Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 5, May-2018

Reversible Data Hiding Methods Based on Audio and Video Synchronization

Mr.Vikram Ramekar, Mr. Mandar Pathak, Mr. Viraj Shirke, Mr. Prince Chaturvedi

Project guide: Prof. Kiran Somase

Department of Computer Engineering

Abstract — Steganography is the technique for concealing any mystery data like secret key, content, and picture, sound behind unique spread record. In this paper we proposed the sound feature crypto-steganography which is the blend of picture steganography and sound steganography utilizing PC crime scene investigation method as an instrument for confirmation. Our point is to shroud mystery data behind picture and sound of feature document. As feature is the use of numerous still edges of pictures and sound, we can choose any casing of feature and sound for concealing our mystery information. Suitable calculation, for example, 4LSB is utilized for picture steganography and stage coding calculation for sound steganography. Suitable parameter of security and verification like PSNR, histogram are acquired at collector and transmitter side which are precisely indistinguishable, subsequently information security can be expanded. This paper center the thought of PC criminology method and its utilization of feature steganography in both investigative and security way

Keywords- *Data Hiding , Steganography , Computer forensics , Histogram ,PSNR*

I.INTRODUCTION

Steganography truly means secured written work. Its will probably shroud the way that correspondence is occurring. This is regularly accomplished by utilizing a (fairly extensive) spread document and implanting the (somewhat short) mystery message into this record. The outcome is a harmless looking record (the stegofile) that contains the mystery message. Presently, it is increasing new ubiquity with the momentum business requests for advanced watermarking and fingerprinting of sound and feature Steganography has seen exponential use following the 1990s. Stegoalgorithm downloads are currently accessible on the Internet as shareware. Governments, military, organizations, and private subjects everywhere throughout the world now utilize steganography for security and protection reason. The music and film commercial enterprises ceaselessly devise new material control techniques, for example, reserving early conveyance of motion picture screenings through steganography.

Government, military, businesses, and private citizens all over the world now use the steganography for security and privacy purpose.The music and movie industries continually device new material control methods such as early distribution of movie screening via steganography . For every nation it has primary need to secure its border lines as well as the communication methods which field are now majorly favored area of interest and importance . As majorly the communication is through internet it has be come prime necessity for every nation to adopt some counter measure to foul use of internets. Recently cyber crime is also increasing exponentially and to avoid such a computer forensic such as digital forensic have been developing rapidly due to advance in computer system data storage device

II.LITERATURE SURVEY

1.PAPER NAME: Data Hiding in Video

AUTHORS: Arup kumarBhaumik, Minkyachoi,

We propose a video information embedding theme during which the embedded signature information is reconstructed while not knowing the first host video. The planned technique allows a high rate of information embedding and is strong to motion stipendiary secret writing, like MPEG-2. Embedding is predicated on texture masking and utilizes a multi-dimensional lattice structure for cryptography signature info. Signature information is embedded in individual video frames mistreatment the block DCT. The embedded frames square measure then MPEG-2 coded. At the receiver each the host and signature pictures square measure recovered from the embedded bit stream. we have a tendency to gift samples of embedding image and video in video

2.PAPER NAME: Information Hiding in BMP Image Implementation, analysis Evaluation

AUTHORS: Alkhraisathabes.

Steganography comes from the Greek words steganos, roughly translating to cov- ered writing. Steganographic techniques enable one party to speak data to a different while not a 3rd party even knowing that the communication is happening. The ways in which todeliver these secret messages vary greatly. This paper explores many strategies well, andattempts to check them go into code, and in apply, through many examples.The goal of steganography is to cover messages within different harmless messages in an exceedingly manner thatdoes not enable any enemy to even sight that there's a second secret message gift.

3.PAPER NAME: Data hiding in audio signal, video signal text and JPEG Image
AUTHORS:V.Sathya, k Balsubramaniyam, N, Murali DIT,Pimpri,
Steganography suggests that concealing a message. info concealing technique may be a new quite secret communication technology. info concealing system uses transmission objects like audio, pictures and text. Digital audio, images, text ar progressively equipped characteristic however insensible marks, which can contain a hidden copyright notice or serial range or maybe facilitate to forestall unauthorized repetition directly. nowadays the expansion within the info technology, particularly in pc networks like net, mobile communication and digital transmission applications like camera, telephone set video etc.
4.PAPER NAME: A Detection algorithm of audio spared spectrum data hiding
AUTHORS:S. Gao, R. M. Zeng H. Jai,A
In this paper, a method of passive steganalysis is proposed. We focus on detecting the existing of data hidden in audio files with spread spectrum (SS) data hiding. SS data hiding is considered as a process of adding noise. The technology of classifier and feature vector extraction are used to achieve the detection. First, we divide an audio signal into several frames. The wavelet coefficients before and after wavelet de-noise in each frame are calculated. Then, we pick some stat, of their difference as the feature vectors of the audio signal. Finally, according to the feature vectors of the audio signal, classifier will decide whether the audio signal have been processed by SS or not. In our experiment, support vector machines (SVM) play role of classifier, 600 audio files are used to be our experiment samples. After the feature vectors of all the samples are calculated, those feature vectors of samples are divided into two parts. One is testing part and the other is training part. The result of experiment shows that if the strength of data hiding is higher than 0.005, the rate of correct detection of training part is higher than 86.5
5.PAPER NAME: Applying public key watermarking technique in forensic imaging to preserve the authenticity of the evidence
AUTHORS: Wen Chao Yang, Che Yen Wen.
The traditional verifying evidence method in court is to check the integrity of the chain of custody of evidence. However, since the digital image can be easily transferred by Internet, it is not easy for us to keep the integrity of the chain of custody.In this article, we use the PKI (PublicKey Infrastructure), Public-Key Cryptography and watermark techniques to design a novel testing and verifying method of digital images. The main strategy of the article is to embed encryption watermarks in the least significant bit (LSB) of digital images. With the designed method, we can check the integrity of digital images by correcting public-key without side information and protecting the watermarks without tampering or forging, even the embedded method is open. Finally the proposed method can be applied in court to digital evidence testing and verification, and used to check the admissibility of digital image.

III. System architecture

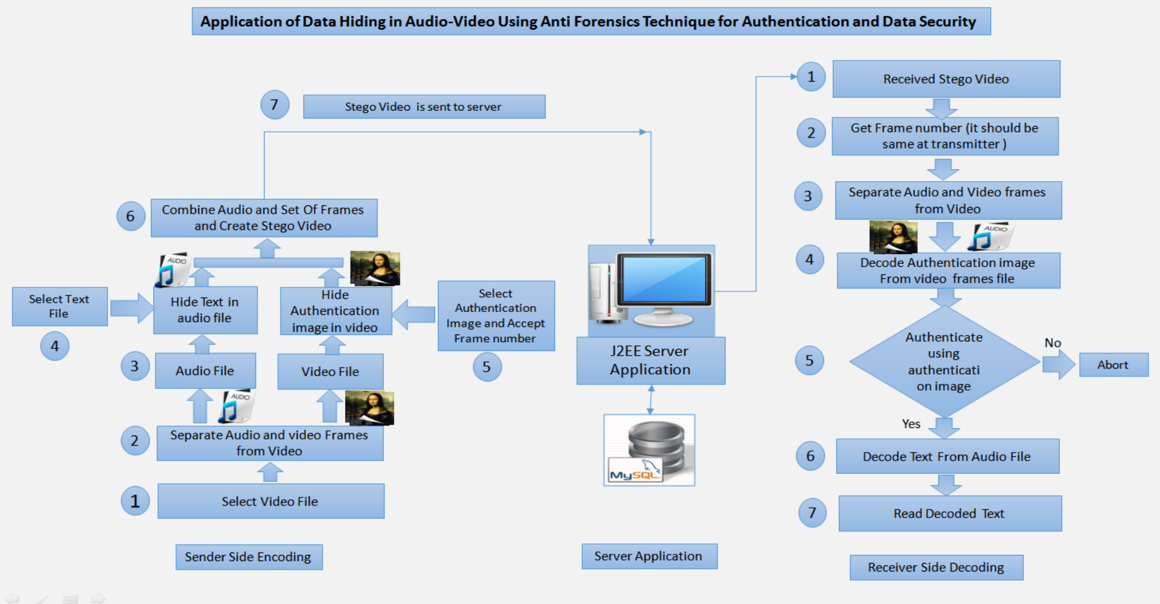

Application of Data Hiding in Audio-Video Using Anti Forensics Technique for Authentication and Data Security
7
Stego Video is sent to server
6
Combine Audio and Set Of Frames and Create Stego Video
Select Text File
4
Hide Text in audio file
Hide Authentication image in video
Select Authentication Image and Accept Frame number
5
3
Audio File
Video File
2
Separate Audio and video Frames from Video
1
Select Video File
Sender Side Encoding
J2EE Server Application
Server Application
1
Received Stego Video
2
Get Frame number (it should be same at transmitter)
3
Separate Audio and Video frames from Video
4
Decode Authentication image From video frames file
5
Authenticate using authenticati on image
No
Abort
Yes
6
Decode Text From Audio File
7
Read Decoded Text
Receiver Side Decoding

Figure: System Architecture

IV. Proposed System

- The proposed system describes a data hiding method that is reversible, if the original cover content can be perfectly recovered from the cover version containing embedded data. even though a slight distortion has been introduced in data embedding procedure. A number of mechanisms, such as difference expansion, histogram shift and lossless compression, have been employed to develop the reversible data hiding techniques for digital images.
- Scope of lossless, a reversible, and a combined information hiding plans for figure content pictures scrambled by open key cryptography with homomorphic and probabilistic properties.
- This technique can be used in Information Transferring Technique and Digital Media.

ADVANTAGES OF PROPOSED SYSTEM:

- ➢ It improves the capacity ranging from 12285 to 34398 bits in a stego texture synthesis image of 1024*1024 pixels.
- ➢ The capacity we offer varies from 4.50 to 50.39 times more than our counterparts.
- ➢ It extracts the secret messages correctly, while their scheme exhibits a small error rate when extracting secret messages.
- ➢ This system performs compression as well as data encryption back side of image.
- ➢ This system easily hide the large amount of data background of image.

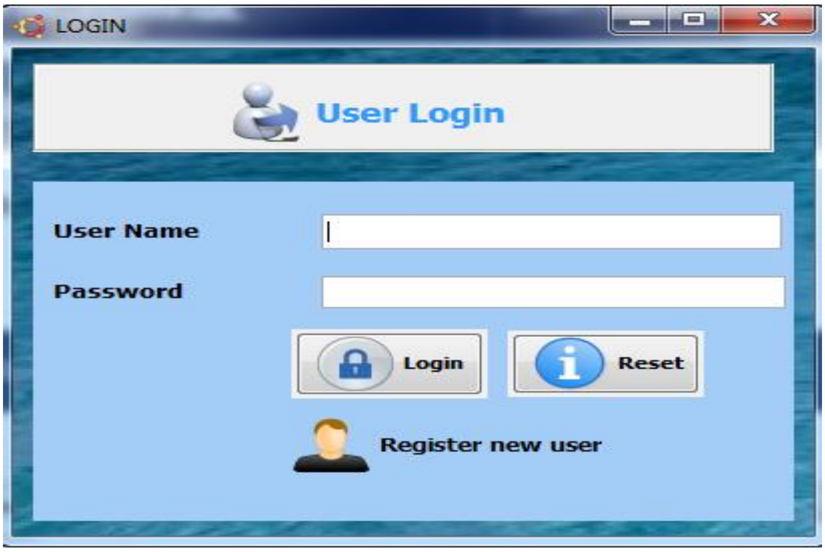
V. Goals and objectives

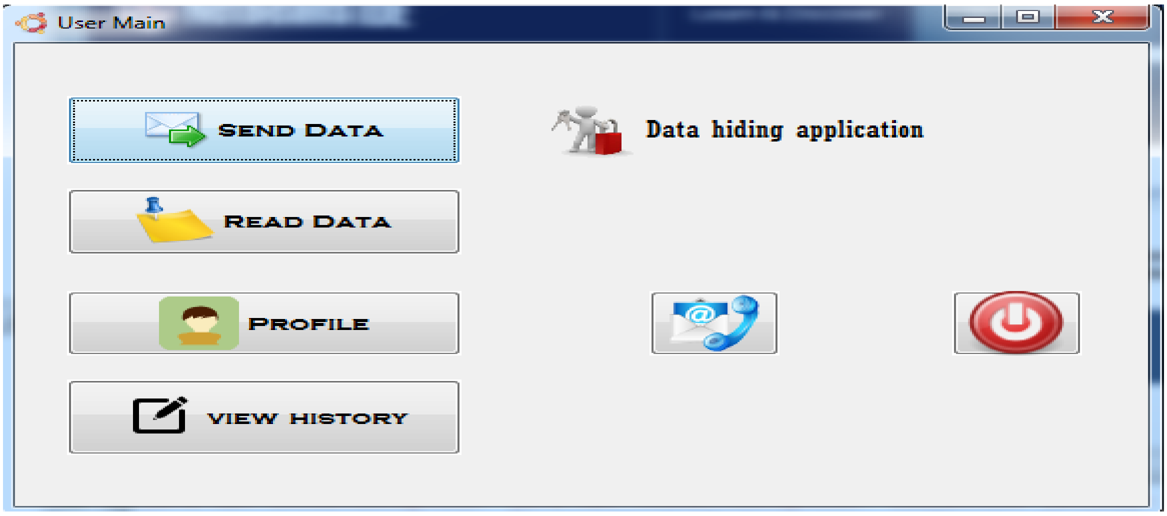
• Objective Secure communication over geographically distributed area and avoid cyber crime
• Goal Integrate Data Security and Authentication techniques for secured communication of two parties and maintain secrecy.

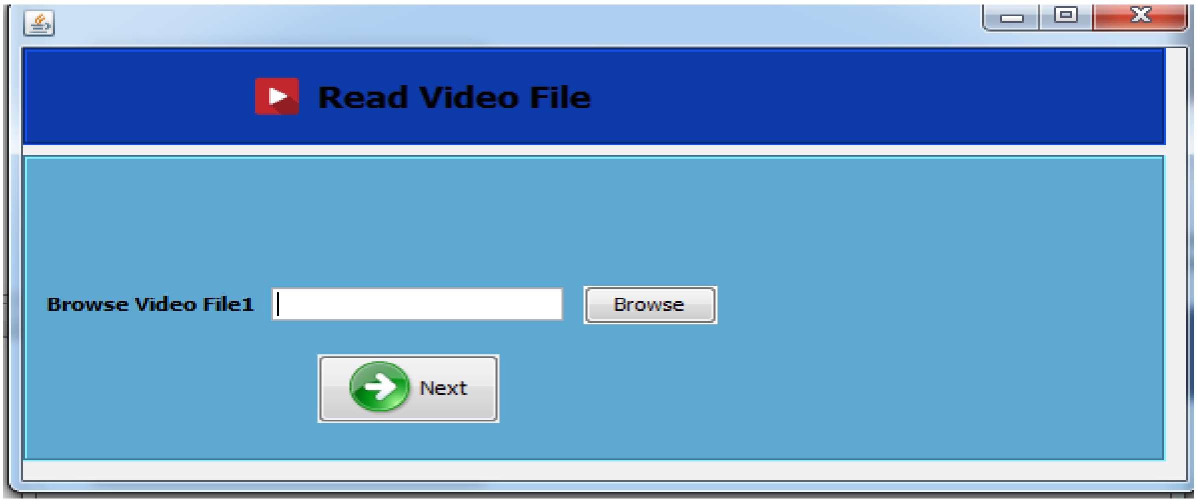
Statement of scope

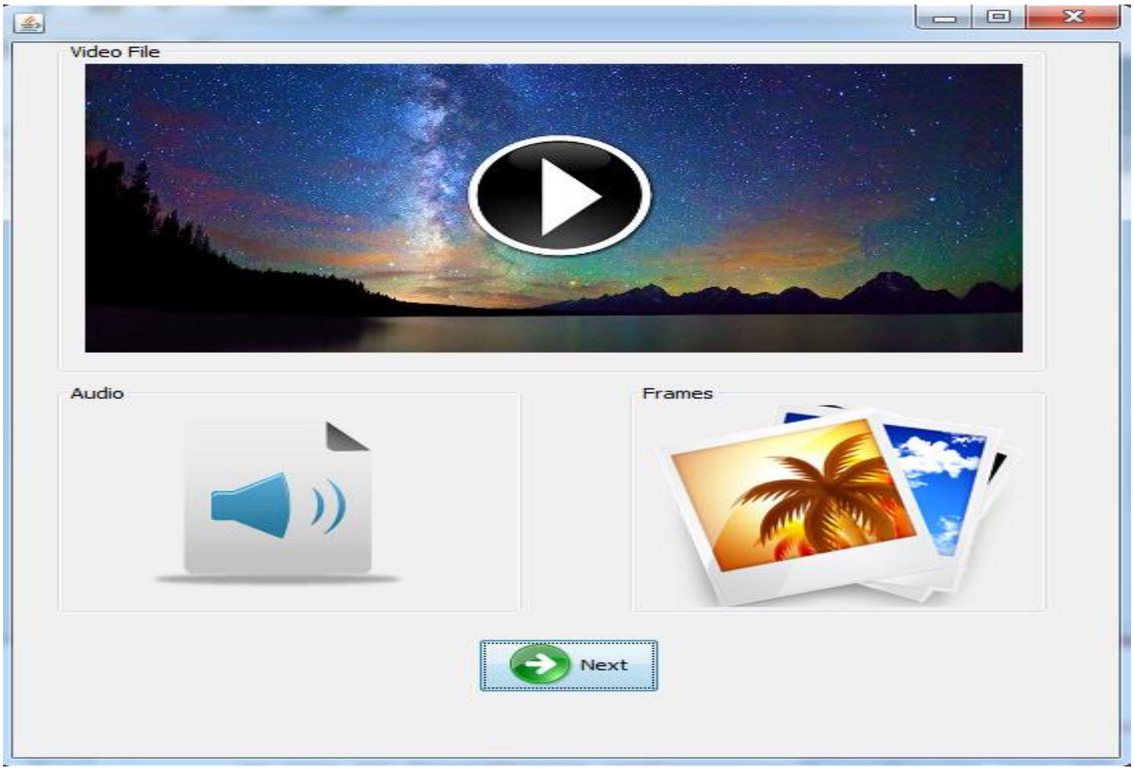
1. provides privacy
2. provide better hiding capacity and security.
3. hiding secret message for long time
4. Assuring data security
5. receiver side to cross check the security parameters and providing authentication at receiver side

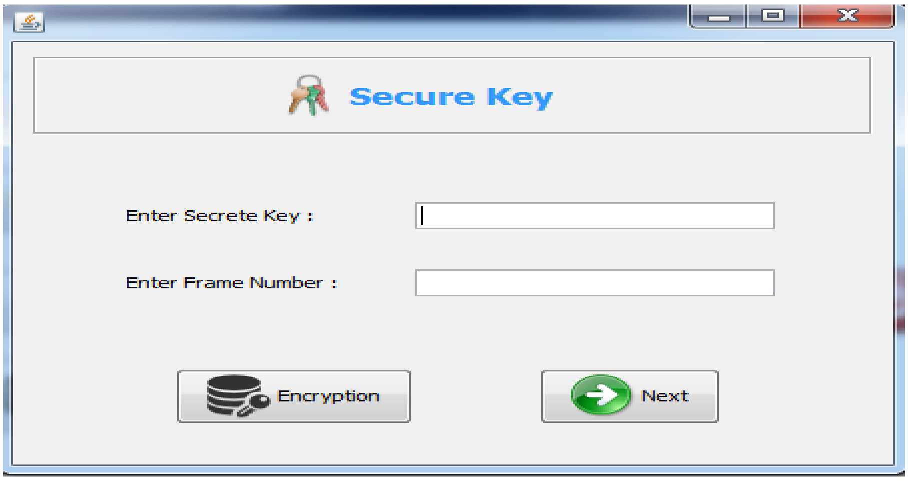
VI. RESULT




User Main
SEND DATA
READ DATA
PROFILE
VIEW HISTORY
Data hiding application


Read Video File
Browse Video File1
Browse
Next

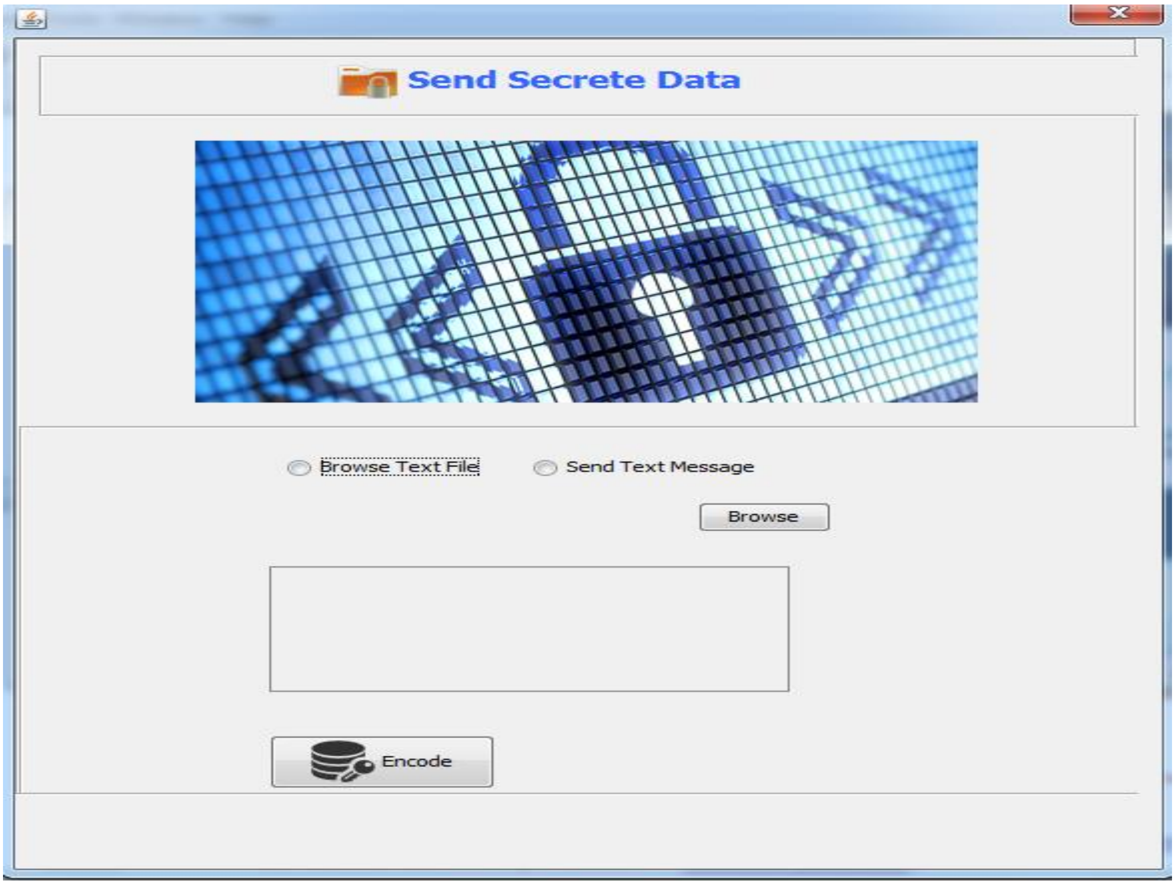

Video File
Audio
Frames
Next



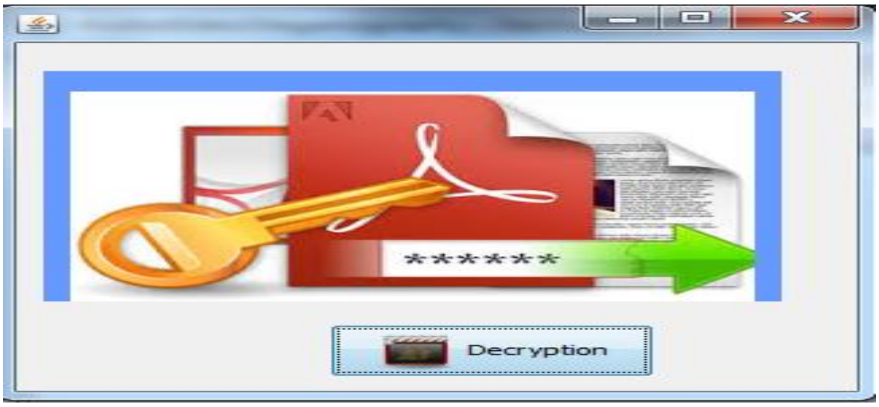
Secure Key

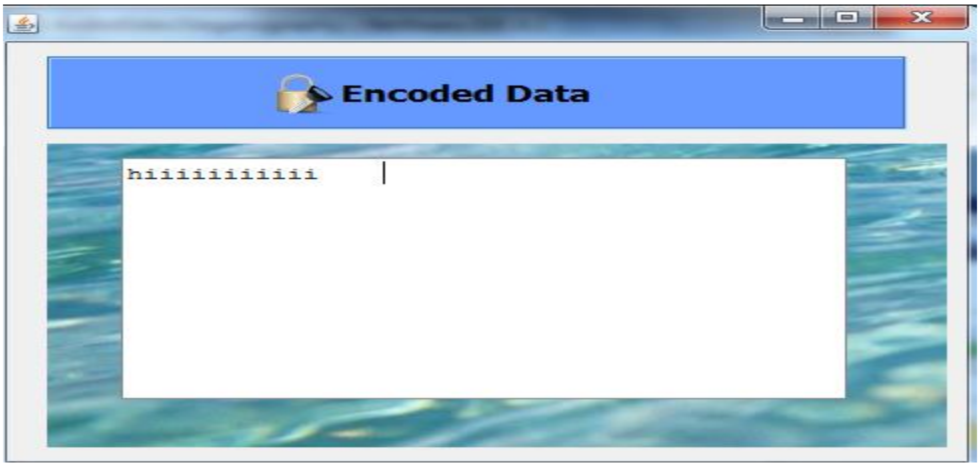
Enter Secrete Key :

Enter Frame Number :



Send Secrete Data





hiiiiiiiiiii

VI.CONCLUSION

Information security victimization information concealment audio video stegnography with the assistance of pc rhetorical techniques provides higher concealment capability we've got worked on concealment image ANd text behind video and audio file and extracted from an file victimization four least important bit insertion methodology for video steganography and part cryptography audio stegnography.We square measure concealment encrypted information victimization stegnography and cryptography behind hand-picked frame of video victimization 4LSB insertion methodology.The conclusion of our project is secure communication between sender and receiver..

REFERENCES

[1] Arup kumarBhaumik, Minkyachoi, Data Hiding in Video IEEE International journal of data base a application, vol 2no.2 june 2009. Pp.9-15

[2] Alkhraisathabes. Information Hiding in BMP Image Implementation, analysis Evaluation Information transmission in computer network, fall2006, Volume 52, issue, pp.1-10

[3] V.Sathya, k Balsubramaniyam, N, Murali, Data hiding in audio signal, video signal text and JPEG Image, IEEE ICAESM 2012, March 30-3-2012, pp741-746

[4] S. Gao, R. M. Zeng H. Jai,A A Detection algorithm of audio spared spectrum data hiding 2008 IEEE international conference, pp1-4.

[5] Wen Chao Yang, Che Yen Wen, Applying public key watermarking technique in forensic imaging to preserve the authenticity of the evidence ISI 2008 Workshop, LNCE 5075, Springer verlag Berlin Heidelberg, pp278-287.

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

[7] SghierGuizani, Nidal Nasser, An Audio/Video Crypto Adaptive Optical Steganography Technique IEEE 2012 2012, pp, 1057-1062.

[8] Fatiha Djebbar,Ayady"A view on latest audio steganography techDIT,Pimpri, Department of Computer Engineering 2017-18 46 niques"IEEE International Conference on I nnovations in Information Technology2011.

[9] George Abboud, Jeffery Marean, "Steganography and cryptography in computer Forensics." 201 0 I EEE, Fifth international workshop on systematic application to digital Forensic application. pp. 25-30.

[10] Hamid A. Jalab, A.A.Zaidan "Frame selectionapproach for data hiding within MPEG Video us ing bit pla ne complexity segmentation" IEEE journal of computing, vo I,Issue 1,dec 2009.pp 108-112.