iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Analysis of Video/Image Steganography Using Encrypted Audio

Kanu Raj Singh[1], Pawanesh Abrol[2]
[1,2] *Department of Computer Science and IT, University of Jammu, Jammu and Kashmir, India.*

Abstract: Steganography is the art of transmitting data by hiding it in a cover medium. Video steganography where video frame is used as a cover media for hiding the data. Limitation of steganography is that amount of data that can be hidden tends is restricted by the size of the medium. Advantage of Video Steganography is that sequence of frames extracted from video is unknown to the attacker. Audio data is one of the various data to be hidden. Different types of Steganographic methods can be used for data hiding.

In proposed paper video is used as a cover media and audio message is hidden in video frame where audio message is encrypted with the help of bitXOR encryption technique and encrypted audio will be embedded into the selected video frame. Standard algorithm such as LSB (Least Significant Bit) is used for hiding the data in video frame. Different steganographic algorithms are also analysed of which LSB algorithm is used for hiding the data. As LSB algorithm is used to hide the data into cover medium, the advantage of using LSB algorithm is that the only single bit of single pixel of cover medium is replaced with the bits of data to be hidden.

Keywords: Cryptography; Steganography; LSB; Matlab; Encryption.

I. INTRODUCTION

With the growth of internet and communication techniques in recent years the security of the sensitive data has become of prime and supreme importance. To protect this data from unwanted access various methods for data hiding like cryptography, hashing, authentication, steganography have been developed and used and are in practice today. Cryptography is concealing the content of the message.

This word is derived from Greek word *kryptos m*eaning hidden. Steganography is the art of transmitting data by hiding it in a cover medium such as image, video, audio. The word is derived from two Greek words *steganos* means "covered or concealed" and *graphein* means "writing". There are various types of cryptography such as Symmetric and Asymmetric cryptography.

In this paper bitXOR encryption technique is used to encrypt the file**.** The various uses of Cryptography are secrecy in transmission, secrecy in storage, transmission integrity, storage integrity, digital signatures. These are some of the uses of cryptography. For example, to transmit information to a colleague by E-mail, the sender encrypts the information to make it confidential and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender's digital signature and decrypts the information using the Corresponding decryption key. By applying cryptographic techniques we can securely transmit our data. The main aim of this paper is to achieve security achieved with the help of Cryptography and LSB steganography techniques.

II. PREVIOUS WORK

A. Asok [1]

proposed technique in which AES is used to encrypt audio signals and key is generated from iris image. Security of audio signals is achieved with the help of encryption. Iris key is converted into binary code for the formulation of secret key. Key with randomness is chosen for improvement in security. Different tests are also performed to check randomness of generated key.

B. Bhojane, Khodke [2]

gave approach of hiding text data in video frames using higher least significant bit algorithm. Selected frame is divided into four images and then data is hidden into the five LSB bits of each pixel in carrier image. Generated key is stored into last pixel of the carrier image. This approach uses 5 bits to be used to increase payload capacity and this approach also provides good security.

C. Almara'beh [3]

©IJRASET: All Rights are Reserved

gave a general review of steganography and different techniques to be used for video steganography and audio steganography. He concluded that a wide variety of audio and video steganography techniques such as DWT, DCT, and LSB helps to improve security.

D. Yadav [4]

proposed approach in which video is embedded into the host video. The secret video to be hidden is converted into binary bits and then encrypted with the help of symmetric XOR encryption before embedding. Also each bit of secret frames will be stored following pattern BGRRGBGR. Also there is no distortion in the host video and recovered secret video is also acceptable.

E. Gupta, Chaturvedi [5]

used video as a cover media and the images are converted into text that is to be embedded into the video frames. Also AVI video format is used where 1 LSB, 2 LSB and 3 LSB of each pixel are replaced and then AES encryption is applied. Since AES is used so it is difficult for intruder to easily hack important information.

F. Lalengmawia [6]

put forward a technique in which an image is used to hide other image. Firstly AES algorithm is used to find the random pixel positions to be embedded. After this another algorithm is used to find position of bits where embedding is to be performed and then embedding algorithm is used for embedding bits into these positions. The generated stego image is good enough to prevent any suspicious arousal.

G. Pillai et al. [7]

proposed an image steganography technique in which image is divided into different segments. K means clustering is used for segmentation of the image. Text to be embedded into the clusters of image is encrypted with the help of DES and then embedded into the segments of image using LSB technique. The combination of cryptography and clustering is used along with steganography in which encrypted text is hidden in each of clusters which reduces the possibility of message being found.

H. Usha [8]

proposed a technique in which message is first encrypted using play fair cipher and then encrypted text is again encrypted using AES encryption. After this second cipher text is embedded into the image using LSB encoding. Reference matrix is used to obtain the key for LSB encoding. The matrix consists of several keys listed out. Also length of the plaintext is also encrypted and then sent for greater security.

I. SaiKrishna [9]

proposed a way in which a message is selected and then a cover image is selected and clustered with the help of k means clustering algorithm. After this message is embedded into the clusters of cover image. They concluded that strength of their approach depends upon number of clusters and pixels to be selected for embedding.

J. Conclusion:

Observed the scope for analyzing the possibility of embedding the encrypted audio into a select frame of a given video and then decrypting it. The effect of size of audio encryption technique, frame selecting procedure may have impact on the strength of the encryption**.**

III. METHODOLOGY

On the basis of the outcome of literature review a framework has been proposed for encryption and decryption of the given audio in the selected video frame. For further strengthening of encryption process the audio is encrypted using bitXOR. Further single frame from the given video has been randomly selected.The detailed methodology has been shown in Fig 1.

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

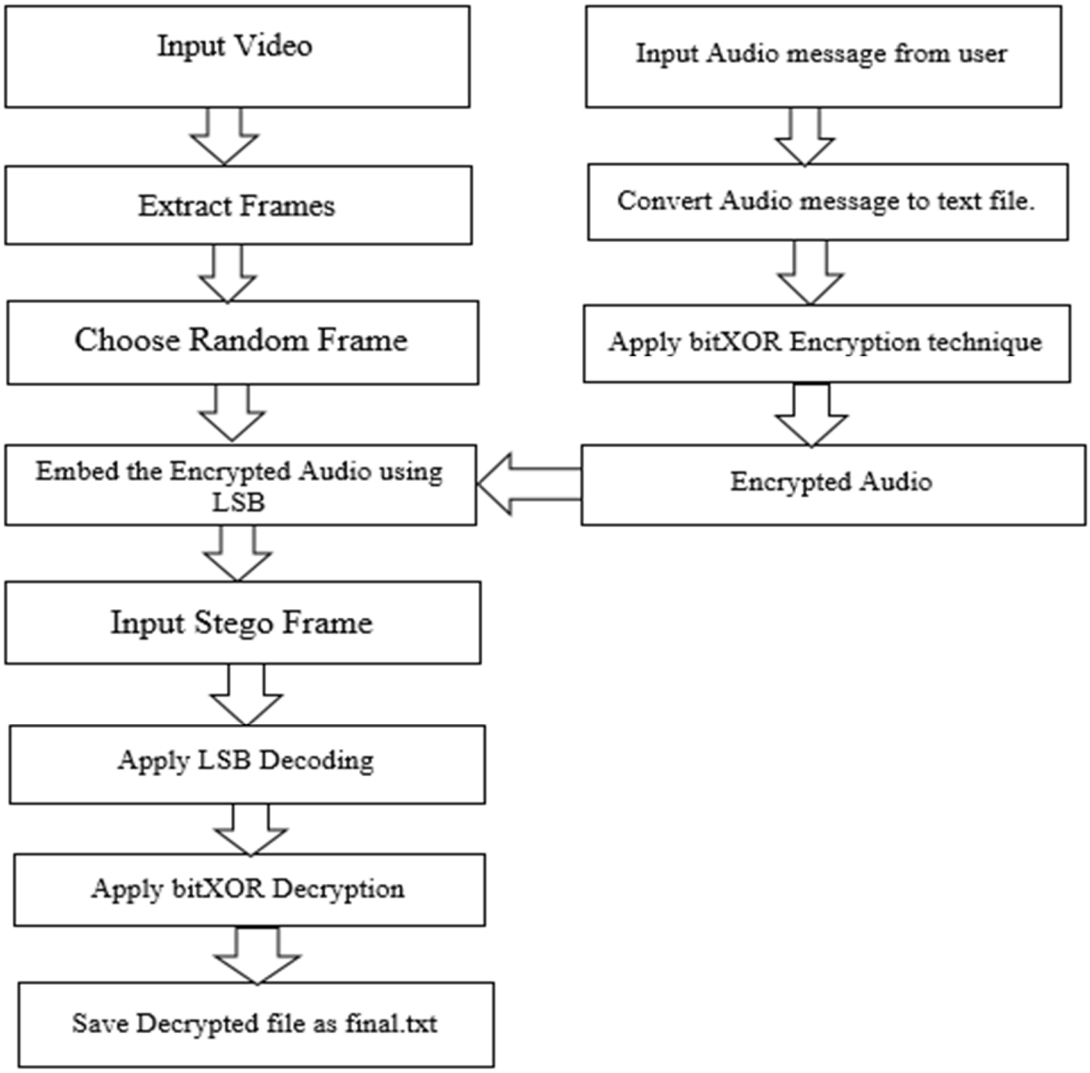


Fig.1. Encryption and Decryption

A. Frame extraction

Random video of different formats such as .mp4, .avi etc. to take and the video frames are extracted in a particular folder. After this a particular video frame is selected with the help of 'randi' function in Matlab 2016a.

```
frsttym = 4000;
Random_Selection = randi ([1 frsttym], 1);
Img_L=imread(strcat('Extract_Frames/',num2str (Random_Selection),'.jpg'));
Figure, imshow (Img_L);
Imwrite (Img_L,'extract.jpg');
```

B. LSB embedding

LSB means Least Significant Bit in which every LSB bit of cover image i.e., selected video frame is replaced with the bit of message to be hidden. Hiding a message with steganography reduces the chance of message being detected and in this paper Cryptography along with Steganography is used for improved security.

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Binary (Decimal: 149)	1	0	0	1	0	1	0	1
Bit weight for given bit position n (2^n)	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Bit position label	MSB	—	—	—	—	—	—	LSB

Fig. 2. LSB and MSB bits

IV. RESULTS

The main objective of this paper is to successfully encrypt and embed the audio text file into the selected video frame. First a random video frame is selected. Selected random frame is as shown in Fig. 3.

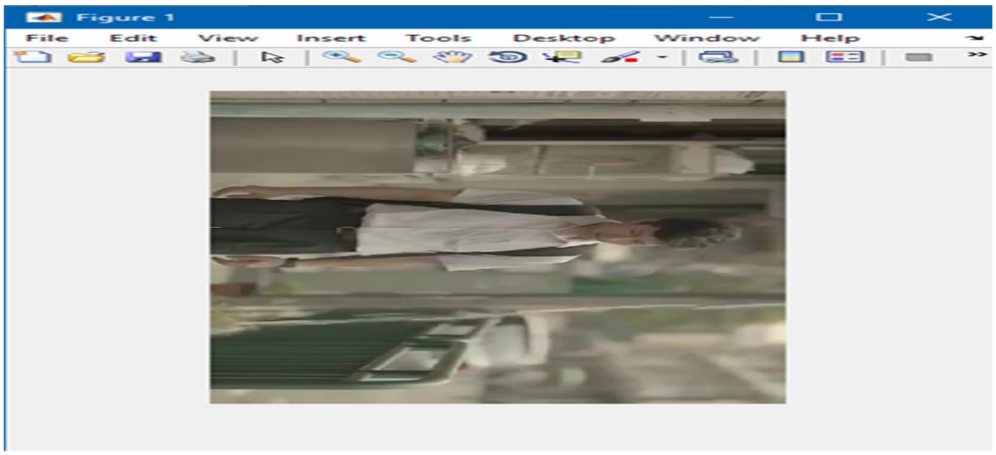


Fig. 3. Selected video frame

After selecting random frame the audio file (.mp3) is selected and saved as a text file. It is necessary to first convert and save audio file as a text file. Audio formats used may include .mp3, .wav etc. for conversion.

```
fid = fopen ('message.txt', 'wt');
 fprintf (fid,'%d', message);
 fclose (fid);
```

The code above shows the audio saved as a text file. Fig. 4 shows the audio file saved as text file.

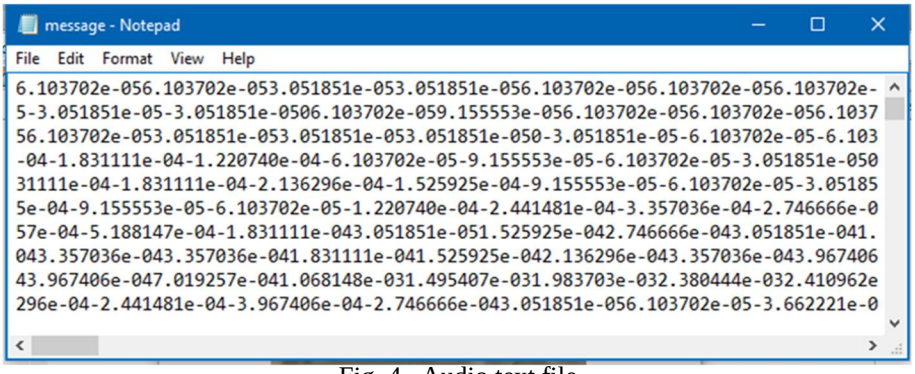


Fig. 4. Audio text file

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

After saving the audio as text file the next step is to encrypt and hide the text file into the selected video frame. Bitwise XOR is used to encrypt the audio text file and LSB steganography is used to hide the file into the selected frame.
To successfully obtain hiding and achieving security of data the size of selected video frame should be larger than audio text file.

Let Size2=Size of audio text file.

Let Size1=Size of selected frame.

So, Size1>Size2 for hiding data.

Fig.5 shows the encrypted text file obtained after encrypting the audio text file using bitXOR encryption technique.

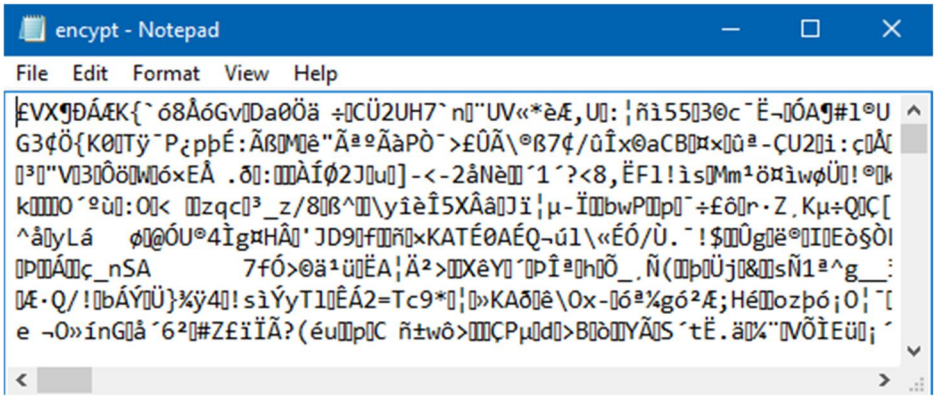


Fig. 5. Encrypted text file

After encryption of text file the file is embedded into the selected video frame as shown in the Fig. 3.Fig. 6 shows the video frame after hiding the audio data using LSB data hiding technique.

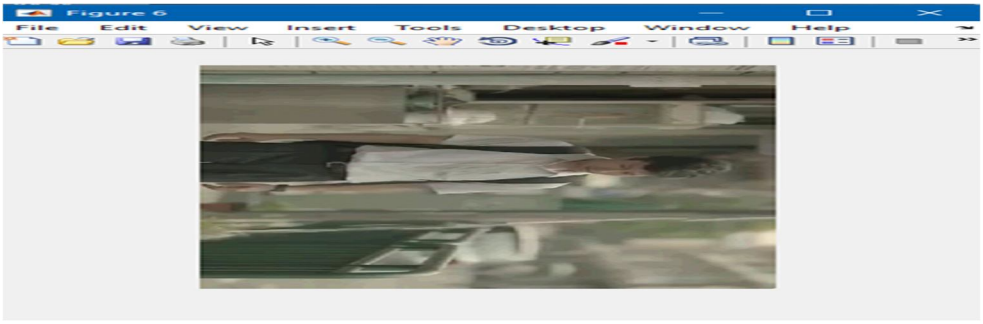


Fig. 6. LSB embedded frame.

Fig. 7 shows the dialog box providing confirmation about the audio data hidden successfully in the selected video frame.

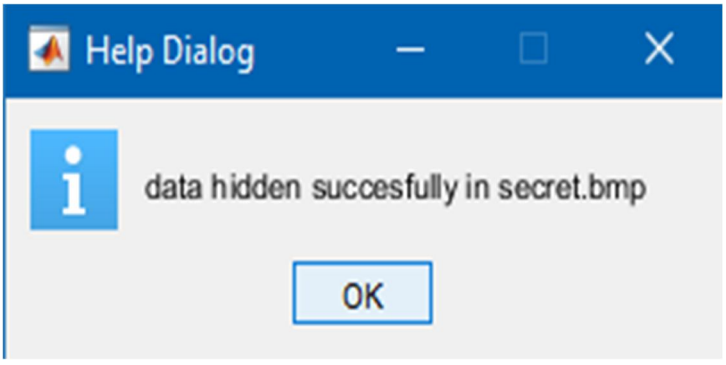


Fig. 7. Prompted dialog box

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

The Fig.8 shows the plot of the audio successfully hidden into the selected video frame.

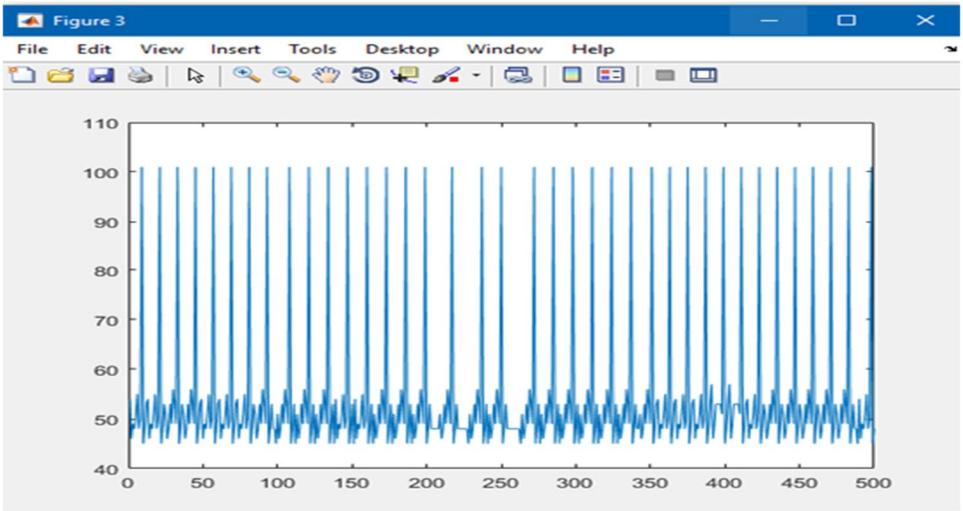


Fig. 8. Audio file plot.

Table 1 shows mp4 format video and three different types of audio format hidden successfully into the stego frame.

TABLE 1.
Showed different audio formats hidden in .mp4 and .3gp Video file

Video	Random frame	Stego frame	Audio Plot
V1 (.mp4)	102 KB 102 KB 102 KB	.mp3 159 KB .wav 159 KB .flac 159 KB	.mp3 audio plot .wav audio plot .flac audio plot
V2 (.3gp)	160 KB 160 KB 160 KB	208 KB 191 KB 191 KB	.mp3 audio file .wav audio file .flac audio file

Decryption process is applied in order to retrieve the hidden text file. LSB embedded frame is selected in order to retrieve the hidden audio text file.

Fig. 9 shows the successfully encrypted audio text file obtained after LSB decoding of stego frame.

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

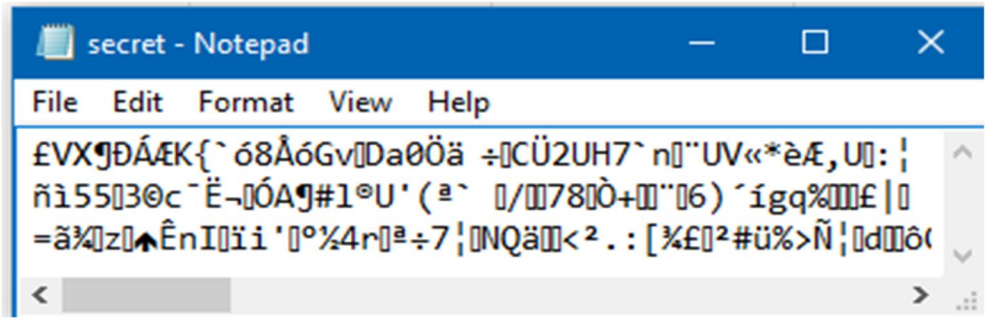


Fig. 10 shows the audio file obtained after successful decryption of the audio file and saved as final.txt.

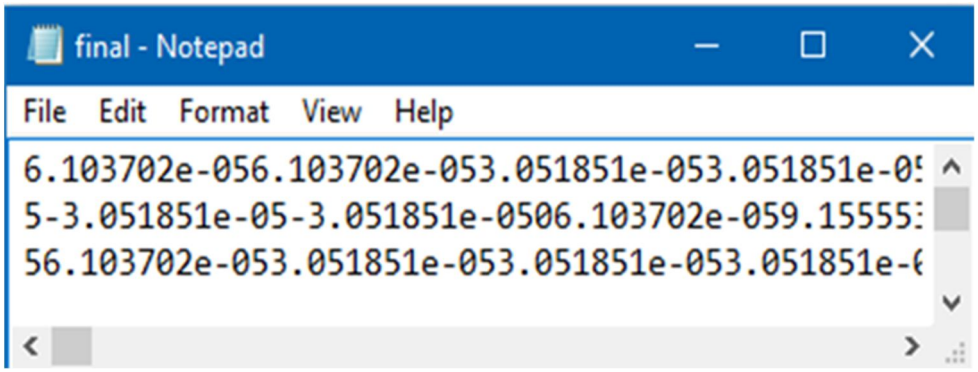


Fig. 10. Audio Decrypted file.

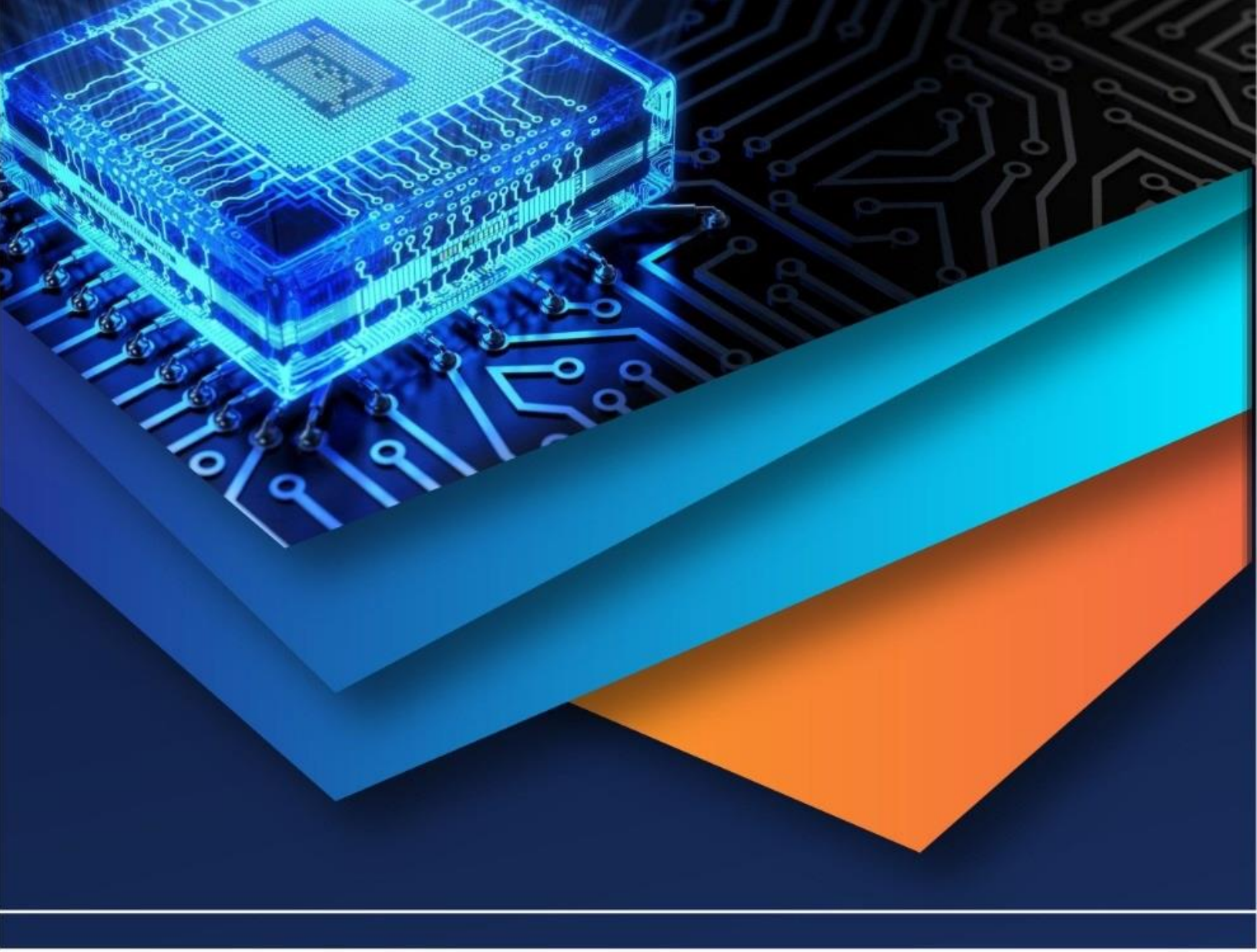
V. CONCLUSION AND FUTURE SCOPE

In this paper LSB embedding and bitXOR technique is used to embed and encrypt the file. The audio is read and saved as text file. The audio text file prior encryption and after decryption is always identical. The size of audio file must be chosen properly as it should be less than selected stego frame. Otherwise the results may produce errors. From the future examination perspective more developed encryption techniques such as AES, RSA etc. can be used to achieve more accuracy. The other techniques such as jsteg algorithm may be used for embedding the file into frame.

REFERENCES

[1] Sruthi B. Asok , P. Karthigaikumar, Sandhya R, Naveen Jarold K, N.M Siva Mangai, “A Secure Cryptographic Scheme for Audio Signals,” International conference on Communication and Signal Processing, IEEE,India,2013.
[2] Miss Amruta B. Bhojane, Prof. Priti A. Khodke, “Data Hiding In Video Stream by Text Substitution,” International Journal of Science, Engineering and Technology, IJSET, 2013.
[3] Hilal Almara'beh, “Steganography Techniques - Data Security Using Audio and Video,” International Journal of Advanced Research in Computer Science and Software Engineering, 2016.
[4] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma, “A Secure Video Steganography with Encryption Based on LSB Technique,” International Conference on Computational Intelligence and Computing Research, IEEE, 2013
[5] Hemant Gupta, Dr. Setu Chaturvedi, “Video Data Hiding Through LSB Substitution Technique,” International Journal Of Engineering And Science, 2013
[6] C. Lalengmawia*, A. Bhattacharya, Member, IEEE and A. Datta, “Image Steganography using Advanced Encryption Standard for Implantation of Audio/Video Data,” Fifth International Conference on Recent Trends in Information Technology, 2016
[7] Bhagya Pillai, Mundra Mounika, Pooja J Rao, Padmamala Sriram, “Image Steganography Method Using K-Means Clustering and Encryption Techniques,” Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016
[8] S Ushll, G A Sathish Kumal, K Boopathybagan, “A Secure Triple Level Encryption Method Using Cryptography and Steganography,” International Conference on Computer Science and Network Technology, IEEE, 2011
[9] A.SaiKrishna/Shankar Parimi, G.Manikandan, Sairam.N, “A Clustering Based Steganographic Approach for Secure Data Communication,” International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)