IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

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

[1]Bincy Babu , [2]Reshma N R
Assistant Professors
Software Development (Department)
Carmel College (Autonomous) Mala, Thrissur

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 Modified Advanced Encryption Standard (AES) algorithm is 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,Modified AES Algorithm.**

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 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

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

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, we combined cryptography and steganography together. 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 first select two images, then encrypt a message using Modified 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 Modified AES decryption.

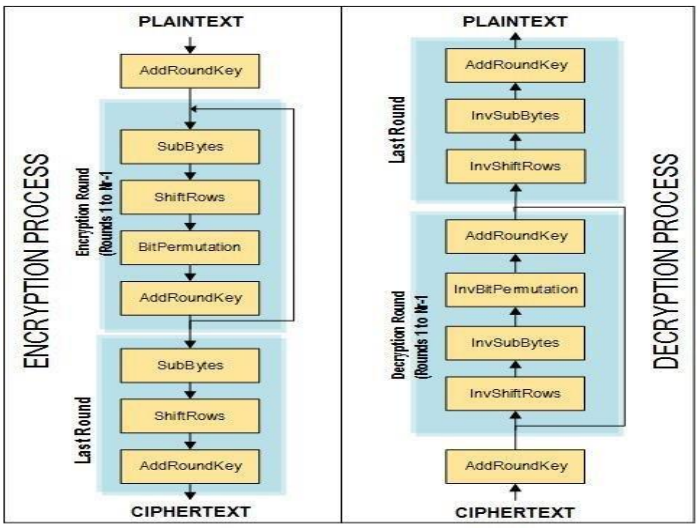
IV. METHODOLOGY

- **TEXT PHASE**

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

- **ENCRYPTION PHASE**

The encryption phase we are used Modified AES algorithm.In Modified-AES encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. The round function consists of four stages. To overcome the problem of high calculation we skip the Mixcolumn step and add the permutation step. Mixcolumn gives better security but it takes large calculation that makes the encryption algorithm slow . The other three junctures remain unbothered as it is in the AES. A single 128-bit block is the input to the encryption and decryption algorithms.This block is a 4×4 square matrix consisting of 16 bytes. This block is copied into the state array. The state array is modified at each stage of encryption or decryption. Similarly the 128-bit key is also depicted into a square matrix. The 128-bit key is expressed into an array of key schedule words: each word is of four bytes. The total key schedule words for ten rounds are 44 words; each round key is similar to one state. The block diagram of the Modified-AES algorithm with 128 bits data is shown below.



The algorithm is divided into four operational blocks where we observe the data at either bytes or bit levels and the algorithm is designed to treat any combination of data and is flexible for key size of 128 bits. These four operational blocks represent one round of Modified-AES. There are 10 rounds for full encryption. The four different stages that we use for Modified-AES Algorithm are:

- Substitution bytes □□
- ShiftRows □□
- Permutation □□
- AddRoundKey

Substitution Bytes, ShiftRows and AddRoundKey remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mixcolumn. These rounds are managed by the IP table. Permutation is widely used in cryptographic algorithms. Permutation operations are interesting and important from both cryptographic and architectural points of view. The DES algorithm will provide us permutation tables. The inputs to the IP table consist of 128 bits. Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and ShiftRows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits. In the permutation table each entry indicates a specific position of a numbered input bit may also consist of 256 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 242th bit of the 256-bit block is in first position, the 226th is in second position and so forth. After applying permutation on 128 bits we again complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit cipher text. he result is cipher message. The cipher message is splitted into two parts. They are LSB bit and MSB bit.

- **STEGANOGRAPHY PHASE**

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.

- **DECRYPTION PHASE**

After these phases the original message is received using Modified AES decryption.

V. CONCLUSION

In this paper, we proposed the combination of cryptography and steganography has been achieved by using the Modified AES algorithm and LSB technique. Modified 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.

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.