International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

IMAGE STEGANOGRAPHY USING SECURED FORCE ALGORITHM FOR HIDING AUDIO SIGNAL INTO COLOUR IMAGE

B.G.AAGARSANA[1], ANJALI[2], T.K.KIRTHIKA[3], Mr. S. SIVAKUMAR[4]

[1,2,3] Jeppiaar SRR Engineering College, Tamil Nadu, India
[4]HOD of ECE Department, Jeppiaar SRR Engineering College, Tamil Nadu, India

---

Abstract–*The increasing growth of internet application, create the need for secured transmission of secret message, data or information. There exist several methods for providing secured transmission of information. The most attractive and latest approach for information security is steganography. Steganography is the practice of hiding any text data, image, audio or video within another image, audio or video. The main aim of this paper is to hide audio signal into colour image using AES algorithm and circular LSB algorithm. And this embedded output is secured using secured force algorithm which provide another layer of security. At decryption side ADS algorithm provides decrypted output. This image steganography provides hiding of data more effective and efficient manner with help of circular LSB and secured force algorithm.*

Key Words: **Advance Encryption Standard Algorithm (AES), Advance Decryption Standard Algorithm (ADS), Circular LSB Algorithm, Secured Force Algorithm**

1. INTRODUCTION

Steganography is an art of hiding data. This is derived from Greek words, steganos means cover and graphien refers to writing, this means hiding message into another medium. There are various mediums in which data can be hidden, depending on those techniques there are various types of steganography. These various types are image steganography, audio steganography, video steganography. In audio steganography and image steganography the type of data that can be hidden are text data, image and audio signal. In video steganography the data that can be hidden are text data, colour image, audio signal and video also.

There are many way of hiding secret data for secret communication they are cryptography, watermarking and steganography, i.e. these are major concern of digital data security . Among these techniques steganography is modern technique which is used in this modern era.

In cryptography technique it is known that data in hidden in that medium but using steganographic technique this drawback is over come, as other than sender and receiver no one else can know that any secret data is hidden in the cover medium. The cover medium after encryption and before encryption look similar and hence forth this technique is more efficient than any other technique.

This steganography technique ensures privacy, integrity and confidentiality for secret communication. This technique follows a general procedure for any type of steganography. Initially an image, audio signal or video is used as medium i.e. cover medium for secret communication, data is hidden in this cover medium. The data that has to be hidden are either text document, image, audio or video. Together the combination of this cover medium and secret data forms stego image. For example hiding text data in image forms stego-image. This stego image at decryption side is converted back into cover medium and secret data using steganalysis method, which is considered as an reverse method as steganography.

2. RELATED WORK

In 2017, Beenish Siddiquiand Sudhi Goswami presented "A Survey on Image Steganography Using LSB Substitution Technique" which consists of overview of steganography and techniques used in steganography and further have proposed a new approach in steganography based on Direct Wavelet Transform using NSGA (Non Dominated Sorting Algorithm) for better quality of stego image.

In 2011 Yong Feng Huang, Shanyu Tang, Senior Member, IEEE, and Jian Yuan presented "Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec". This paper describes a novel high-capacity steganography algorithm for embedding data in the inactive frames of low bit rate audio streams encoded by G.723.1 source codec, which is used extensively in Voice over Internet Protocol (VoIP). This study reveals that, contrary to existing thought, the inactive frames of VoIP streams are more suitable for data embedding than the active frames of the streams; that is, steganography in the inactive audio frames attains a larger data embedding capacity than that in the active audio frames under the same imperceptibility.

In 2012 Yongfeng Huang, Chenghao Liu, Shanyu Tang, Senior Member, IEEE,and SenBai presented, "Steganography Integration Into a Low-Bit Rate Speech Codec". Low bit-rate speech codecs have been widely used in audio communications like VoIP and mobile communications, so that steganography in low bit-rate audio streams would have broad applications in practice. In this paper, the authors propose a new algorithm for steganography in low bit-rate VoIP audio streams by integrating information hiding into the process of speech

encoding. The proposed algorithm performs data embedding while pitch period prediction is conducted during low bit-rate speech encoding, thus maintaining synchronization between information hiding and speech encoding.

In 2013, Ankitha Gangwar and Vishal Shrivastava presented "Improved RGB-LSB steganography using Secret Key." In this paper steganography based on LSB technique is further enhanced by improving the security level of hidden information, in which new approach of hiding secret information in different location of lsb in pixel using secret key is proposed. The experimental result shows that the new approached methods is an effective way of hiding information and also is difficult for unauthorized user to identify the hidden data. The use of secret key is to secure information only to legal users.

3. PROPOSED WORK

Increasing the layer of security in communication of data using secured force algorithm. The algorithms used in encryption side are

- Advance Encryption Standard Algorithm
- Circular LSB Algorithm
- Secured Force Algorithm

And towards the decryption side the algorithms used are

- Advance Decryption Standard Algorithm

In this paper both AES algorithm along with Circular LSB algorithm hide the audio in form of data into lsb bit of pixel of image and this encrypted image is further secured it using a password. At the decryption side the if the entered password is correct then ADS algorithm reverse the process of AES algorithm and separate the cover image and hidden data independently.

ENCRYPTION SIDE

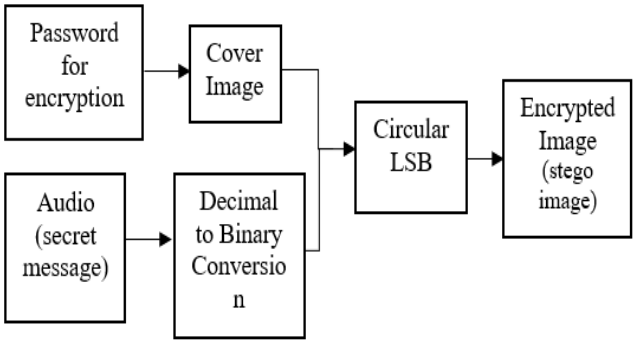

Fig. 1 Block diagram of encryption side

3.1 AES Algorithm

Advance Encryption Standard is an international standard algorithm for encryption. Data Encryption Standard (DES) is used to implement cryptographic techniques since long time, AES is the advanced technology development for DES which is based on block cipher. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

MATLAB is a Matrix-oriented programming language, which can beabsolutely used for thematrix-based Data-Structure of AES.

This can be used for encryption of randomly chosen plain text to chipper text. AES is a block cipher, same operations are performed in four cycles:

a. Add round key
b. Byte sub
c. Shift row
d. Mix column

The complete iteration of these four steps which is mentioned above is called round. The number of rounds depend on the size of key. And each round has several processing steps are: Sub Byte, Shift Rows, Mix Column and Add Round key.

3.2 Circular LSB Algorithm

The secret information(audio file) in form of decimal number is converted into binary form and these binary bits which is form of 0's and 1's is substituted in lsb bit of pixels of the cover image. This process of hiding for linear LSB varies from circular LSB technique.

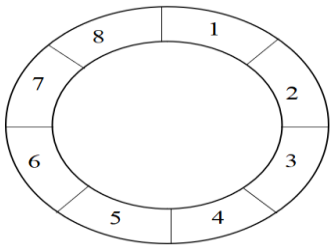

Fig. 2 Circular LSB frame format.

According to fig 2 in this any bit can be selected as LSB bit and accordingly the next adjacent bit will be MSB bit. This is advantage of circular LSB over linear LSB technique. Thus the way of hiding the data in the LSB bit of pixel of image is in circular layer form.

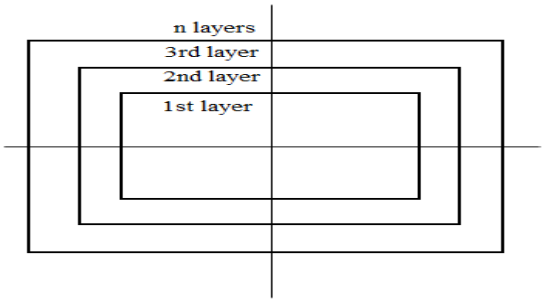

Fig. 3 Layer by layer hiding of data in cover image.

Initially in this algorithm according to amount of data to be hidden the no. of layer if fixed and the secret data in 0's and 1's is substituted in LSB bit of pixel of cover image. For example if layer =5, then in 5th layer the few secret data is hidden and as no. of frames in this layer is finished it goes to next layer i.e. 4th layer. And this process continues till all the data are hidden.

3.3 Secured Force Algorithm

This secured force algorithm is used to secure the secret data in the stego image using password. This way when unauthorized person try to decrypt the stego image will need a password to start with decryption process. Only after entering the correct password the process of decryption can be done. Thus the password in not encrypted into cover image but it just influence the hidden data, i.e. if password is correct hidden data can be retrieved else it cannot be retrieved.

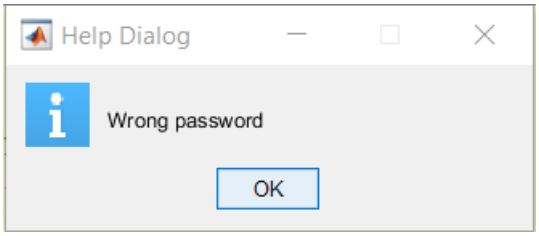

Fig.4 Dialog box is displayed if password entered is wrong

DECRYPTION SIDE

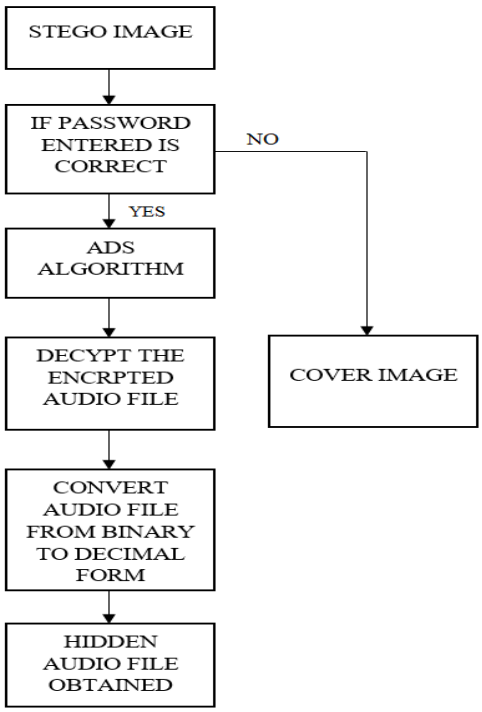

Fig. 5 Flow chart of decryption side

3.4 ADS Algorithm

The stego image or encrypted image undergoes decryption using ADS Algorithm i.e. Advance Decryption Standard Algorithm. This algorithm works in reverse manner to AES Algorithm. Initially this algorithm initiate the inverse of Circular LSB algorithm for example while encrypting the last layer in which data was hidden was in layer 1 so the decryption of 1st layer starts and continues till all the layer in which data is hidden is decrypted and hidden data is being retrieved.

And thus this helps to separate the stego-image as encrypted audio file and cover image.
This encrypted audio file which is form of binary bits as 0's and 1's is coverted back into decimal form, and then the secret audio can be heard.

4 REQUIREMENTS

The requirement for this project is mentioned as below software and hardware.

4.1 Software Requirement

Mat lab 2016(A)

MATLAB is a scientific programming language and provides strong mathematical and numerical support for the implementation of advanced algorithms. It is for this reason that MATLAB is widely used by the image processing and computer vision community. New algorithms are very likely to be implemented first in MATLAB, indeed they may only be available in MATLAB.

4.2 Hardware Requirement

Processor	:	Any processor above 2GHZ
RAM	:	2GB
Hard Disk	:	500GB and above

5 PERFORMANCE ANALYSIS

The performance of the proposed technique is analysed based on mean square error and peak signal to noise ratio.

5.1 Mean Square Error

One the main key parameter for analysing the quality of image before and after embedding process is Mean Square Error(MSE). This Mean Square Error represents the cumulative square error between the original image and encrypted image. Means Square Error is a risk function that represents the cumulative square error between compressed and original image.

$$MSE=1/MN\Sigma_{x=0}^{M-1}\Sigma_{y=0}^{N-1}((C(x,y)-S(x,y))^2$$

Where (x,y) are the two coordinates of image, (M,N) are two dimensions. So S(x,y) creates Stego-image and C(x,y) creates cover image.

5.2 Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR) represents peak error, the lower the MSE and higher the PSNR values indicates that the stego image quality is better than original.Image quality is observed using PSNR. Generally higher value of PSNR indicates that reconstructed image is of high quality. The PSNR between two images having 8 bits per pixel or sample in terms of decibels(dBs) is given by:

$$PSNR = 10 \log_{10}[Max^2/MSE]$$

Where MAX^2 = Max value of pixels in Original image

MSE = Mean Square Error

	MSE	PSNR
Original image	5.1922e-06	100.9773
Embedded image	2.2112e-04	84.6844

Table 1: Comparison of MSE and PSNR of Original and Embedded image

6 RESULT ANALYSIS

Below are the results and values obtained after the experiment i.e. implementation of Circular LSB technique in MATLAB.

ORIGINAL AND ENCRYPTED COVER IMAGE

Original image is cover image before encryption and encrypted image is cover image with secret data hidden under the lsb of this image i.e. cover image after encryption. The difference between these images cannot be identified with naked eyes.

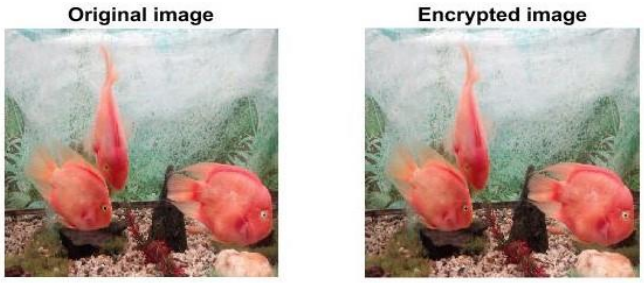

Fig.6 Original cover image and Encrypted cover image

HISTOGRAM OF ORIGINAL AND ENCRYPTED COVER IMAGE

Through this histogram of the original and embedded image it can be seen that the data which is hidden in the cover image i.e. stego image and original cove image has very less difference. Thus it becomes difficult for (HVS) Human Visual System to identify the hidden secret data.

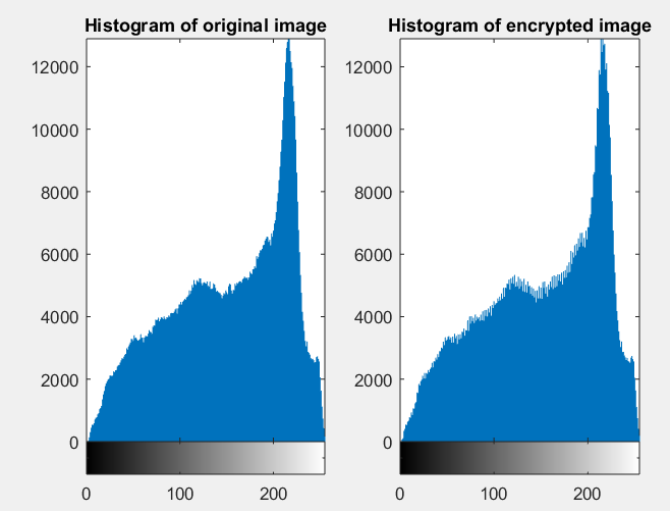

Fig. 7 Histogram of original cover image and Encrypted cover image

CONCLUSION

This paper present a more efficient way for hiding secret data into an image and also provides a more secure way of secret communication. Also a novel way of hiding an audio signal into colour image and transmitting through more secured way. This also prevent attackers from hacking the hidden data into the cover medium because only using password the decryption process can be carried out on stego image.

REFERENCE

1. Beenish Siddiquiand Sudhi Goswami, "A Survey On Image Steganography Using LSB Substitution Technique" International Research Journal of Engineering and Technology Volume:04 Issue:05|May-2017.

2. F.C.Er and E. Gul, "Comparison of digital audio watermarking techniques for the security of voip communications," in Information Assurance and Security (IAS), 2011 7th International Conference on. IEEE, 2011, pp. 13–18.

3. Y.F.Huang, S. Tang, and J. Yuan, "Steganography in inactive frames of voip streams encoded by source codec," Information Forensics and Security, IEEE Transactions on, vol. 6, no. 2, pp. 296–306, 2011.

4. Y.Huang, C. Liu, S. Tang, and S. Bai, "Steganography integration into a low-bit rate speech codec," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 6, pp. 1865–1875, 2012.

5. A.Valizadeh and Z. J. Wang, "An improved multiplicative spread spectrum embedding scheme for data hiding," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 4, pp. 1127–1143, 2012.

6. Y.Huang, S. Tang, and Y. Zhang, "Detection of covert voice-over internet protocol communications using sliding window-based steganalysis," Communications, IET, vol. 5, no. 7, pp. 929–936, 2011.

7. S.T. Yong feng Huang and Y. J. Y. Chunlai Bao, "Steganalysis of compressed speech to detect covert voip channels," IET Information Security, vol. 5, no. 1, pp. 1–7, 2011.

8. A.Valizadeh and Z. J. Wang, "Efficient blind decoders for additive spread spectrum embedding based data hiding," EURASIP Journal on Advances in Signal Processing, vol. 2012, no. 1, pp. 1–21, 2012.

9. M. Boloursaz, R. Kazemi, B. Barazandeh, and F. Behnia, "Bounds on compressed voice channel capacity," in Communication and Information Theory (IWCIT), 2014 Iran Workshop on. IEEE, 2014, pp. 1–6.

10. W. Mazurczyk, "Voip steganography and its detectiona survey," ACM Computing Surveys (CSUR), vol. 46, no. 2, p. 20, 2013.

11. Ankitha Gangwar and Vishal Shrivastava, "Improved RGB-LSB steganography using Secret Key" International Journal of Computer Trends and Technology-vVolume 4 Issue 2- 2013

BIOGRAPHIES

B.G.AAGARSANA,
PURSUING DEGREE IN B.E/ECE, JEPPIAAR SRR ENGINEERING COLLEGE, AFFLIATED ANNA UNIVERSITY COLLEGE, TAMIL NADU,INDIA

ANJALI
PURSUING DEGREE IN B.E/ECE,JEPPIAAR SRR ENGINEERING COLLEGE, AFFLIATED ANNA UNIVERSITY COLLEGE, TAMIL NADU,INDIA

T.K.KIRTHIKA
PURSUING DEGREE IN B.E/ECE,JEPPIAAR SRR ENGINEERING COLLEGE, AFFLIATED ANNA UNIVERSITY COLLEGE, TAMIL NADU,INDIA

Mr.S. SIVA KUMAR/M.E.
HOD OF ECE DEPARTMENT, JEPPIAAR SRR ENGINEERING COLLEGE, AFFLIATED ANNA UNIVERSITY COLLEGE, TAMIL NADU,INDIA