are unused or insignificant to ensure that the image itself is not significantly modified.

2. LITERATURE SURVEY

[1] M Saritha, Sushravya M, Vishwanath M Kadabadi, "Image and Text Steganography with Cryptography using MATLAB": This paper presents a system in which the text is encrypted using Symmetric XOR algorithm and Sequential algorithm is used to hide the data in cover image. The level of security provided is low. Also, the system defined is limited to low quality and to few types of images.

[2] Aman Arora, Manish Pratap Singh, Prateek Thakral, and Naveen Jarwal, "Image Steganography using Enhanced LSB Substitution technique": **T**his paper presents a system in which the bits are modified according to first bit set. If image has same pixel repeating over a region, then this method fails because the bit modification will be bring changes to the entire pixels in the range, thus now the change in colour values will be noticeable to human eyes very easily.

[3] Utsav Seth and Shiva Saxena, "Image Steganography using AES Encryption and Least Significant Nibble": This system provides a good security in comparison with other papers above by using AES encryption. But there the quality of image is low and the after Steganography the final images have more noise compared to other papers this is because here least significant nibble is chosen over 1 or 2 least significant bits. Thus the human eyes can detect the fact that data is hidden in the image.

[4] Kamaldeep Joshi and Rajkumar Yadav, "New Approach toward Data Hiding using XOR for Image Steganography": This method assumes that both sender and receiver agree upon a cover image which is present at both

the ends. But this method is very difficult as it will be difficult to maintain same image having same properties like size, resolution etc.

[5] Yambem Jina Chanu, T. Tuithung, k. Manglem Singh, "A short survey on image Steganography and steganalysis techniques": The paper describes a short survey on different types of Steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image.

3. SYSTEM ANALYSIS

3.1.1 Existing System

The image or text is directly hidden in cover image. Thus hacker/intruder can use Steg-Analyser and extract the least significant bits and then convert it back to original form. The system supports only few image types, thus only a limited no of users are benefitted. Cover image may be more polluted or noise is more when storing large data.

3.1.2 Proposed System

The system first encrypts the given message using AES encryption and then it is written on to the cover image. This provides very high security. The system supports 24-bit and 32-bit BMP images. The system uses a unique LSB technique which stores more data than original algorithm and also maintains good quality while doing so.

3.2 System Requirements

3.2.1 Hardware Requirements

- Processor: Intel or AMD with 2GHz or higher.
- Memory: 2GigaBytes or More.
- Storage: Depending on images being used.

3.2.2 Software Requirements

- OS: Windows 8 or Higher.
- Tools: Visual Studio (.NET Framework)
- Programming Language: Visual C#

4. METHODOLOGY

The proposed LSB Technique is as follows:

1. Input: Text or Image, Cover Image.
2. Read the given cover image Pixel values (RGB).
3. For each component of pixel, replace rightmost 2 bits in R or G or B if it is highest among them and is greater than a threshold value.
4. For remaining values, replace only the rightmost bit.
5. Continue step 3 or 4 till end of text/image.
6. Output: Stego Image.

The above algorithm is expected to store more data than the original LSB algorithm and also maintain its quality.

The flow of data in system is as follows:

1. Choose the cover image.
2. If text, then input the text in the system.
3. If image, input the secret image.
4. Encrypt the text/secret image using AES encryption algorithm.
5. Embed the encrypted information in the cover image using LSB technique proposed.
6. The stego image is stored in the system.

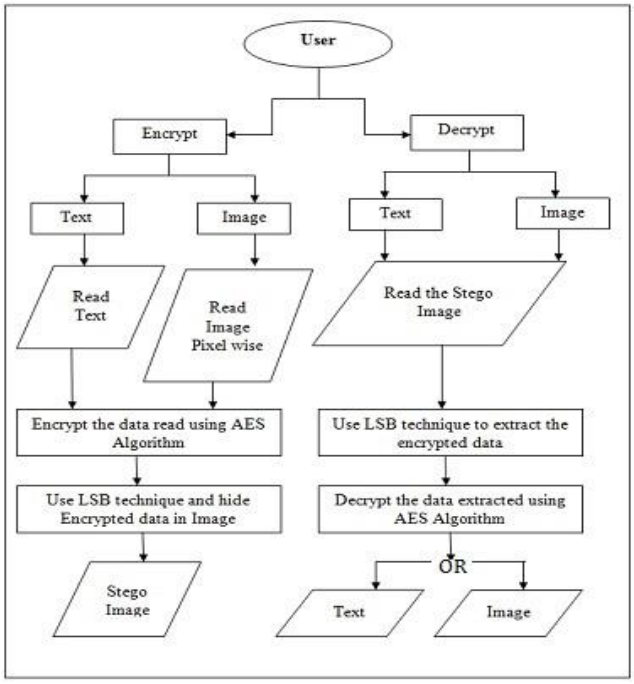

Fig.1: Data flow Diagram.

5. RESULTS

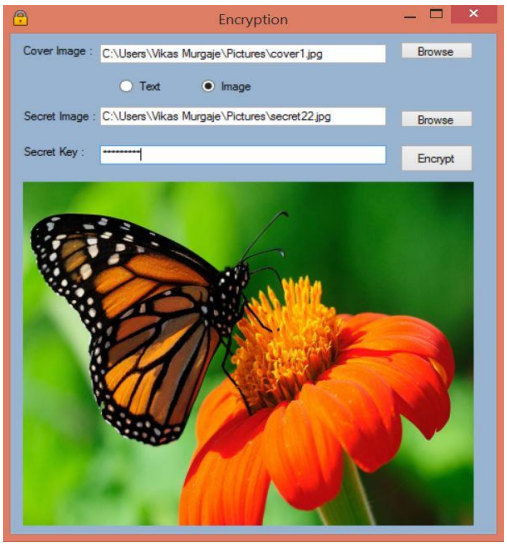

Fig.2: Encryption Screen

The screenshot is of Encryption window of Image hiding process. The figure 2 shows window in which all the fields are filled.

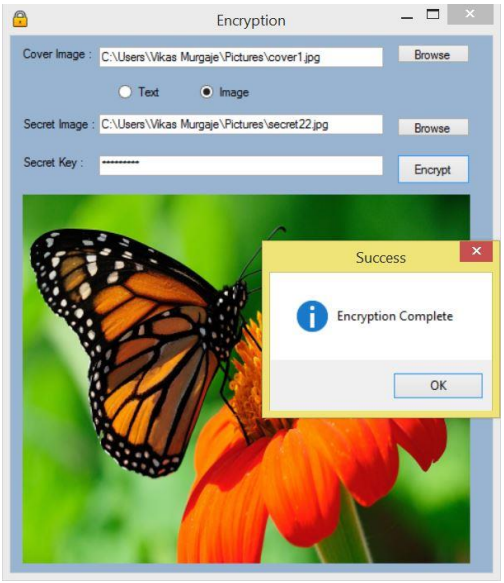

Fig.3: Encryption Success

The figure 3 shows encryption complete message once the encryption is finished and stego image is stored on the computer.

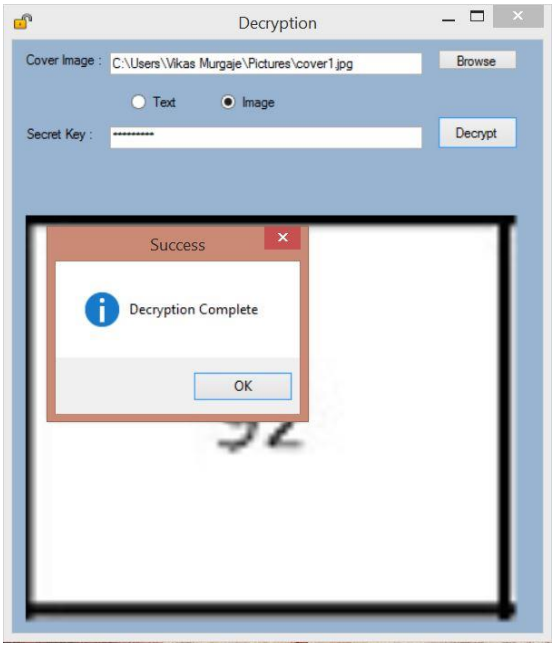

Fig.4: Decryption Window

The figure 4 of Decryption window is as given here. This window here shows decryption of secret image from given cover image and it displays a success message and shows the secret image in the window and also stores it on the computer.

6. CONCLUSION & FUTURE WORK

This method will help us to reduce risk of security while transferring secret information over the network. Proposed system is user friendly and anyone with basic computer knowledge can use the system without any difficulties. Further the system can be extended to different types of files like Audio, Video etc. also it can be applied to different formats of files.

REFERENCES

[1] M.Saritha, Sushravya.M, Vishwanath.M.Kadabadi, "Image and Text Steganography with Cryptography using MATLAB", 2016.

[2] Aman Arora, Manish Pratap Singh, Prateek Thakral, and Naveen Jarwal, "Image Steganography using Enhanced LSB Substitution Technique", 2016.

[3] Utsav Seth and Shiva Saxena, "Image Steganography using AES Encryption and Least Significant Nibble", 2016.

[4] Kamaldeep Joshi and Rajkumar Yadav, "New Approach toward Data Hiding using XOR for Image Steganography", 2016.

[5] Yambem Jina Chanu, T. Tuithung, k. Manglem Singh, "A short survey on image Steganography and steganalysis techniques", 2016.

[6] "Cryptography and Network Security", Behroz Forouzan, SIE, 2nd Edition, McGraw-Hill.

[7] "Cryptography and Network Security", Principles and Practice; Fifth Edition by William Stallings, Prentice Hall.

[8] Anjali Tiwari, Seema Rani Yadav, N.K. Mittal, "A Review on Different Image Steganography Techniques", 2014.