International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 05 | May 2024 www.irjet.net p-ISSN: 2395-0072

DIGITAL DATA CONCEALMENT USING ADVANCED STEGANOGRAPHY

Mr. Hemanth C [1], Mr. Rudrayya S[2], Mr. Srinidhi S[3], Ms. Varshini K Y [4], Ms. Sahana D P[5]

[1] *Assistant Professor, Dept. of Computer Science and Engineering, Maharaja Institute of Technology, Thandavapura, Karnataka, India*
[2-5]*Students, Dept of Computer Science and Engineering, Maharaja Institute of Technology, country Thandavapura, Karnataka, India*

Abstract - *Steganography, an ancient art form, has evolved into a modern technique for covert communication. It involves concealing a message within an innocuous carrier, like a picture, sound, or video to evade detection. Unlike cryptography, which encrypts a message, steganography conceals the message's actual existence Utilizing imperceptible alterations in the carrier, steganography embeds bits of information, imperceivable to the human eye or ear, yet retrievable by intended recipients using specialized tools. This clandestine method finds applications in various fields, including cybersecurity, digital watermarking, and espionage. With the exponential growth of digital media and communication channels, steganography poses both a threat and a defense mechanism in the realm of information security. Its continuous development challenges researchers and practitioners to create robust detection techniques whilealso advancing the sophistication of concealment methods, shaping the ongoing cat-and-mouse game of covert communicatio*n.

Key Words: **Steganography, covert communication, concealment, carrier, cryptography, digital media, imperceptible alterations, cybersecurity.**

1.INTRODUCTION

Advanced steganography represents the cutting edge of covert communication techniques, leveraging sophisticated methods to embed and extract information from digital carriers with unprecedented stealth and resilience. In contrast to traditionalsteganography, which primarily focuses on concealing data within static images, audio, video text, advanced steganography explores innovative approaches acrossa diverse range of multimedia formats, including audio, video. Moreover, advanced steganography techniques often incorporate encryption mechanisms to enhance security of the hidden data, ensuring that even if the carrier is intercepted, the concealed information remains protected from unauthorized access.

1.1 PROBLEM DEFINITION

In the realm of cybersecurity, steganography poses a significant challenge as a covert communication technique, presenting both a threat to informationsafety additionally a challenge for detection and mitigation efforts. Despite advancements in detectionmethods, the continuous evolution of steganographic techniques complicates the task of identifying and intercepting hidden messages within digital carriers. Additionally, the proliferation of digital media platforms and communication channels exacerbates the potential impact of steganography on sensitive data and critical infrastructure.

1.2 OBJECTIVE

The objectives of steganography encompass several key aims. Firstly, it serves as a means of covert communication innocuous carriers like images or audio files. This includes applications such as digital watermarking to safeguard intellectual property or embedding digital signatures for authentication. Additionally, steganography aims to enhance security by adding an extra layer of complexity to data transmission and storage, making it more challenging for adversaries to identify and intercept hidden data. Moreover, steganography plays a role in anti-forensics by concealing traces of illicit activities within digital content, and in counter-forensics by aiding investigators in uncovering hidden information withindigital evidence.

1.3 SCOPE

The extent of steganography is extensive, encompassing various domains like cybersecurity, digital forensics, and privacy protection. Its applications range from covert communication and data hiding to anti-forensics and copyright protection.With the proliferation of digital media and communication channels, steganography continues to evolve, presenting new challenges and opportunities.

2. LITERATURE SURVEY

[A] Sabah Abdulazeez Jebur, Abbas Khalifa Nawar,Lubna Emad Kadhim, Mothefer Majeed JaheferImanAl-Kadhum College, Baghdad, The highest way to protect data from intruder and unauthorized persons has developed into a major issue. This matter led to the development of many techniques for data security, such as Steganography, Cryptography, and Water marking to disguise data.

[B] : Jayakanth Kunhoth1 Nandhini Subramanian1 Somaya Al-Maadeed1 Ahmed Bouridane2 Video steganography approach enables hiding chunks of secret information inside video sequences. The features of video sequences including high capacity aswell.structure make them the more desirable

option when selecting a cover material compared to other options like text, image, or audio.C. Sobin, SRM University AP, Amaravati, India,Engineering and Computer Science Department, V. M. Manikandan, SRM University AP, Amaravati, India,

[C] Department of Mechanical Design and Computer Science. The steganography is a data hiding process which helps to transmit secure messages by embedding it into a cover medium. The cover medium can be any digital information like images, audio, video, text file, etc. The audio steganography is a very popular scheme in which an audio signal will be used as a cover medium and the secret message can be any digital data It may note that any digital data can be shown as a sequence of bits irrespective of its type. Ingeneral, an audio steganography scheme involves two actors: a sender who will embed secret bits in audio and send to the receiver, and a receiver who will extract the secret message from the received audio signal and ignores the cover audio signal used for data hiding process. as image, text, or audio

[D] M. Anusha Department of Computer Science, Amrita Vishwa Vidyapeetham, Mysore, India, Amrita University of Arts & Sciences Amrita University of & Amrita Vishwa Vidyapeetham, Mysore, India, Sciences / K. N. Bhanu Computer Science Department D. Divyashree Amrita Vishwa Vidyapeetham, Mysore, India; Amrita School of Arts & Sciences, Department of Computer Science. Data security has gained an utmost importance due to the unprecedented increase in the produced data over the internet, which is a basic necessity of any application in information technology. Steganography is a specialty of science to manage and conceal a piece of important information inside image, audio, video or text documents

3. EXISTING SYSYTEM

Existing systems often incorporate encryption mechanisms to improve the security of hidden data, ensuring that even if the carrier is intercepted, the concealed information remains protected from unauthorized access. However, despite these advancements, the existing systems may still face challenges such as detection by advanced steganalysis techniques or vulnerabilities in implementation leading to potential exploitation. Overall, the existing system of steganography provides a foundation for secure communication and data protection but requires ongoing research and development to address emerging threats and enhance resilience against detection and attacks.

4. PROPOSED SYSTEM

Our proposed steganography system integrates advanced encryption techniques with image hiding algorithms to conceal secret messages within digital images. Leveraging LSB (Least Significant Bit) insertion method for embedding data ensures minimal visual distortion. Additionally, employing AES (Advanced Encryption Standard) encryption fortifies message security, enhancing resistance against unauthorized access. The system offers a user- friendly interface for seamless encoding and decoding operations, facilitating efficient communication in sensitive contexts. Through meticulous attention to both security and usability, our project aims to provide a robust and reliable steganographic solutionfor clandestine data transmission.

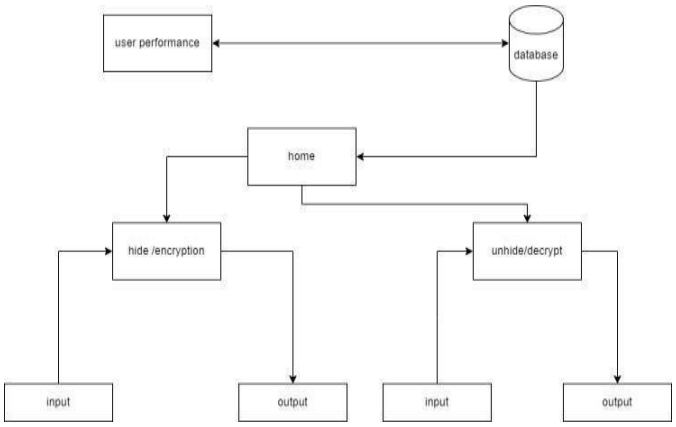

Fig -1: Flow Diagram

5. SYSTEM ARECHITECTURE

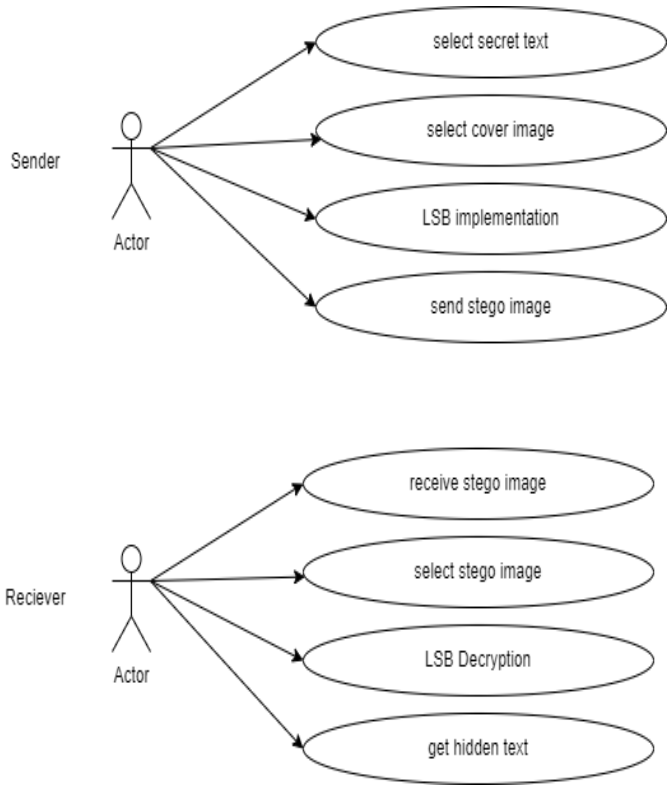

Fig -2: Use Case Diagram

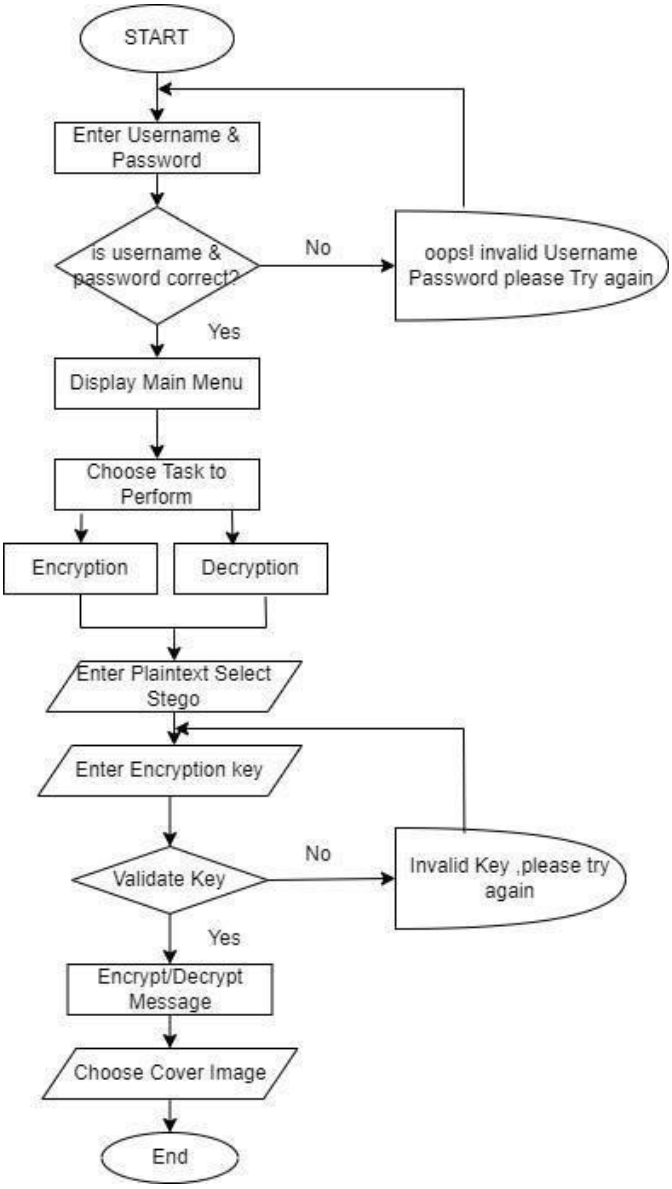

Fig -3: Schematic Of The System Architecture

5.1 TEXT STEGANOGRAPHY

For every character of the secret message We get its ascii value and it is incremented or decremented based on if ascii value between 32 and 64 , Yes, it is incremented by 48(ascii value for 0) else it is decremented by 48 Then xor the obtained value with 170(binary equivalent-10101010) Convert the obtained number from first two step to its binary equivalent then add "0011" if it earlier belonged to ascii value between 32 and 64 else add "0110" makingit 12 bit for each character. With the final binary equivalent we also 111111111111 as delimiter to findthe end of message Now from 12 bit representing eachcharacter every 2 bit is replaced with equivalent ZWCsaccording to the table. Each character is hidden after aword in the cover text. After receiving a stego file, theextraction algorithm discovers the contractual 2-bit of each ZWCs, every 12 bit from conclusion of the word, stego file. point. Now we divide the 12 bit into two parts first 4 bit and another 8bit on which we do the xor operation with 170(binary value 10101010). Nowaccording to the first 4bit if its is "0110" we incrementit by 48 else we decrement by 48. At last we convert the convert an ASCII value to the corresponding character to get the final hidden message from the stego file.

5.4 VEDIO STEGANOGRAPHY

In video steganography we have used combination of cryptography abd Steganography. We encode the message through two parts We convert plaintext to cipher text for doing so we have used Cryptography Algorithm RC4. RC 4 is a variable-length key algorithmand stream cipher. A byte at a time is encrypted usingthis approach. It is divided into two main sections: encryption and decryption. KSA (Key-Scheduling Algorithm)- A list S of length 256 is made and the entries of set to the values in ascending sequence, ranging from 0 to 255. We request the user's key. andconvert it to its equivalent ascii code. S [] is a permutation of 0,1,2. 255, now a variable j is assigned as j=(j+S[i]+key[i%key_length) mod 256 and swap S(i) with S(j) and accordingly we get new permutationfor the whole keystream according to the key.

5.3 AUDIO STEGANOGRAPHY

In audio we will be using Cover Audio as a Cover file to encode the given text. Wave module is used to read the audio file. Firstly we convert our secret message to its binary equivalent and added delimiter '*****' to conclusion of the message. For encoding we have modified the LSB Algorithm, for that we take each frame byte of the converting to 8 bit format then check for the 4th LSB and see if it matches with the secret message bit. If yes change the 2nd LSB to 0 using logical AND operator between each frame byte and 253(11111101). Else we change the 2nd LSB to 1 using logical AND operation with 253 and then logical OR to change it to 1 and now add secret message bit in LSB for achieving that use logical AND operation between each frame byte of carrier audio and a binary number of 254 (11111110).

6. RESULT

Result Is Shown bellow:

```
                TEXT STEGANOGRAPHY OPERATIONS
1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice:1
Maximum number of words that can be inserted :-  879

Enter data to be encoded:- This is our minor project on the topic "STEGANOGRAPHY". SEM 5
tubh sinha 3.Vaibhav Kansal

Inputed message can be hidden in the cover file

The string after binary conversion appyling all the transformation :- 0110100011100110
0100110100100110110111010010011111110100110100101011011101111011011010000011111110
1001010101101111010000011111110100110111010100110111010000110100101010110100100000
0011010010101011010010100001111111010011011101110011011001001001101001111001111110
0100110110100110010011111110100011111100001101000100101100011100110101111110110101
1101011110101101000100001101011101101100010100110101100100110100000110011111110000
1111011010110111001111111010001110011100111111101001101011110001101110100001101001
1110010110011111110100110100100001101001101101101110111001101001100101101001000111
1001101110100001101001001101101110001101101001101101100101000110111010010110100100
0011010110111010000011010010111010100110111001111111010001111100100000011111101000
0110111011100110111011110110100100001101001001000111111101001101110100101101001100
1101000111100100100111111010001101000110001101001101101100100110110011000011010010
1010110001011010011011011010010100011011101001011010011011010010110111111111111
Length of binary after conversion:-  1536

Enter the name of the Stego Key file after Encoding(with extension):- stego.txt

Stego file has successfully generated
```

Fig -4: Text Steganography

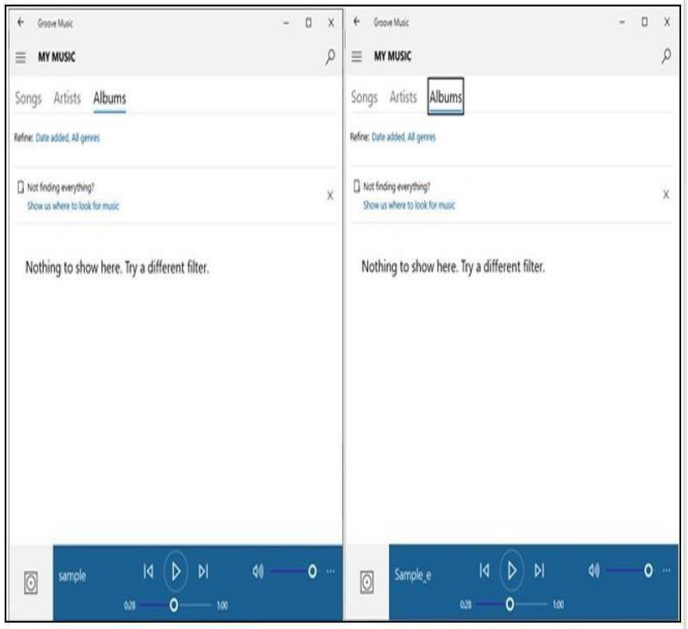

Fig -5: Audio Steganography

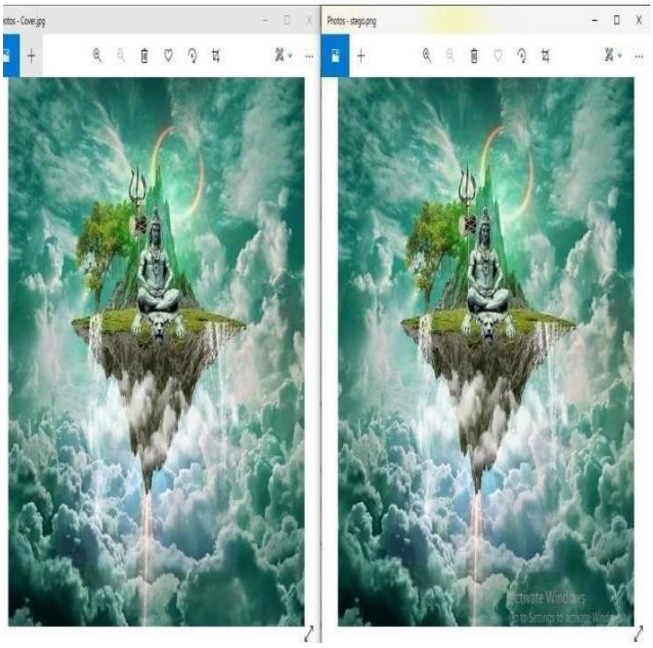

Fig -5: Image Steganography

Fig -5: Audio Steganography

8. CONCLUSIONS

Conclusion, this steganography project confirms the efficacy of concealing information within digital media, highlighting its relevance in secure communication and data protection. Through rigorous analysis, it demonstrates the robustness of modern techniques against common attacks and explores their diverse applications in digital forensics and copyright protection. Looking ahead, future research should prioritize

enhancing security and exploring novel applications in emerging technologies. This project underscores steganography's pivotal role in safeguarding digital information and privacy in an interconnected world, contributing to ongoing efforts to mitigate risks associated with unauthorized access and tampering.

ACKNOWLEDGEMENT

We wish to express our deepest appreciation to our esteemed Project Guide, Prof. Hemanth, whose invaluable guidance and suggestions have propelled our project beyond our expectations. We extend our heartfelt gratitude to our Project Coordinator, Dr. HK Chethan, for his unwavering support and dedication in helping us complete this project within a tight timeframe. We would also like to acknowledge our Head of Department, Dr. Ranjit KN, for fostering an environment that encourages innovation and practical application of our academic Dr. Y curriculum. Finally, we extend our sincerest thanks to our Principal, Dr. Y T Krishne Gowda, for providing us with a golden opportunity to carry out project on the topic of 'Digital Data Concealment Using Advanced Steganography'.

REFERENCES

[1] Sabah Abdulazeez Jebur, Abbas Khalifa Nawar, Lubna Emad Kadhim, Mothefer Majeed JaheferIman AlKadhum Baghdad.

[2] Jayakanth Kunhoth1 Nandhini Subramanian1 Somaya Al-Maadeed1.

[3] C.Sobin Department of Computer Science and Engineering, SRM University AP, Amaravati, IndiaV. M. ManikandanDepartment of Computer Science and Engineering.

[4] M. AnushaDepartment, Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysore,K. N. Bhanu,Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysore.

[5] M. Anusha , K. N. Bhanu Department of Computer Science, Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysore, India