DUAL LAYER SECURITY USING AES ENCRYPTION AND SECURE SYSTEM FOR HIDING MULTIMEDIA FILES IN DUAL RGB COVER IMAGES

[1]Bincy Babu, [2]Neethu Tressa
[1]Student, [2]Assistant Professor
[1]Computer Science
[1]St.Joseph's college, Thrissur, India

Abstract: ***The fast growth in communication technologies and the increased availability of the public networks facilitated data transfer. However, the public communication channels are vulnerable to security attacks that may lead to unauthorized access to some information. Now a day's there is a challenges faced by data or information security field. We have to make this data free from harm during transmission. The primary aim is to make an application which enable information by covering securely in statistically undetectable communication channel. The two important concept of securely transmitting information or data over a medium like steganography and cryptography. Although cryptography and steganography are used to provide data security. Steganography and encryption combined enhance security by providing dual layer protection to the data, as steganography aims at hiding the existence of the data itself and encryption prevents the correct interpretation of the data. Firstly, the Advanced Encryption Standard(AES)algorithm has been modified and used to encrypt the secret message. Secondly, the encrypted message has hidden into two color RGB cover image. The multimedia files split vertically into two parts; one part contains the least significant half-bytes, and the other part contains the most significant half-bytes. The two parts are hidden inside to uncompressed RGB cover images using a least significant 4-bit replacement technique. The dual stego images are expected to be send separately, through separate channels, to avoid capture of both stego files by an adversary. Extraction of the secret file is achieved through merging LSB half-bytes and MSB half-bytes from the two stego files. The extracted file is identical in content and structure with the original secret message.***

Index Terms – Security, Steganography, Cryptography, AES algorithm, dual hiding, MSB, LSB, LSB technique.

I. INTRODUCTION

The concept of what you see is what you get with respect to digital image is no longer accurate. Image may be more than what we can see using our human visual system because it can hold an embedded data that cannot be seen. Securing multimedia data requires preventing unauthorized users from access, distortion, destruction, detection or modification of the data during its transfer. There are two primary methods for data security protection encryption, and steganography [1]. Cryptography method is used for secret communication. It involves converting a message text into an unreadable cipher. Cryptography differs from steganography. In that steganography hides the messages so it cannot be seen while the cryptography technique scrambles the messages so it cannot be understood. However, both of them can be combined to produce better security and protection of the message. Three objects are involved in the embedding process; the secret message, the original cover file and the stego file which combines the secret and cover files. Some data hiding scheme use lossy compression, to allow for higher hiding capacity at the expense of losing bits of the secret message [1].

The work in this paper presents a data hiding technique for the protection of multimedia files, through embedding in dual cover RGB images, with the aim of reducing the cover image size, increasing the hiding capacity, and protecting the secret messages through a safe partitioning scheme.

II. EXISTING SYSTEM

In the existing system, the original message is encrypted using RSA and the cipher text that is obtained as its output is taken as input data for embedding in the cover image, the resultant stego image has cipher text embedded in it. While decoding the image the cipher text is retrieved and is therefore decrypted using RSA private key. After RSA decryption the original input message is produced as the final output [2].

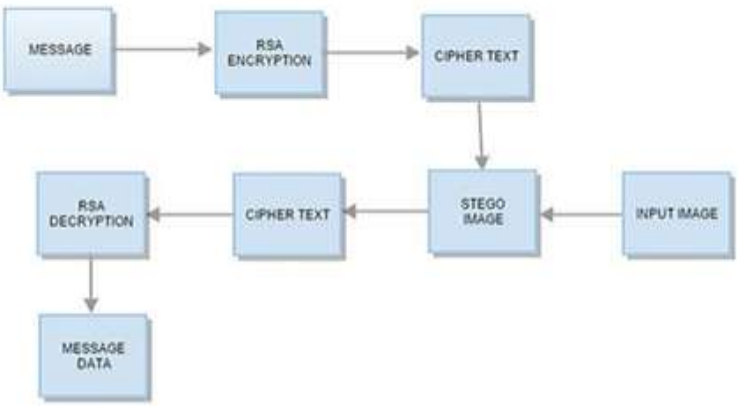

figure 1

III. PROPOSED SYSTEM

The aim of proposed scheme is to make a more secure and robust method of information exchange so that confidential and private data must be protected against attacks and illegal access. To order to achieve the required robustness and cryptography and steganography is combined. For hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access. In this method we first image select two images, then encrypt a message using AES algorithm to provide security to secret messages. After encryption we can receive cipher message. Then, the cipher message is split into two. They are MSB bit and LSB bit. These bits are hided into two cover images using LSB embedding method. Then the original messages are retrieved using AES decryption.

IV. METHODOLOGY

4.1Text phase

The text phase requires first to select two cover image. Then write the secret message for their hiding purpose.

4.2 Encryption phase

The encryption phase we are used AES algorithm. AES method is a non-Feistel cipher that encrypt and decrypt a data block of 128 bits. It uses 10,12, or 14 rounds. The key size, which can be 128,192, or 256 bits, and the number of rounds depended on the key size because it allows the secret key to be expanded to produce sub key for each round. In AES method, the input and output sequence have the same length. According to AES method, substitution bytes, shift rows, mixing column and key adding steps are implemented in every encryption round to encrypt the message, but the Mixing Column step doesn't include in the last round. In the decryption, the four steps are implemented in the reverse way. Also, the inverse of mixing column step doesn't include in the last round of the decryption. The pseudo code of AES is as follows

```
1. InitialRound (State, RoundKey)
   {
    AddRoundKey (State, RoundKey)
    }

2. Rounds (State, RoundKey)
   {
    SubBytes (State);
    ShiftRows (State);
    MixColumn (State);
    AddRoundKey (State, RoundKey);
   }

3. FinalRound (State, RoundKey)
   {
    SubBytes (State);
    ShiftRows (State);
    AddRoundKey (State, RoundKey);
    }
```

The advantages of using AES algorithm are; it is more secure, faster in both hardware and software, reasonable cost, and its main characteristics flexibility and simplicity [3]. In this phase the message is encrypted using AES algorithm. The result is cipher message. The cipher message is splitted into two parts. They are LSB bit and MSB bit.

4.3 Steganography phase

Steganography is communication that uses the technique of cloaked writing that aims at hiding the existence of any message or data. Steganography has been in use for secret communication since ancient times in multiple forms. In this technological era, it is deployed for secured transfer of data over digital channel in which the information can be hidden in image, text, audio or video and are called image steganography, text steganography, audio or video steganography respectively [2].

We have studied image steganography. In image steganography cover image is converted into a stego image. The information or message is embedded into the cover image which is then called stego image. Also the text message hidden in the two images (i.e.LSB bit hidden in the one image and MSB bit hidden in the another image) cause little distortion as a single bit of the entire byte is altered (i.e. the bits that can be altered as per requirement without affect the original images) which make it easier to hide the information or message in it. LSB i.e. least significant bit technique is a simple and effective technique that can be used for implementing image steganography. In the additive color model 3 primary RGB (Red, Green, Blue) colors are combined in various proportions in order to make multiple different colors.

4.4Decryption phase

This section after these phases the original message is received using AES decryption.

V. IMPLEMENTATION

figure2: Original images

figure 3: Enter the message and size of key

figure 4: After encryption the message is splitted into two, LSB and MSB bit they hide into two images

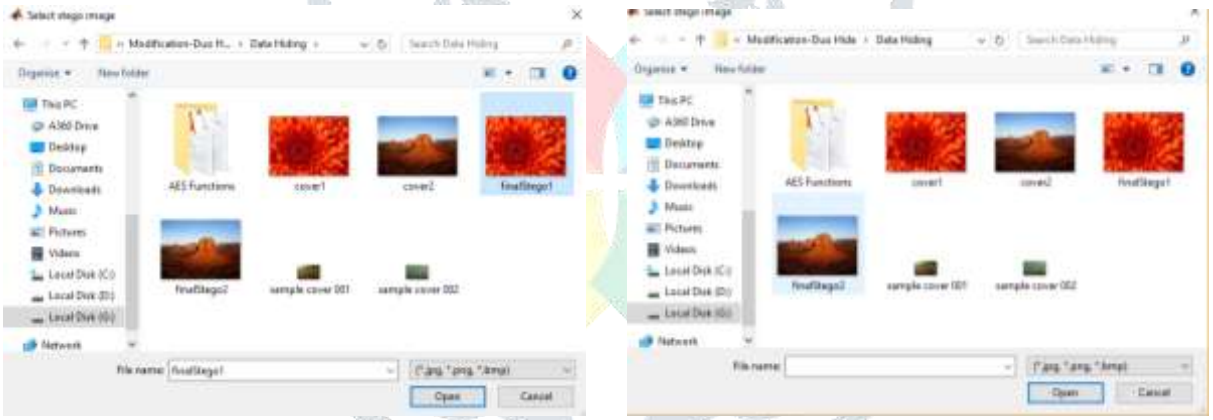

figure 5: The recovery stage to select two stego images

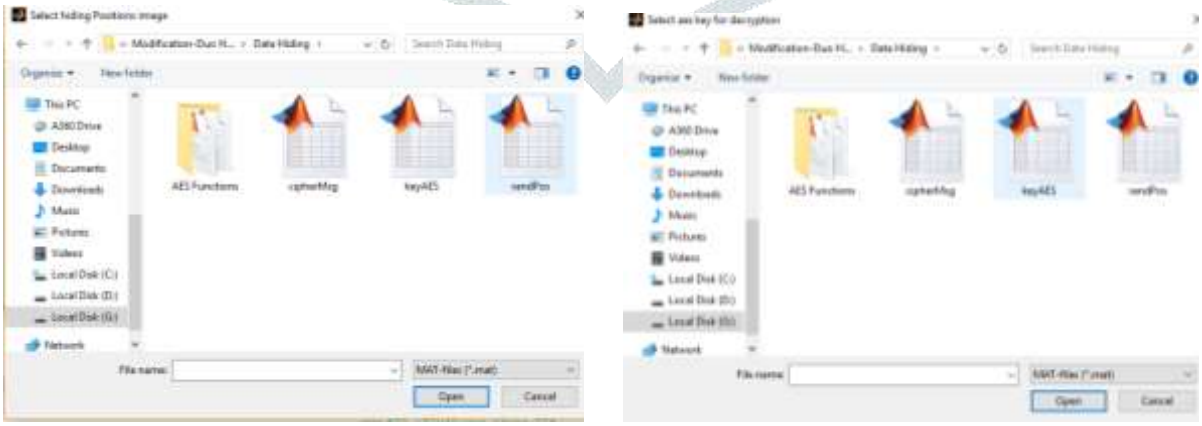

figure 6: To select random positions and key

figure 7: To get original message

VI. CONCLUSION

In this paper, we proposed the combination of cryptography and steganography has been achieved by using the AES algorithm and LSB technique. Advanced Encryption Standard is used to encrypt secret message and secret message is splitted into two, LSB bit and MSB bit. LSB technique is used to hide encrypted secret message into two cover images. When steganography is combined with encryption a good security was achieved between two parties in case of secret communication, it is hardly attracted from eavesdropper by naked eye. Finally, we can conclude that the proposed technique is effective for secret data communication. In future we can use audio, video in case of image as cover for hiding the data.

VII. ACKNOWLEDGMENT

First of all, I am grateful to The Almighty God for establishing me to complete this project. I am especially thankful to my guide, MS. Neethu Tressa, and all other faculty members from the department of computer science and my friends, for giving me their sole co-operations and encouragement and critical inputs in the preparation of this report. Finally, I express my heartfelt thanks to our Lab Instructors, colleagues, friends and my dear parents for giving me valuable advice and support throughout my project work.

REFERENCES

[1] Marwa Tariq Al-Bayati Mudhafar M. Al-Jarrah," Duo-Hide: a secure system for Hiding Multimedia Files in Dual RGB Cover Images ",2016 9th International Conference on Developments in eSystems Engineering.

[2] Shubhi Mittal, Shivika Arora, Rachna Jain," PData Security using RSA Encryption Combined with Image Steganography", 978-1-4673-6984-8/16/$31.00 © 2016 IEEE.

[3] Marwa E. Saleh, Abdelmgeid A, Fatma A. Omara," Data Security Using Cryptography and Steganography Techniques", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.