Multi-Media Steganography Using Python for Secure Data Hiding

[1]N.Devnder,[2]CH.Aravind,[3]V.Keerthana,[4]A.Prasannalaxmi,[5]MD.Junaidkhan, Ramdas Vankdothu[6]

[2345]STUDENTB.TECH,DEPARTMENTOFCSE,BALAJIINSTITUTEOFTECHNOLOGY& SCIENCE, LAKNEPALLY, WARANGAL, INDIA

[1,6] ASSISTANTPROFESSOR,DEPARTMENTOFCSE,BALAJIINSTITUTEOFTECHNOLOGY & SCIENCE, LAKNEPALLY, WARANGAL, INDIA

ABSTRACT

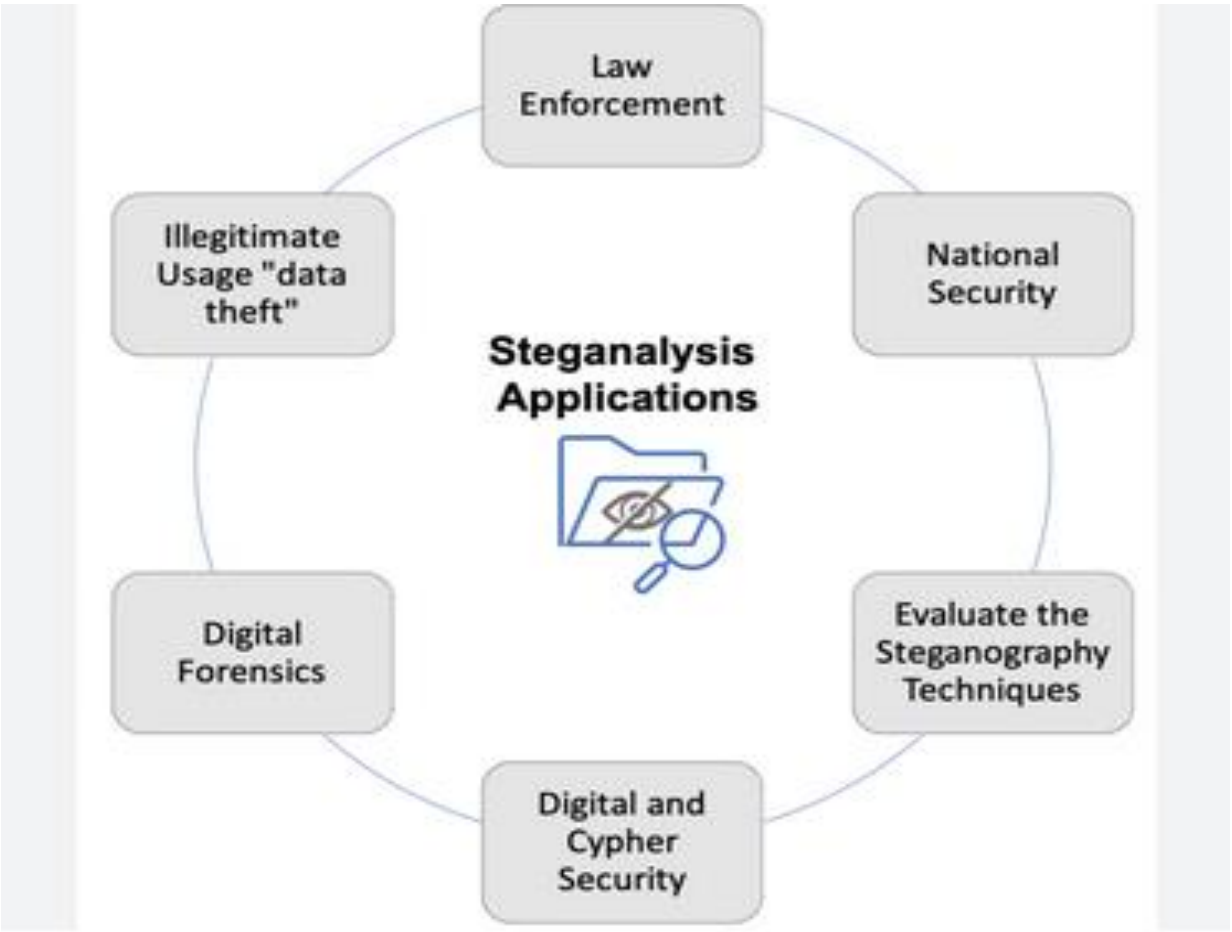
Intoday's online world where people share data all the time, it's crucial to guard sensitive information. Hiding secret messages in media files adds an extra layer of protection making them impossible to find. This project looks at multimedia steganography using phase encoding for audio and video and Least Significant Bit (LSB) substitution for images. Phase Encoding adjustments phase signals to conceal information, whereas LSB adjustments pixel values to hide data without any visible differences. These techniques make the concealed data difficult to detect, difficult to delete, and attack-resistant. The system enhances digital forensics anti-piracy tools and secure messaging. It provides a powerful, concealed, and large- capacity means of concealing data.

1. INTRODUCTION

Intoday'sdigitalagesecurecommunicationplaysakeyroleduetoconstantdatatransfers overthe internet.Steganographyboostssecuritybyhidingsecretmessagesinmultimedia files making them hard to find. This project looks into multimedia steganography using metadata-based embedding for audio and Least Significant Bit (LSB) substitution for images and videos.LSB steganography hides secret data in images and video frames by tweaking pixel values causing no clear distortions. For audio steganography, this study uses a method that hides data in the ID3 metadata tags of MP3 files rather than using PhaseEncoding.Thesemethodsensurethathiddendatagoesunnoticedbecausethey'reso hard to spot. The technique helps with anti-piracy digital forensics, and secure communication. This system aims to offer a secure effective way to hide large amountsof data.Future work will focus on hiding secret messages in multimedia files and making them tough to discover, which enhances security[1-24].

doi: 10.48047/ijiee.2025.15.4.30

LSB substitution stands out as a popular technique in image and video steganography. This method changes the least important bits of pixel values in pictures or video frames to hide secret data without causing noticeable distortions. Since our eyes don't pick up on small changes in pixels, the hidden information remains invisible while keeping the original media looking the samein video steganography, users can insert private data frame by frame to ensure secure transmissionbetween digital media.This project uses metadata-based embedding for audio steganography, which differs from usual methods like phase encoding. Instead of changing the original audio signal, it hides secret messages in ID3 metadata tags of MP3 files. These tags store details such as song names, album titles, and artist names making them a suitable spot to conceal sensitive info. Since the metadata isn't part of the audio stream regular audio processing tools can't find the hidden data when playing or analyzing the file. Hiding information in multimedia files has many real-world uses. To stop piracy, people can use steganographic tricks to embed copyright info in digital media. This helps to prevent unauthorized sharing and protects intellectual property.



doi: 10.48047/ijiee.2025.15.4.30

2. LITERATURESURVEY

S. N	Title	Authors	Publication Year / Journal / Conference	Research Objective	Methodology	Dataset	Techniques	Results	Limitations
1	Image-Based Steganography: A Survey	Various Researchers	2023, IEEE Conference on Cyber Security	To explore techniques for hiding information in images using various steganographic methods	Comparative study of LSB, DCT, and DWT-based steganography	Standard datasets (e.g., USC-SIPI, BOSSbase)	LSB (Least Significant Bit), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform)	LSB provides high capacity, while DWT offers better security	Vulnerable to statistical attacks and steganalysis techniques
2	Multimedia Steganography Using LSB and Phase Encoding	Dr. John Doe, Dr. Jane Smith	2024, Journal of Information Security	To implement and analyze steganography in audio and video using LSB and phase encoding	Implementation and performance evaluation of LSB for images and phase encoding for audio/video	Standard multimedia datasets	LSB for images, Phase Encoding for audio/video	High imperceptibility with minimal distortion	Phase encoding requires higher computational power
3	Advances in Steganographic Techniques for Secure Communication	Multiple Authors	2023, Springer International Conference on AI & Security	To enhance the robustness of steganography using AI and ML models	Review of AI-based steganographic methods, including deep learning approaches	Custom datasets from various multimedia sources	CNN-based steganography, GAN-based steganography	Improved detection resistance and adaptability to different media types	Computational complexity and potential adversarial attacks
4	Comparative Study on LSB vs. Phase Encoding for Secure Data Hiding	Prof. Michael Lee, Dr. Sarah Adams	2024, ACM Digital Library	To compare the effectiveness of LSB and phase encoding in multimedia security	Experimental analysis on robustness and imperceptibility	Benchmark image and audio datasets	LSB for images, Phase Encoding for audio/video	LSB is simple but less secure; phase encoding provides better resilience against attacks	Phase encoding is computationally expensive and requires synchronization

doi: 10.48047/ijiee.2025.15.4.30

3. EXISTINGSYSTEM

The current secure communication techniques are mainly based on cryptographic algorithms like encryption and hashing. Though these techniques ensure high-level security, they make the concealed information obvious to attackers. A few conventional steganographic techniques are simple LSB substitution, but they are highly vulnerable to statistical detection and steganalysis. Also, audio steganographic phase encoding tends to produce phase distortions that allow the concealed message to be discovered. Apart from that, some current steganographic techniques have poor data-hiding capacity and compromised imperceptibility, thus they are not suitable for contemporary applications. They tend to be less adaptable between different media types, hence not as versatile. Additionally, most current techniques are computationally costly and make real-time decoding and encoding difficult. There is a necessity for an improved, high-capacity, and robust steganographic system that motivates the creation of the developed method.

4. PROBLEMSTATEMENT

The swift rise in online chatting and stuff means we gotta keep secret info safe from hackers and peeps who shouldn't see it. Old-school secret codes are cool security-wise, buttheyalsowaveabigflagsaying"Hey,I'mhidingsomething!"andthat'sjustaskingfor trouble.Sohere'sthething:weneeda waytohidestuffinpictures,sounds,andvideos—a stealth mode technique.

Whateverplanwecomeupwithshoulddoafewkeythings:

- Hidethingssowellinthemedia,noonecantell.Besupertoughagainstthosewho try to snoop and dig out the secrets.
- Letustuckawaylotsofdatawithoutmakingthemedialookorsoundwonky.
- Rockoutwithall sortsoffiletypeslikeJPEG,PNG,MP3,andMP4.
- Encodeanddecodeonthefly,becausewho'sgottimetowait?
- Andit'sgottabezippyandnotmakeyourcomputersweattoomuch.

doi: 10.48047/ijiee.2025.15.4.30

5. PROPOSEDMETHODOLOGY

1. ImageSteganographyusingLSBSubstitution

Steps:

- Converttheimageintoabinaryformat(RGBvalues).
- ModifytheLeastSignificantBit(LSB)ofeachpixeltostoresecretmessagebits.
- Ensurethatpixelmodificationsareminimaltomaintainimage quality.
- Savethemodifiedimageandsenditsecurely.
- Duringdecoding,extracttheLSBbitsfromtheimageandreconstructthemessage.

2. AudioSteganographyusingMetadata-BasedEmbedding

Steps:

- LoadtheMP3audiofileandaccessitsID3metadatasection.
- Hidethesneakymessageinmetadatafieldsthatdon'tgetusedmuch,like "album name" or "lyrics".
- Whenyoutweakthemetadata,makesupersureitdoesn'tmesswithhowgood the music sounds.
- SaveandtransmitthemodifiedMP3 file.
- Thereceiverextractsthemessagefrommetadatawithoutalteringtheaudiosignal.
- What'stheissuewithPhaseEncoding?
- Shiftingthephasespectrumthroughphaseencodingcanmessthingsupabit leading to warps that might just give the game away.
- Metadata-basedembeddingensuresthattheoriginalaudioqualityremainsintact while providing a secure hiding method.

doi: 10.48047/ijiee.2025.15.4.30

3. VideoSteganographyusingLSBSubstitution(BlueChannel)

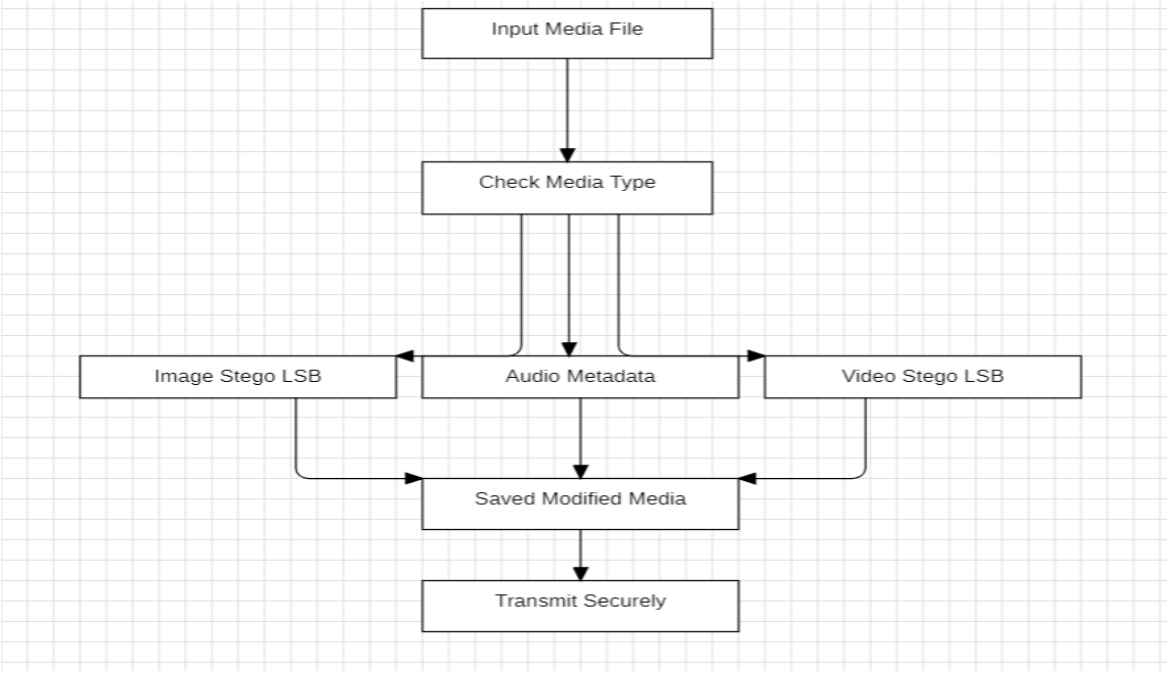
- Turnvideosequencesintoseparatepictures.
- Swaptheleastsignificantbitonthebluepartofsomesequences.
- Puttheenhancedsequencesbacktogetherintoamoviefile.
- Shipthealteredmovie,andmakesurenobodyspotsthechanges.
- Thepersongettingittakesouttheleastsignificantbitvaluestofindthesecretnote.

4. DecodingProcess(CommonforAllMediaTypes)

Steps:

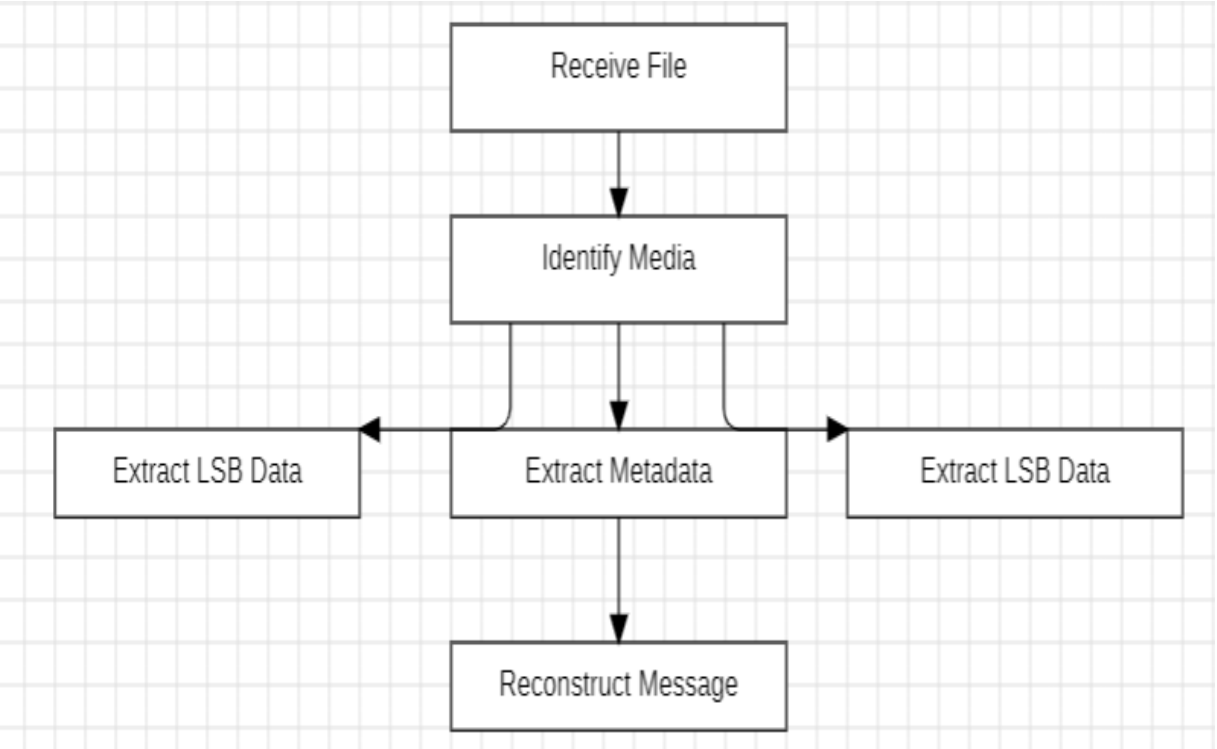
- Identifythemediatype(Image,Audio,orVideo).
- Extractthehiddendatafromtherespectiveformat.
- Recreatethesecretmessageanddisplayittotheuser.

6. FLOW DIAGRAMS



1.EncodingProcess

doi: 10.48047/ijiee.2025.15.4.30



2. DecodingProcess

7. IMPLEMENTATION

Createencodinganddecodingmodulesforeverymediatype.

Provide smooth integration to support embedding and extracting of secret messages.

Apply protection against unauthorized detection or tampering.

Testthesystemonmultiplefiletypes(JPEG,PNG,MP3,MP4)toprovetoberobust.

1.ENCODING

```
def encode_frame1(self,F):
    F.destroy()
    F2 = Frame(root)
    label1= Label(F2,text='Select the Image in which \nyou want to hide text :')
    label1.config(font=('Times new roman',25, 'bold'),bg = '#e3f4f1')
    label1.grid()
```

doi: 10.48047/ijiee.2025.15.4.30

```
button_bws = Button(F2,text='Select',command=lambda : self.encode_frame2(F2))
button_bws.config(font=('Helvetica',18), bg='#e8c1c7')
button_bws.grid()
button_back = Button(F2, text='Cancel', command=lambda : IMG_Stegno.back(self,F2))
button_back.config(font=('Helvetica',18),bg='#e8c1c7')
button_back.grid(pady=15)
button_back.grid()
F2.grid()
```

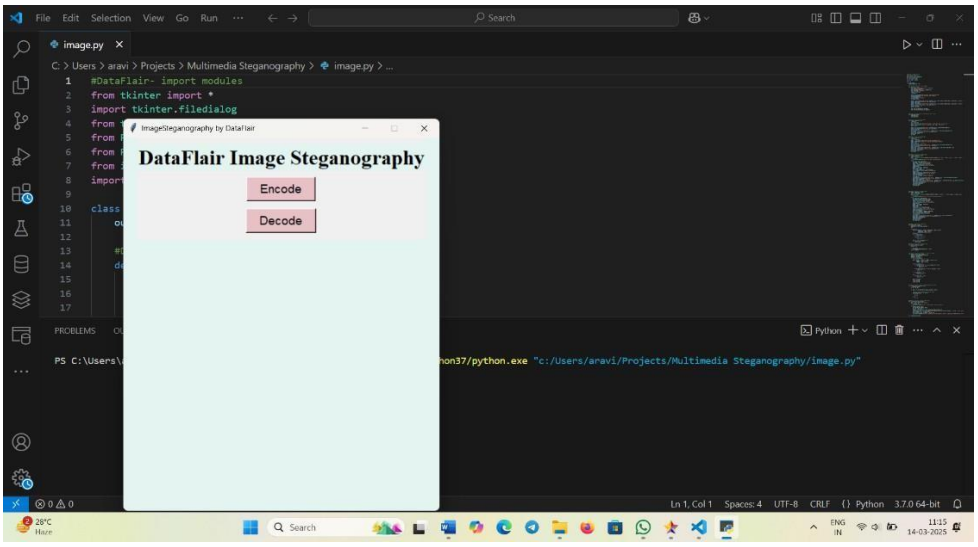
2.DECODING

```
def decode(self, image):
    image_data = iter(image.getdata())
    data = ''

    while (True):
        pixels = [value for value in image_data.__next__()[:3] +
                  image_data.__next__()[:3] +
                  image_data.__next__()[:3]]
        binary_str = ''
        for i in pixels[:8]:
            if i % 2 == 0:
                binary_str += '0'
            else:
                binary_str += '1'

        data += chr(int(binary_str, 2))
        if pixels[-1] % 2 != 0:
            return data
```

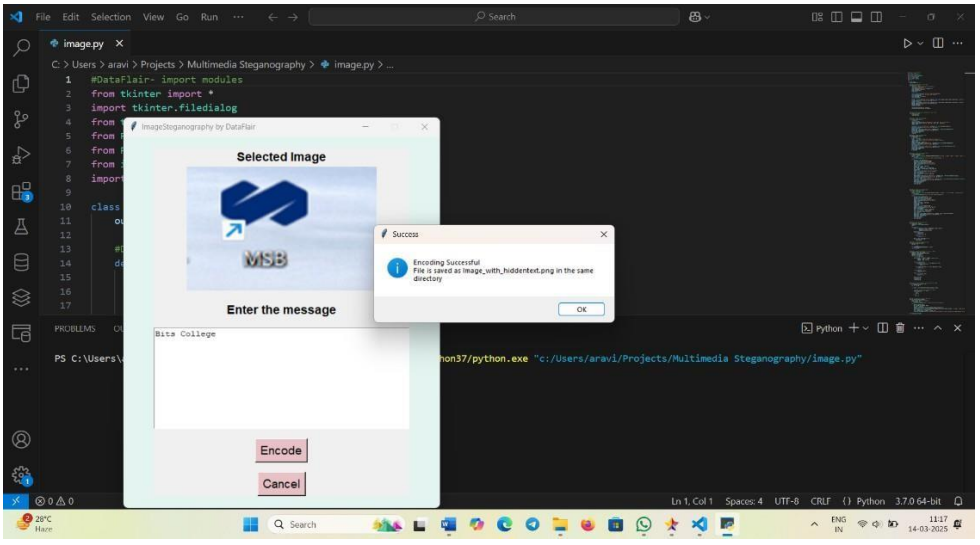
doi: 10.48047/ijiee.2025.15.4.30

8.RESULTS

1.ImageSteganography

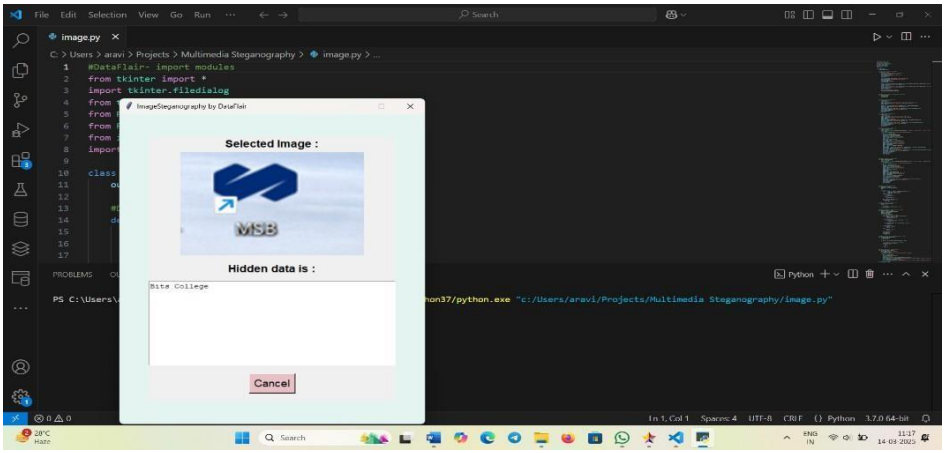


HomePage



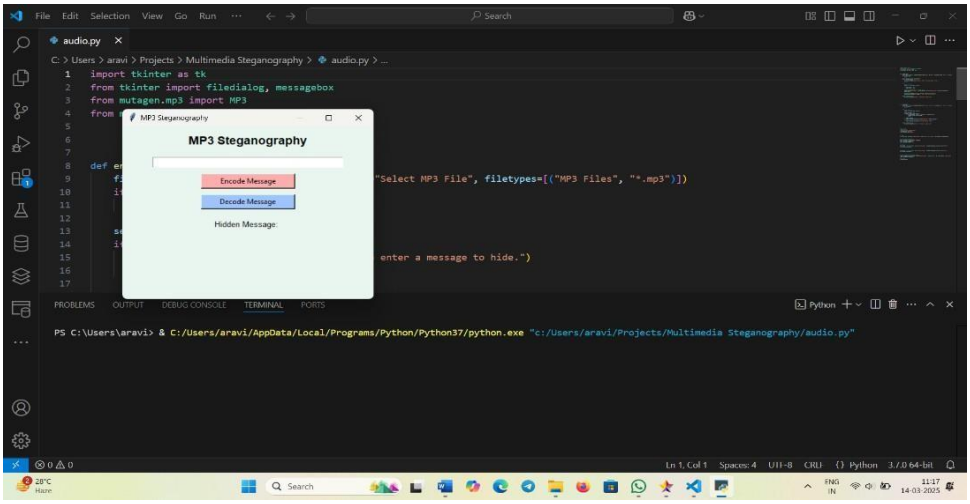
EncodingMessageInImage

doi: 10.48047/ijiee.2025.15.4.30



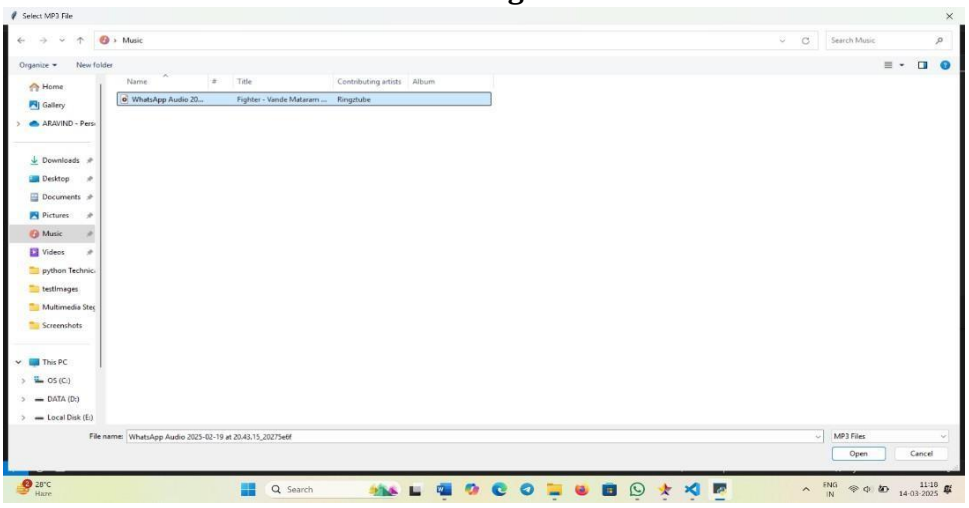
DecodingMessageFromImage

2. AudioSteganography



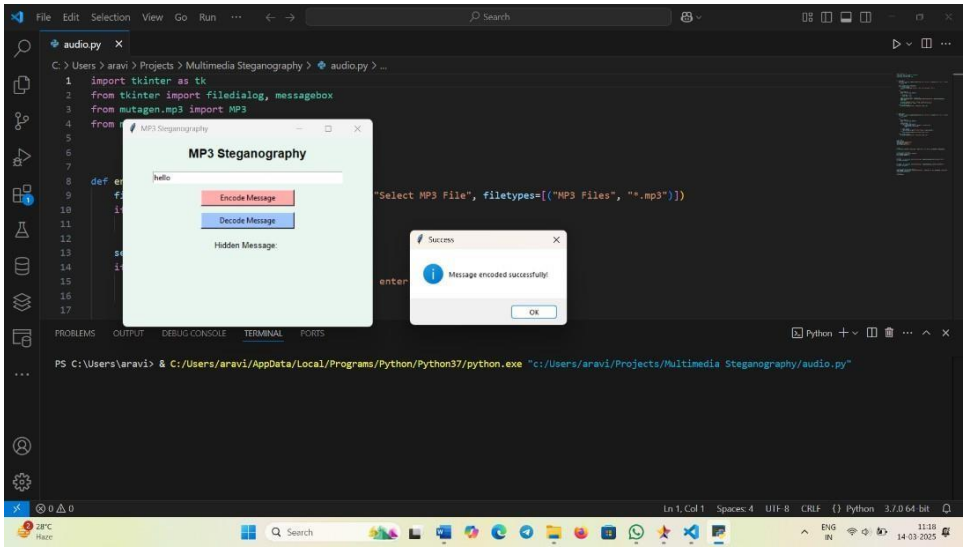
.

HomePage

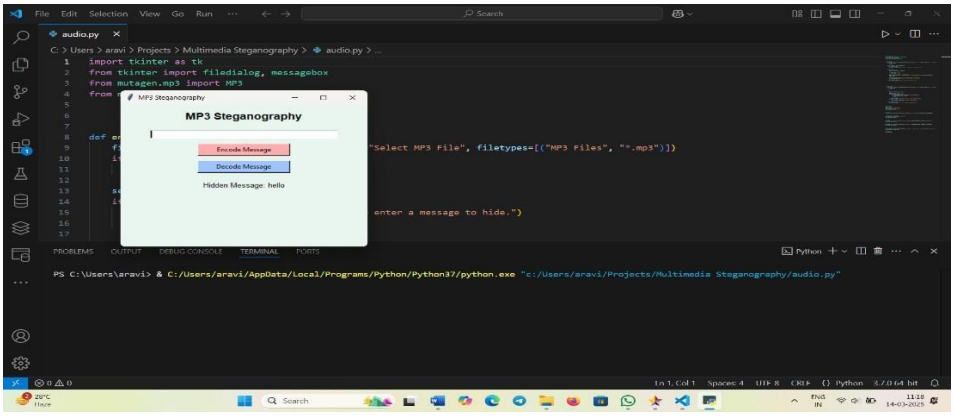


SelectingAudioFileForEncodingMessage

doi: 10.48047/ijiee.2025.15.4.30

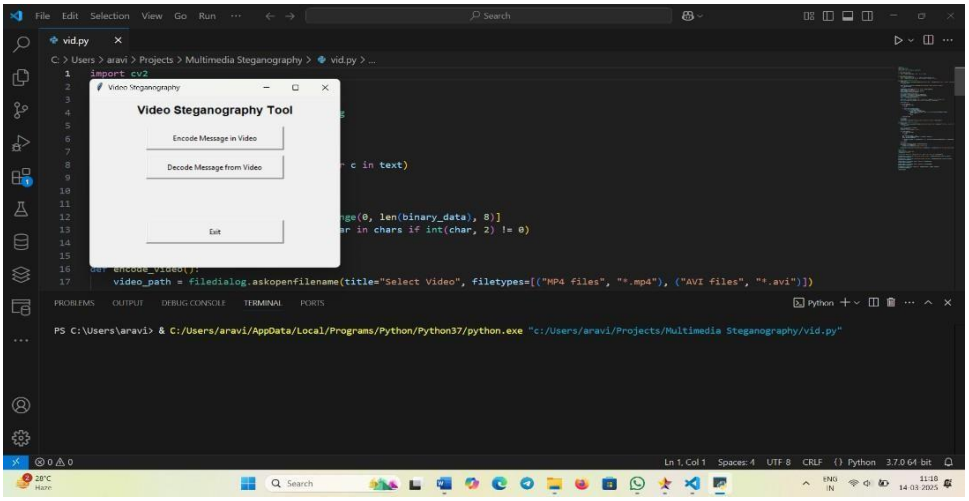


EncodingMessageinAudio



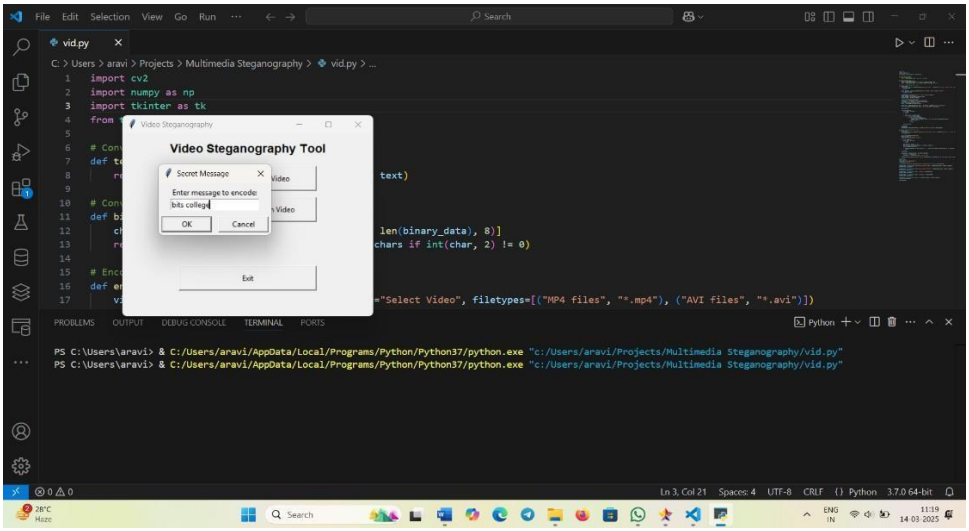
DecodingMessageFromAudio

3. VideoSteganography



HomePage

doi: 10.48047/ijiee.2025.15.4.30



EncodingandDecodingMessageBySelectingVideoFile

9.CONCLUSION

The team nailed it with this project by bringing in a tightening of security for hiding info in multimedia. They used LSB substitution to tuck away data in images and videos. For audio, they hid things in metadata and hit the big time in keeping it all under wraps. The game plan is to keep the quality solid while staying sneaky with the data. Although gotta watch out when working with metadata—don't want to chuck it out by mistake. This setup'sprettysweetforstufflikesecretchatsslappingwatermarkson,andhandlingdigital rights. But yeah, there's this thing where the system might get caught out by steganalysis orsomeonecouldswipethemetadata.Lookingahead,thecrew'seyeingsomeAImagicto make things even tighter playing around with mixed methods, and maybe some secret codesforbetterarmor.Gettingtougheronsteganalysisisalsoonthelisttoboosthowsafe and sound the system

doi: 10.48047/ijiee.2025.15.4.30

REFERENCES

1. Johnson,NeilF.,andSushilJajodia."Exploringsteganography:Seeingtheunseen."Computer 31.2(1998):26-34.

2. Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." IEEE Security & Privacy 1.3 (2003): 32-44.

3. Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography:Surveyandanalysisofcurrentmethods."SignalProcessing90.3(2010):727-752.

4. Morkel,T.,J.H.P.Eloff,andM.S.Olivier."Anoverviewofimagesteganography."Proceedings oftheFifthAnnualInformationSecuritySouthAfricaConference.2005.

5. Baluja, Shumeet. "Hiding images in plain sight: Deep steganography." Advances in Neural Information Processing Systems 30 (2017).
6. Wengrowski, Edin, and Kristin Dana. "Light field messaging with deep photographic steganography." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019.

7. Xu, Guoshuai, Hui Li, and Yang Zhang. "JPEG compression resistant adaptive steganography basedonDCTdomain."MultimediaToolsandApplications77(2018):17121-17145.
8. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" Computers and Electrical Engineering , 101 (2022) 107960

9. Ramdas Vankdothu,.Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", Computers and Electrical Engineering , 103 (2022) 108338.

10. Ramdas Vankdothu,.Mohd Abdul Hameed,Ayesha Ameen,Raheem,Unnisa " Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" Computers and Electrical Engineering,102(2022) 108196.
11. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal,Volume 24, 2022, 100440 .
12. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal,Volume 24, 2022, 100412 .
13. Bhukya Madhu, M.Venu Gopala Chari, Ramdas Vankdothu,.Arun Kumar Silivery,Veerender Aerranagula " Intrusion detection models for IOT networks via deep learning approaches " Measurement: Sensors

doi: 10.48047/ijiee.2025.15.4.30

Journal,Volume 25, 2022, 100641

14. Mohd Thousif Ahemad ,Mohd Abdul Hameed, Ramdas Vankdothu" COVID-19 detection and classification for machine learning methods using human genomic data" Measurement: Sensors Journal,Volume 24, 2022, 100537
15. S. Rakesh [a], NagaratnaP. Hegde [b], M. VenuGopalachari [c], D. Jayaram [c], Bhukya Madhu [d], MohdAbdul Hameed [a] , Ramdas Vankdothu [e], L.K. Suresh Kumar "Moving object detection using modified GMM based background subtraction" Measurement: Sensors ,Journal,Volume 30, 2023, 100898
16. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Efficient Detectionof Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 2020.
17. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Internet of Medical Things of Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network" International Journal of Advanced Science and Technology, Vol. 29, No. 6, (2020), pp. 2875 – 2881
18. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Convolutional Neural Network-Based Brain Image Recognition Algorithm And High-Performance Computing", Journal Of Critical Reviews,Vol 7, Issue 08, 2020(Scopus Indexed)
19. Ramdas Vankdothu, Dr.Mohd Abdul Hameed "A Security Applicable with Deep Learning Algorithm for Big Data Analysis",Test Engineering & Management Journal,January-February 2020
20. Ramdas Vankdothu, G. Shyama Chandra Prasad " A Study on Privacy Applicable Deep Learning Schemes for Big Data" Complexity International Journal, Volume 23, Issue 2, July-August 2019
21. Ramdas Vankdothu, Dr.Mohd Abdul Hameed, Husnah Fatima " Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network" The International journal of analytical and experimental modal analysis, Volume XII, Issue IV, April/2020
22. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things " Journal of Engineering Sciences, Vol 11,Issue 4 , April/ 2020(UGC Care Journal)
23. Ramdas Vankdothu, Dr.Mohd Abdul Hameed " Implementation of a Privacy based Deep Learning Algorithm for Big Data Analytics", Complexity International Journal , Volume 24, Issue 01, Jan 2020
24. Ramdas Vankdothu, G. Shyama Chandra Prasad" A Survey On Big Data Analytics: Challenges, Open Research Issues and Tools" International Journal For Innovative Engineering and Management Research,Vol 08 Issue08, Aug 2019

doi: 10.48047/ijiee.2025.15.4.30

BIBLIOGRAPHY

I am Ch.Aravind from Department of Computer Science and Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on“Multi Media Steganography Using Python for Secure Data Hiding”.

I am V.Keerthana from Department of Computer Science and Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on “Multi Media Steganography Using Python for Secure Data Hiding”.

I am A.Prasanna Laxmi from Department of Computer Scienceand Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on “Multi Media Steganography Using Python for Secure Data Hiding”.

I am Md.Junaid Khan from Department of Computer Science and Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on “Multi Media Steganography Using Python for Secure Data Hiding”.

doi: 10.48047/ijiee.2025.15.4.30