International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Reversible Data Hiding with Optimal Value Transfer

Viki Kharke[1], Pranay More[2], Prashant Pardeshi[3], Shriraj Ghosalkar[4], Prachi Gadhire[5]

[1]*Student VIII SEM, B.E., Computer Engg., DRIEMS, Neral, India*
[2]*Student VIII SEM, B.E., Computer Engg., DRIEMS, Neral, India*
[3]*Student VIII SEM, B.E., Computer Engg., DRIEMS, Neral, India*
[4]*Student VIII SEM, B.E., Computer Engg., DRIEMS, Neral, India*
[5]*Professor, Dept. of Computer Engineering, DRIEMS, Neral, India*

Abstract: *Information security has become the area of concern as a result of widespread use of communication medium over the internet. This paper focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files. The high results are achieved by providing the security to data before transmitting it over the internet. The files such as images, audio, video contains collection of bits that can be further translated into images, audio and video. The files composed of insignificant bits or unused areas which can be used for overwriting of other data. This paper explains the proposed algorithm using video Steganography for enhancing data security.*

1. INTRODUCTION

The Steganography, Cryptography and Digital Watermarking techniques can be used to obtain security and privacy of data. The Steganography is the art of hiding data inside another data such as cover medium by applying different steganographic techniques. While cryptography results in making the data human unreadable form called as cipher thus cryptography is scrambling of messages. Whereas the Steganography results in exploitation of human awareness so it remains unobserved and undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in Steganography. Generally Steganography technique is applied where the cryptography is ineffective.

The Steganography system consists of the cover file (image, video) and the secret message that is hidden inside the cover file by applying Steganography and stego file is generated which is same as cover image and go undetected or unaltered. The revolution in digital information has created new challenges for sending a message in a safe and secure way. Whatever method we choose, the most important question is its degree of security. Numerous approaches have been developed for addressing the issue of information security such as cryptography and Steganography. Cryptography provides an obvious approach to securing information. It scrambles the secret message, such that it becomes meaningless to eavesdroppers. However, this is not always adequate in practice as the encrypted content itself draws attention. Regardless how strong is the encryption algorithm, given enough time and tools, it could be broken. Furthermore, some cases require sending information without anyone noticing that the communication happened. Insuch cases, Steganography was the answer. Steganography is the art and science of invisible communication. The origin of the word Steganography comes from the Greek language. It is derived from two Greek words “stegos” which means “cover” and “grafia” which means “writing”.

2. LITERATUR SURVEY

1)In W. Zhang, B. Chen, and N. Yu method, a decompression algorithm for embedding the data is used. They proved that using this construction they can achieve the rate-distortion bound as long as the compression algorithm reaches the entropy. In this they have improved three RDH schemes that are using binary features sequence as covers. Using this system, embedding distortion can be reduced. It also improves reversible data hiding schemes for binary JPEG images. This system did not work on gray scale covers for designing recursive codes.

2) J. Fridrich, M. Goljan, and D. Rui’s system, a general framework for RDH is proposed. Extracted compressible features of cover images are firstly introduced by them. In this system, they have reserved a space to hide data by compressing the proper bit-planes having minimum redundancy. The lowest bit-planes which offer lossless compression are used if the image is not noisy. In completely noisy image some bit-planes are having strong correlations.

2.1 Existing system

In the existing system, histogram shifting technique is used.

The image is firstly divided into two planes A and B using image partition technique. Then the LSBs of A are reversibly embedded into B using standard RDH technique.

The estimating error is calculated so that data can be embedded into estimating error sequence using histogram shift technique.

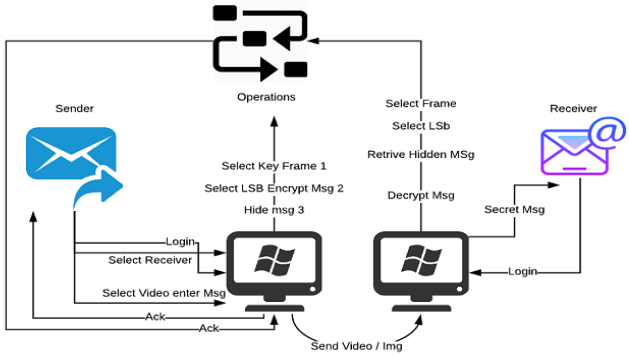
By using bidirectional histogram shift, some messages can be embedded on each error sequence. The information for data hider is embedded into LSBs of first 10 pixels in encrypted image.

After image encryption, the data hider or any third person cannot access the content of the original image without using encryption key.

2.2 Proposed System

The proposed system architecture is as shown in the figure below; it consists of image encryption, data embedding, image decryption, data extraction and image recovery block. The cover image here is the original image used for hiding data.

This system uses two keys one for encryption and one for data hiding. The encryption key is required for decryption process, if the key doesn't matched with encryption key image decryption is not possible. Same for data hiding key, data retrieval is possible only with data hiding key.



. **Fig -1**: Proposed Design/ Architecture

3. SYSTEM DESIGN

3.1 Sender

At sender side user is allowed to select either video or image in which sender has to hide the secret message. And specify the receiver and message to be hidden in the cover video or image. The message to be hidden is encrypted using AES. The Key frames are extracted from the video and the secret encrypted message is hidden in the LSB of the pixel of the frames of video or image. And this video is send to the receiver.

LSB Algorithm to embed text message

Step 1: Read the cover image and text message which is to be hidden in the cover image.

Step 2: Convert text message in binary.

Step 3: Calculate LSB of each pixels of cover image. Step 4: Replace LSB of cover image with each bit of secret messageonebyone. Step 5: Write stego image Algorithm to retrieve text message:-

Step 1: Read the stego image.

Step 2: Calculate LSB of each pixels of stego image.

Step 3: Retrieve bits and convert each 8 bit into character

Least Significant Bit (LSB): LSB is the lowest bit in a series of numbers in binary. E.g. in the binary number: 10110001, the least significant bit is far right. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS:

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001) **240**: 011110000

RESULT:

(00100110 11101001 11001001) (00100111 11001001 11101000) (11001000 00100110 11101000)

Here number **240** is embedded into first eight bytes of the grid and only 6 bits are changed.

AES Encryption Algorithm

1) Derive the set of round keys from the cipher key.
2) Initialize the state array with the block data (plaintext). 3) Add the initial round key to the starting state array.
4) Perform nine rounds of state manipulation.
5) Perform the tenth and final round of statemanipulation. 6) Copy the final state array out as the encrypted data (ciphertext).

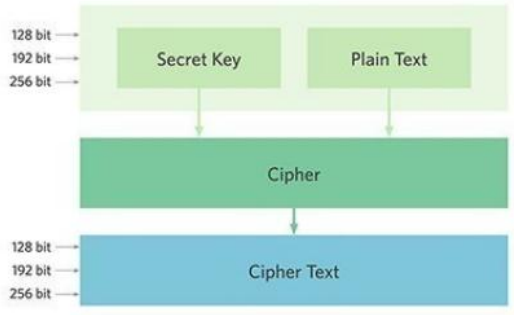


Chart -1: AES Encription

Receiver

At receiver side the receiver accepts the video or image. The Key frames are extracted from the video and the secret encrypted message is extracted from in the LSB of the pixel of the frames of video or image. The message received message is in the encrypted form so it is decrypted using AES and message is displayed to the receiver.

AES decryption Algorithm.

1) Perform initial decryption round:
XorRoundKey InvShiftRows InvSubBytes

2) Perform nine full decryption rounds:
XorRoundKey InvMixColumns InvShiftRows InvSubBytes
3) Perform final XorRoundKey
4) Retrieve the plain text.

3.2diagram Reversible data hiding

1) Encrypted Image Generation: Input: In this the image passed by first module, encryption key are the inputs.
2) Data Hiding in Encrypted Image: Input: In this the marked encrypted image, the data hiding key, the data files to be embedded are taken as inputs.
3) Data Extraction and Image Recovery: Input: In this the data embedded image, data hiding key and encryption key is taken as input.

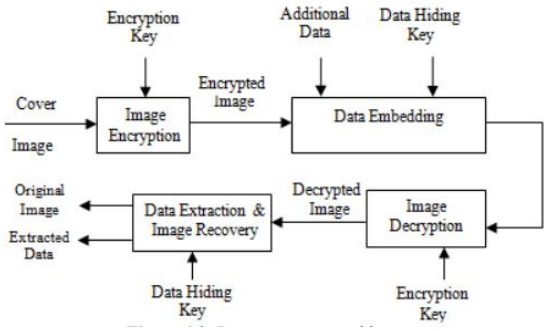


Fig -1: Flow diagram Reversible data hiding.

4. APPLICATION

The proposed application can be used in bank to send the pin number to the customer.

Army can also use steganography to keep their communications secret and to coordinate attacks. All of this sounds fairly nefarious, and in fact the obvious uses of steganography are for things like espionage. But there are a number of peaceful applications. The simplest and oldest are used in map making, where cartographers sometimes add a tiny fictional street to their maps, allowing them to prosecute copycats. A similar trick is to add fictional names to mailing lists as a check against unauthorized resellers.

5. CONCLUSION

In this paper we presented several ways of hiding the secret data inside the cover medium such as image, audio, video. The proposed system for data hiding uses AES for encryption. Which results in more secure technique for data hiding. We can conclude that the proposed system is more effective for secret communication over the network channel.

6. REFERENCES

[1] Steganography and steganalysis-Robert Krenn, Internet Publication,March2004 http://www.krenn.nl/univ/cry/steg/article.pdf.
[2] Steganography, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213717,00.html.
[3] Johnson, Neil F., "Steganography", 2000 http://www.jjtc.com/stegdoc/index2.html.
[4] The WEPIN Store, "Steganography (Hidden Writing)", 1995, http://www.wepin.com/pgp/stego.html.