Application of Data hiding using Anti-Forensic Technique

[1] *Prof. D.J.Bonde, Department of Computer Engineering, MMIT Lohgaon, Maharastra,India*
[2] *Shinde Govind Narayan, Department of Computer Engineering, MMIT Lohgaon, Maharastra,India*
[3] *Salunkhe Vaishali Pandharinath, Department of Computer Engineering, MMIT Lohgaon, Maharastra,India*
[4] *Shete Puja Pandurang, Department of Computer Engineering, MMIT Lohgaon, Maharastra,India*
[5] *Shinde Rupesh Tanaji, Department of Computer Engineering, MMIT Lohgaon, Maharastra,India*

Abstract - ***Steganography is art and science of hiding data.Our propose system proposed combinations of Audio and video steganography using Anti forensics techniques. The main aim is to hide information in both image and audio of video files. Forbidden Zone Data Hiding(FZDH) is used for image steganography and phase Coding algorithm is used for Audio Steganography. Security is preserved with the process of histogram matching and PSNR at both sender and receiver side which are exactly matching to increase security. Also computer forensics technique used at receiver side to cross check security hence data is more secured.***

Key Words: FZDH,*LSB,Phase coding technique,Anti-Forensics Technique*,PSNR,Histrogram.

1. INTRODUCTION

The art and science of hiding information by embedding messages within other files,Also steganography is hide communication or message from a third party.Steganography works by replacing bit of useless or unused data in regular computer files(such as graphics,sound,text)with bits of different,invisible information. Now a day cyber crime is increase to avoid this crime and to protect our personal information computer forensic methods are used.In proposed work,we used FZDH and Phase coding algorithm instead of LSB and Watermarking techniques.System has ability to hide more data because it includes both image and audio steganography which increases security.FZDH is (Forbidden Zone Data Hiding) in which no change is available at the time of data hiding proess[1].In Phase coding technique split the original audio into blocks and hide authenticate data into first block.This authenticate data is not spared over entire file,So attacker remove or crop easily.In our proposed work phase coding technique work as follow,Splite the audio file whose length is equal to size of data with embedded message.Then apply Discrete Fourier Transform(DFT) on each segment and insert secrete data into that segment.

2.Related Work

In proposed work AntiForensic technique used to increased security and hiding capacity. Embedded signature data is reconstructed without knowing original host video by using Watermarking technique also can be viewed simply as an extension of image watermarking[2].
In next invention, to avoid extraction error use of lifting wavlet because of using this Pseudo noise sequence is generated and that is essential for more data hiding[3].
Select audio video file. From this file audio and video frames are separated. In audio file text data hide using phase coding algorithm and in video file image is hide using FZDH.Video is nothing but collection of audio and video frames, In video file authenticate image hide in selected frame number and text data is hide behind audio file.Then combine this audio and video frams is called "Stego video."As shown in fig.1. Then this stego video is send to the sever..

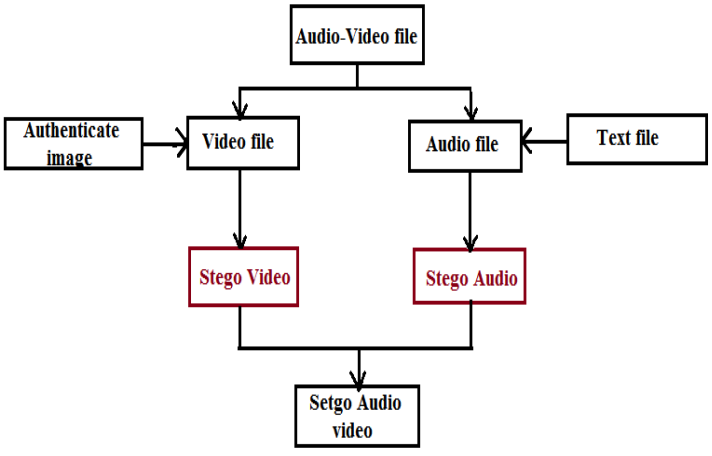

Fig -1: Sender Side

Receiver receive this stego video and enter frame number.It shoud be same both the transmitter and receiver side.When this frame number is same then only authenticate data received by receiver otherwise discarded.As shown in Fig.2. receive authenticate data otherwise discarded.And finally receiver decode the

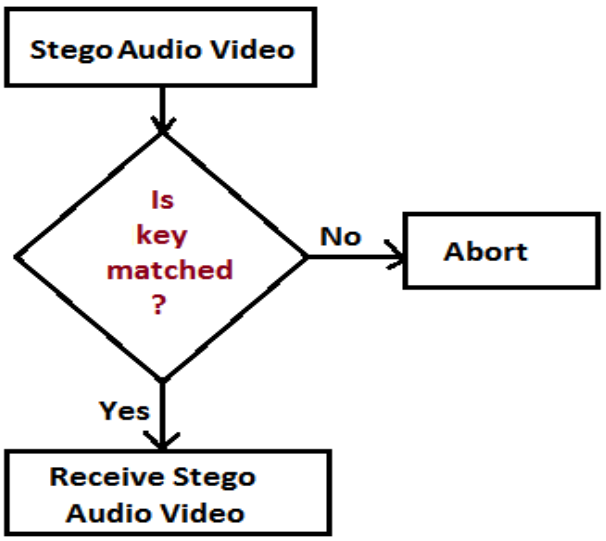

Fig -2: Autentication at receiver side

At receiver side both histrogram and PSNR value are check.When both this are same at transmitter and receiver then only receiver authenticate image from the video file and decode the text from audio file.As shown in fig.3.

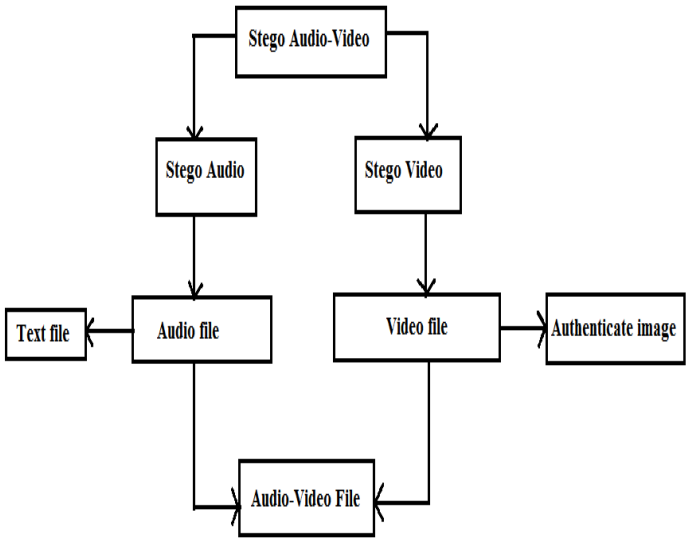

Fig -3: Receiver Side

An Audio-video cryptoadaptive with optical steganography technique also Adaptive Steganography(AS) is used for Audio-Video sequence encryption and decryption. In that Double Random phase encoding algorithm and Asymmetric Encryption method are applied. Due to this method wastage of memory and time[4].Computer forensic technique used to find parameters like histrogram,PSNR at both the sender and receiver side.PSNR is peak signal to noise ratio.It is used to measure quality between original image and comprssed image.When image is compressed then noise or error is produced to reduced this noise PSNR is used.Higher value of PSNR is better for reconstructed image.

3.Overall System Flow

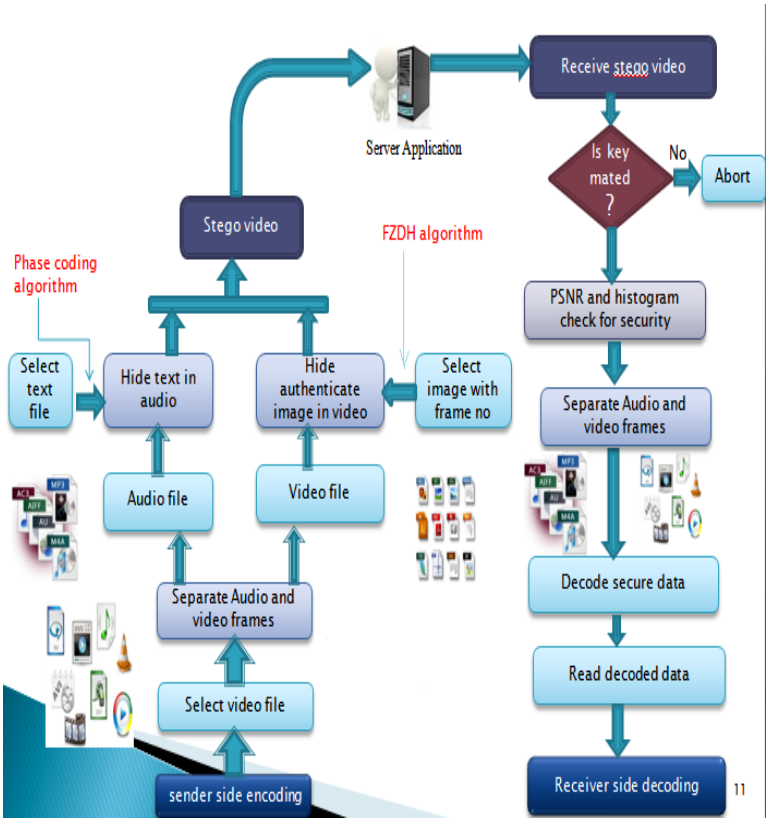

Fig -4:Overall Architecture

4.Algorithm

At Sender Side

1.Select any audio-video file.
2.Seperate audio file and video file.
3.Seprate video file into number of frames.
4.Select frame number from selected video file, for hiding authenticate image using FZDH algorithm.
5.Similarly,hide text data behind Audio file using Phase Coding algorithm.
6.Combine Stego Audio and Stego Video to Generate Stego Audio-Video.

At Receiver Side

1.Receive Stego Audio-Video.
2.Seperate stego Audio-Video into audio file and video file.

3.Enter frame number(i.e,pass key).If that frame number is identical for both sides goto 4.
otherwise abort.
4.Authentication for extracting hidden data from stego Audio-Video file.
5.Check PSNR and Histrogram are either identical or not,If found identical goto 6,else abort.
6.Receiver extract authenticate information successfully.

4. EXPECTED RESULT

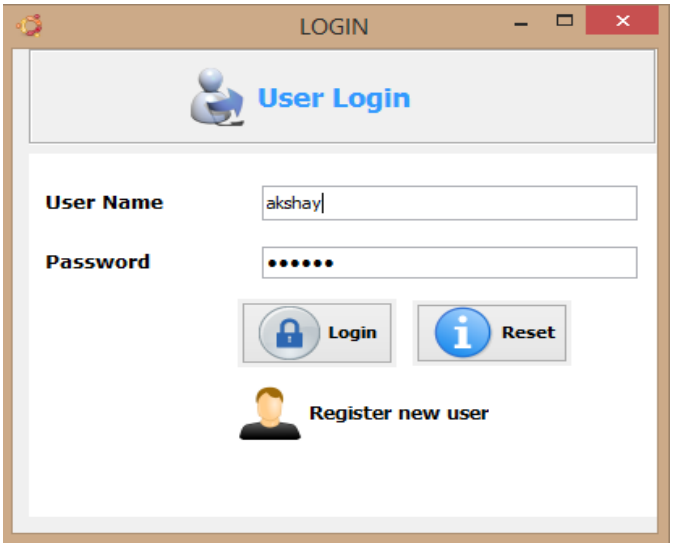

Fig -5: User Authentication

Fig -6: Transmitter Side

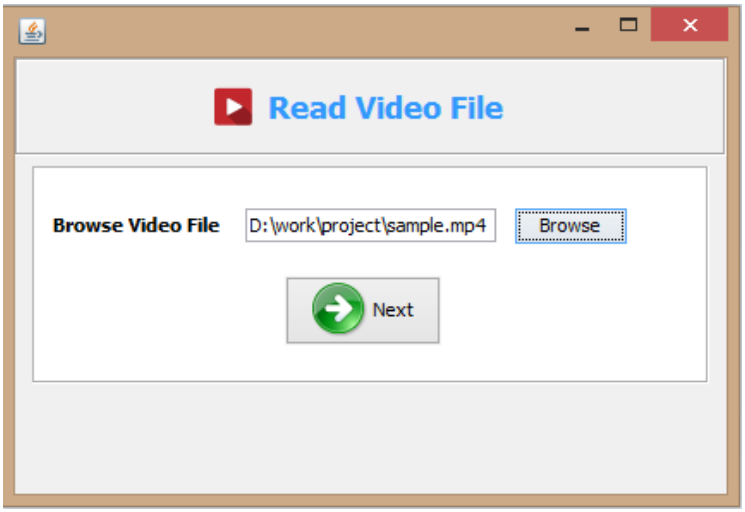

Fig -7: Select video

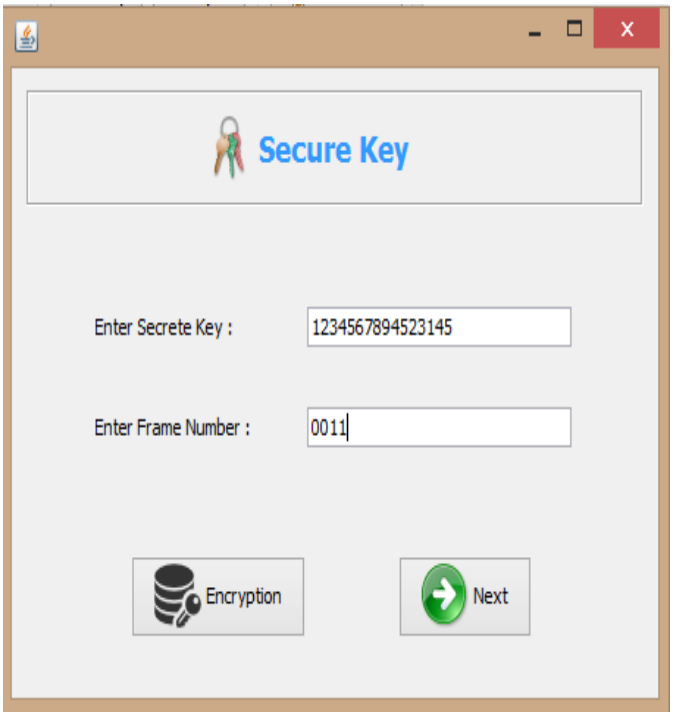

Fig -8: Provide Authentication

5. CONCLUSIONS

Hiding image and text behind audio and video file and extracted from an AVI file using FZDH method for video steganography and phase coding.Information security using data hiding audio video steganography with the help

of computer forensic techniques provide better hiding capacity and security.

REFERENCES

[1] K.Mohan,S.E.Neelakandan,"Secured robust video data hiding using symmetric encryption algorithms", International Journal of Innovative Research in Engineering & Science (December 2012].

[2] Arup Kumar Bhaumik,Minkya Choi "Data hiding in video"IEEE international journal of database a application june 2009.

[3] M,Pooyam,A,Delforouzi "LSB based steganography method based on lifting wavelet transform"2007 IEEE International symposium on signal processing and information technology,pp600-603

[4] Sghaier Guizni,Nidal Naser,"An Audio/Video Crypto Adaptive Optical stegnography Technique"IEEE 2012