Hiding Secure Data in Audio, Text & Image BY Steganalysis

1.Tushar Khandagale, 2. Gaurav Patil, 3. Atharva Harmale, 4. Deepak Dhumal

Guide: Prof. Dr. Ninad More

D. Y. Patil College of Engineering, Pune

Abstract–Steganography is the method of hiding any secret information like password, text, and image, audio behind original cover file. In this paper we proposed the audio-image crypto steganography which is the combination of image steganography and audio steganography using computer forensics technique as a tool for authentication. Our aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable algorithm such as 4LSB is used for image steganography and phase coding algorithm for audio steganography.

❖ **Keywords:**
Data Hiding, Steganography, Computer forensics, Histogram, PSNR

♦ INTRODUCTION

Steganography is the art of covered or hidden text message. The purpose of steganography is covert communication to hide the existence of a secret message from a third party. This paper is intended as a high-level technical introduction to steganography for those unfamiliar with the field. It is directed at forensic computer examiners who need a practical understanding of steganography without study into the mathematical, although references are provided to many of the ongoing research for the person who needs or wants additional detail covered by audio-text, image file. Although in this paper gives a historical context for steganography, the significance is on digital applications use anti Forensics technique, focusing on hiding information in online audio and video files. Examples for tools of software that employ steganography to hide data inside of audio-text & image file as well as software to detect such hidden files will also be presented. Suitable algorithm such as LSB is used for image steganography suitable parameter of security and authentication is like PSNR, histogram is obtained at transmitter\sender and receiver side which are exactly identical, hence data security can be increased. This paper focus on the idea of computer anti forensics technique and its use of video steganography in both investigative and security manner.

♦ MOTIVATION

1]Government, military, businesses, and private citizens all over the world now use the steganography for security and privacy purpose.
2]The music and movie industries continually device new material control methods such as early distribution of movie screening via steganography.
3]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 become prime
necessity for every nation to adopt some counter measure to foul use of internets.
4] Recently cybercrime 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.

♦ PROBLEM STATEMENT

• Hide secret data inside the cover medium without changing the overall quality of cover medium
• A special problem for steganography is the conversion of digital files to different formats or with different compression levels. Both can affect the embedded information, and the technology needs to be robust against this type of attack and signal modification.
• The challenge of steganalysis is that: The suspect information stream, such as a signal or a file, may or may not have hidden data encoded into them. The hidden data, if any, may have been encrypted before inserted into the signal or file.
• Even if there are noticeable distortions and noise, predictable patterns cannot always be detected. Some steganographic techniques are particularly difficult to detect without the original image.

♦ SOFTWARE REQUIREMENT

Hardware Resources Required:

Software Resources Required:

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.

Project Resources:
Windows, VS code, eclipse, 8 GB RAM, High speed internet connection.

♦ RELATED WORK

❖ *Risk Management W.R.T. Np Hard Analysis:*

This section discusses Project risks and the approach to managing them.
Risk Identification:
For risks identification, review of scope document, requirements specifications and schedule is done. Answers to questionnaire revealed some risks. Each risk is categorized as per the categories mentioned in. Please refer table for all the risks. You can refereed following risk identification questionnaire.
1. Have top software and customer managers formally committed to support the project?
Ans - Not applicable.
2. Are end-users enthusiastically committed to the project and the system/product to be built?
Ans - Not known at this time.
3. Are requirements fully understood by the software engineering team and its customers?
Ans – Yes.

❖ *Design Constraints*

1. Apache Tomcat webserver.
2. SQL Yog community/ XAMPP Server.

❖ *Software Interface Description*

The software interface(s) to the outside world is (are) described. The requirements for interfaces to other devices/systems/networks/human are stated.

❖ *Area Of Project:*

1. Internet of Things
2. WSN
3. Embedded System

❖ *Relevant Mathematics Associated with The Project*

Let S is the Whole System Consist of
S = I, P, O
Where,
I = input
I = U, AF, VF, A, B
U = User

Sr. No.	Parameter	Minimum Requirement
1	Processor	AMD Ryzen 5
2	RAM	8 GB
3	Hard Disk	40 GB and Above.
4	USB Drive	1

U=u1, u2, ... un

Sr. No.	Parameter	Minimum Requirement
1	OPERATING SYSTEM	Windows 10/11.
2	CODING LANGUAGE	JAVA/J2EE,
3	IDE	VS code/ Eclipse

AF = Audio File.
VF = Video File.
A = Variable a.
B = Variable b
P = Process
P = I, F
F = Functions.
F = AR AW
TR = Text Reader.
TW = Text Writer.

Activity Diagram:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

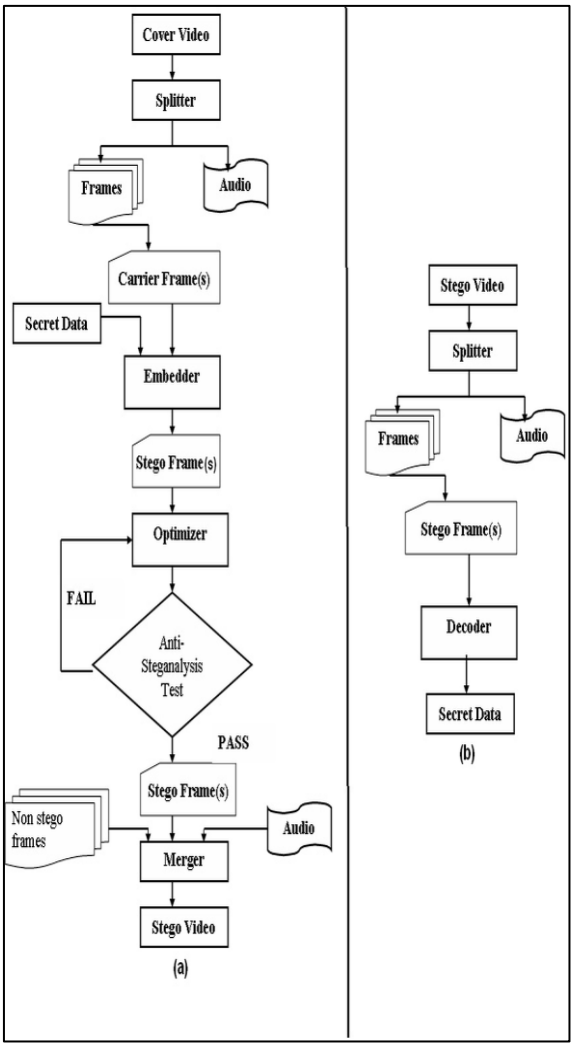


Fig.: DFD 0 level

❖ ***Methodologies Of Problem Solving and Efficiency***

1. **Requirement gathering and analysis:**
   In this step of waterfall, we identify what are various requirements are need for our project such are software and hardware required, database, and interfaces.
2. **System Design:**
   In this system design phase, we design the system which is easily understood for end user i.e., user friendly. We design some UML diagrams and data flow diagram to understand the system flow and system module and sequence of execution.
3. **Implementation:**
   In implementation phase of our project, we have implemented various module re- quired of successfully getting expected outcome at the different module levels. With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase.
4. **Testing:**
   The different test cases are performed to test whether the project module are giving expected outcome in assumed time: All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.
5. **Deployment of System:**
   Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market. There are some issues which come up in the client environment. To fix those issues patches are released. Also, to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment. All these phases are cascaded to each other in which progress is seen as flowing steadily down- wards like a waterfall through the phases. The next phase is started only after the defined set of goals are achieved for previous phase and it is signed off, so the name "Waterfall Model". In this model phases do not overlap.

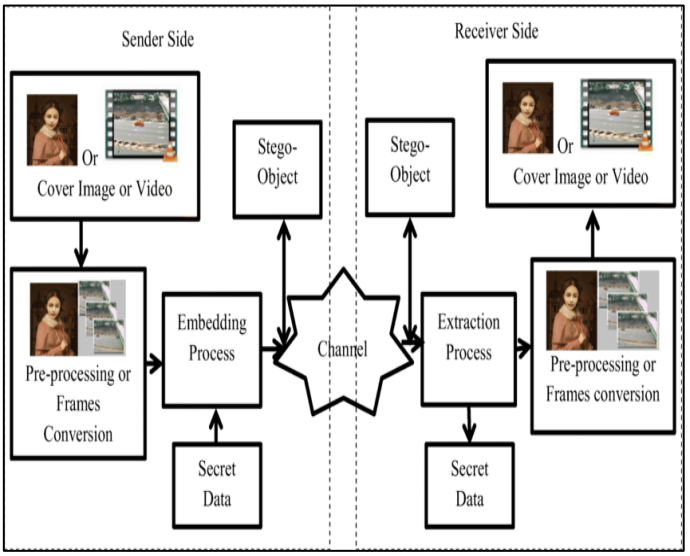


Fig.: Working Model

❖ ***Overview of responsibilities of Developer***

1. To have understanding of the problem statement.
2. To know what are the hardware and software requirements of Proposed system.
3. To have understanding of proposed system.
4. To do planning various activities with the help of planner.
5. Designing, programming, testing etc.

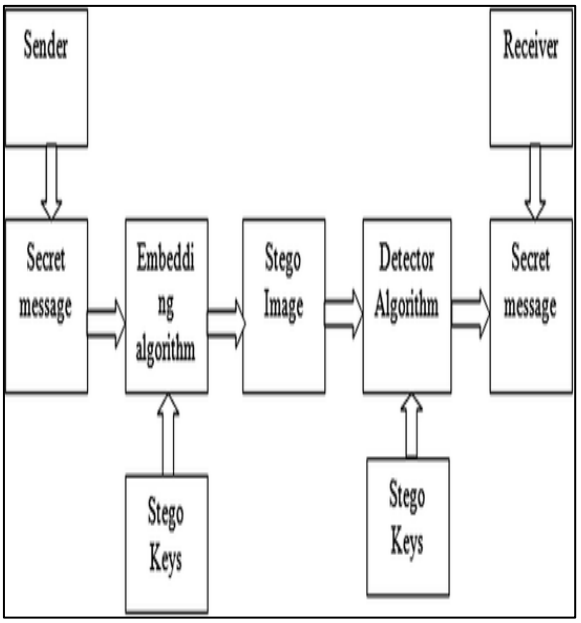
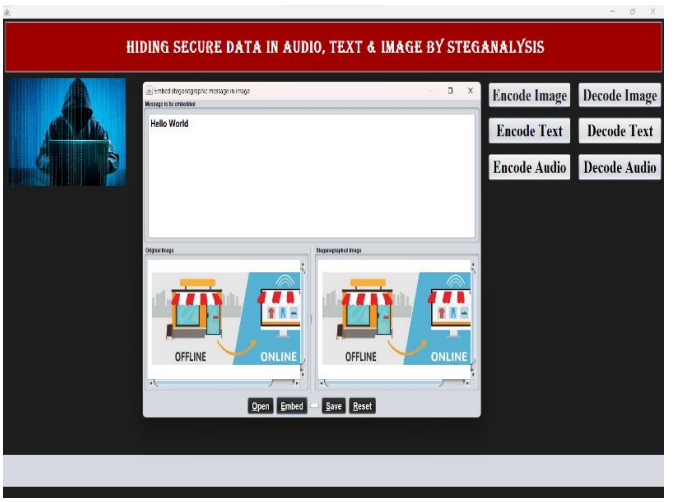
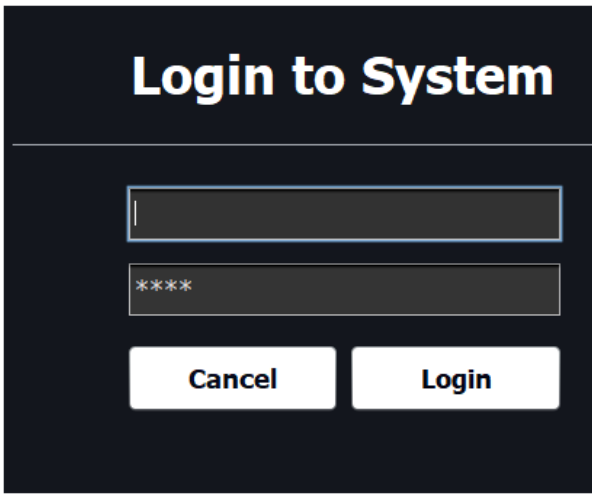


Fig.: Steganography Hiding Videos in Plain Sight

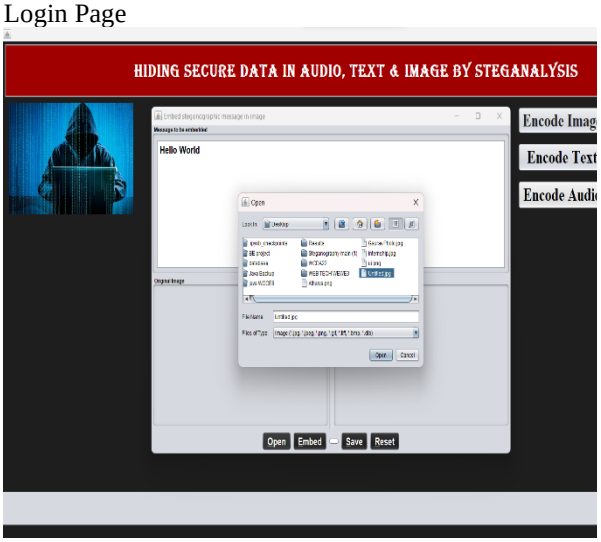


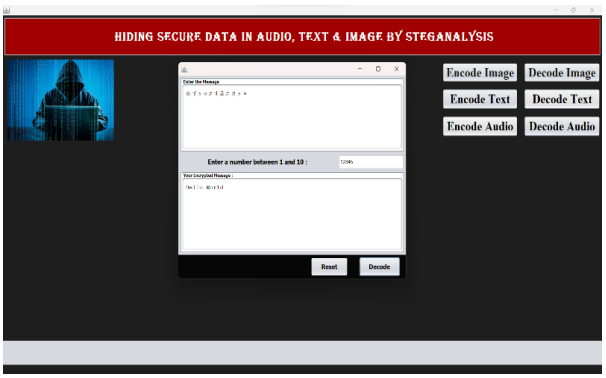
Encode & Decode Image

- **OUTPUT**

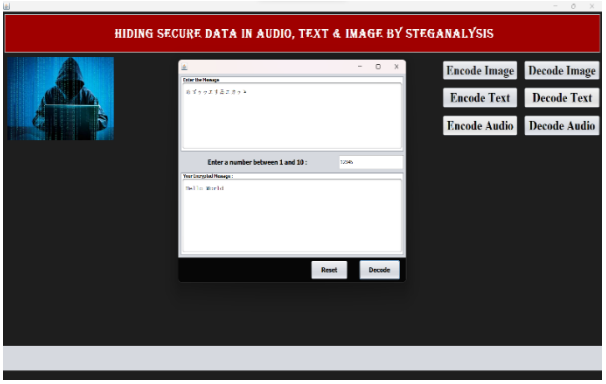


Login Page

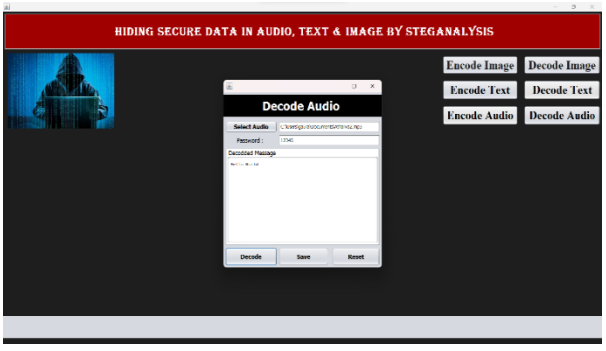




Encode & Decode Text



Encode & Decode Audio



♦ CONCLUSION

In this conclusion, we will be understanding that Steganography use different approaches to secure the communication. Many developers combine different algorithms or modify the original algorithm to generate a new algorithm. The newly generated algorithms come up with more benefits. In this paper we do the survey of different previous papers. Many developers used the LSB, MSB. Parity Coding Phase Coding and 4LSB steganography techniques to hide the secret data. Finally, we conclude that data hiding in audio-video steganalysis by anti-forensics technique is the best technique to hide the secret messages. The data is triple secured with this technique and it provides strong authentication.

♦ FUTURE SCOPE

The project paper does not address the LIVE content streaming of Audio, text, etc. The scope could further be extended to the process of fetching LIVE video content securely by implementing an RBVE algorithm and performing user authentication, as this is an emerging factor within the field of video streaming.

♦ REFERENCES

[1] Ravi Kumar, Kavita Choudhary, Nishant Dubey, “An Introduction of Image Steganographic Techniques and Comparison”, International Journal of Electronics and Computer Science Engineering.
[2] Arup kumar Bhaumik, Minkyachoi, Data Hiding in Video IEEE International journal of data base an application, vol 2no.2 june 2016. Pp.9-15
[3] Namita Tiwari, Dr. Madhu Shandilya, “Evaluation of Various LSB based Methods of Image Steganography on GIF File Format”, International Journal of Computer Applications, Vol. 6– No.2, September 2010, pp .1-4.
[4] Alkhraisathabes. Information Hiding in BMP Image Implementation, analysis Evaluation Information transmission in computer network, fall2017, Volume 52. issue, pp. 1-10
[5] V. Sathya, K. Balsubramaniyam, N, Murali, Data hiding in audio signal, video signal text and JPEG Image, IEEE ICAESM 2019, March 30-3-2019, pp741-746
[6] S. Gao, R. M. Zeng H. Jai, A A Detection algorithm of audio spared spectrum data hiding 2020 IEEE international conference, pp1-4.