ENHANCING VIDEO STEGANOGRAPHY USING GENETIC ALGORITHM

Mrs Gunjal S.V, More Sahil, More Rohan, Darekar Dhananjay

Lecturer Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India
Student Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India
Student Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India
Student Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India

ABSTRACT

Today's age century of modernism, there is a broad variety of technical developments accessible, and anyone can easily make utilize these breakthroughs to improve the effectiveness of their enterprises. This is one of the many benefits of living in a time age of modernity. On the contrary extreme, as technical advancement increases, so does the complexity of criminal behavior. [Criminals] are becoming more and more sophisticated. Particularly with reference to the stealing of data as well as the pirating of material by bad actors. The application of steganography is one of numerous methods that, when combined, have the potential to protect the transmission of information and, as a result, lessen the likelihood of deceptive practices and violation. Steganography is a process that hides content in digital photos in such a way that it cannot be identified by any persons who are not permitted to see it. The secrecy of the information that is being sent is maintained as a result of this measure. The process of acquiring steganography on such a video is one of the greatest cutting-edge extremely challenging tasks that has been performed in the recent few years. Steganography may be used to hide information on a recording. Steganography is a method that is used in order to conceal content on videos. As a result, in attempt to execute video steganography a byte Extraction along with Genetic Algorithm for bit Identification is employed for Least Significant Bytes Labeling. All of these steps take place prior to the labeling of the least significant bytes. Quantification of the technique has been achieved by exhaustive assessments, which have been essential in confirming the success of the suggested strategy.

Keywords: Frame Extraction, Genetic Algorithm, LSB Labeling, , Steganography.

INTRODUCTION

The establishment of online media that is accumulated on the online platform has evolved into a consideration which is of vital significance as a result of the rapid increment in the number of personal devices and the proliferation of information, in addition to the considerable rise in the utilization of mediums of communication in the transmission and reception of relevant data. As a consequence of this, the researches concentrate their resources on the development of methods that may protect the key data and make it a bit more secret, with the purpose of deterring cybercriminals as well as other unwelcome individuals from obtaining accessibility to the information. Cryptography is a process that is used to protect sensitive information by encoding it in such a way that nobody else except the reliable individual who holds the special key can comprehend or gain access to it. This approach is known as an encryption technique. Encryption is the method that is used in order to achieve this goal. It is conceivable to encode and decipher data employing any among a variety of different methods. However, with the

development of the Internet, each of those methods became obsolete, which is why it became necessary to search for further techniques for data concealment.

Individuals who are now functioning in our contemporary day depend heavily on the internet for a variety of reasons. The rapid spread of something like the Worldwide Web is assisting in simplifying people's day-to-day lives easier in a variety of ways. The examples listed below are examples of usage of the online network that may function as characterizations: computerized banking transactions, online booking reservation, mobile shopping, etc.

The other component of the architecture which has the greatest impact on individual life is the social media services. These include webpages including such Messenger, Snapchat, Instagram, and Google, among many others. Through this characteristic, individuals are capable of communicating really crucial data and articles among themselves. People are more likely to share their private information with other people as a direct consequence of the World Wide Web. If users communicate sensitive information through the internet, you put yourself at danger of being attacked by hackers and other cybercriminals. Therefore, ensuring a high degree of data security throughout the whole of the purpose of transitioning data from the internet has to be of the utmost importance. Encryption and steganography are likely to be absolutely important in attempt for us to be successful in overcoming this obstacle.

Initially, the sensitive data is confidential, and then, when it has been encoded, it is hidden among the image sequences of the movie. A methodology that employs cryptographic methods to jumble personal information in order to safeguard that information from becoming decoded by unapproved persons, cryptography is known as a cryptographic procedure. The procedure of hiding data below an image or video is exactly the same as the technique of hiding data behind such a short video clip. Within the framework of the technique that has been described, video is used as the supplemental content. The video is dissected into its component parts, also known as frames or images, so that the private information may be concealed. Last but not least, the sensitive information may be sent in the form of words, or it might cloak as part of a documentation that is shown as a clip.

The concept of steganography emerged as a logical result of this event and continued to develop from there. The process of steganography makes reference to the scientific knowledge of hiding information or the interaction between both the transceiver and the receiver of private information by utilizing the host form of media as a shroud, which may include clip, sound, pictures, or message. Steganography is a procedure that pertains to the scientific knowledge of knowledge concealing or the information exchange here between transponder and the receiver of private information. The distinction between cryptography and steganography is based on the fact that perhaps the definition pertains to the procedure of rearranging the contents in such a fashion of that kind so that only the envisioned recipient of the message can acknowledge it, while the second term describes the process of disguising information within a shield without modifying the arrangement of the information in any way. This is the key difference between the two terms.

The Caesar as well as Vigenere cyphers as well as bit - wise and or functions are included into the initialization step in the least significant bit steganography technique. The strategy that was proposed was tested with a number of various pictures and three distinct messaging lengths; the results showed that a mean maximum signal to noise ratio of more than 40 dB could be reached. According to the findings, the strategy seems to be successful. Having a higher payload size, on the other hand, has a negative impact on the picture quality. During the process of encrypting a signal, a peak signal noise ratio that was less than 40 dB was observed; nonetheless, the ratio remained larger than 30 decibels. As a result, it is recommended that an increased image resolution be employed so that the graphical fidelity may be maintained. To maintain your covert status, one should encrypt the payload.

LITERATURE SURVEY

The Caesar as well as Vigenere cyphers as well as bit - wise and or functions are included into the initialization step in the least significant bit steganographic technique that was suggested by P. A. Shofro et al. [1]. The strategy that was proposed was tested with a number of various pictures and three distinct messaging lengths; the results showed that a mean maximum signal to noise ratio of more than 40 dB could be reached. According to the findings, the strategy seems to be successful. Having a higher payload size, on the other hand, has a negative impact on the picture quality. During the process of encrypting a signal, a peak signal noise ratio that was less than 40 dB was observed; nonetheless, the ratio remained larger than 30 decibels. As a result, it is recommended that an increased

image resolution be employed so that the graphical fidelity may be maintained. To maintain your covert status, one should encrypt the payload.
A test photo was encrypted using an embedding encryption approach that was introduced by H. Mathur and his colleagues. They used MATLAB to model the intended task, and then they used it to accomplish the simulation. The proposed architecture has indeed been modeled, and the outcomes have been published and contrasted to earlier work in regards to the number of bits per pixel, the entropy, and the amount of processing time. A histogram was also created based on the work that was recommended [2]. The modeling and implementations in real-world settings of the work that is being suggested illustrate its remarkable efficiency and higher level of security. Whenever the time arrives, they might decide to utilize cheerful text attacks to evaluate how effectively the recommended strategy secures important data. There are a few adjustments that need to be made in order to increase the decorrelating capacities of the iterative method. It is possible that the affine conversion that has being recommended for picture deconstruction decoding and encoding will need to be switched to a different transformation that has better decorrelating characteristics and a reduced computational expense.

Xianfeng et al. [3] suggest using video steganography as a defensive mechanism versus the standard occurrence of transcoding films before posting these to social media platforms. This strategy is intended to combat the ubiquitous use of the technique. To get started, an adaptable screening strategy that is centered on principal component analysis is used to choose regions that are suitable for resilient anchoring. A dual-channel simultaneous implantation that is dependent on the constituents is constructed so that the insertion and extraction regions may be synchronized with one another. In the third step of the process, a video processing method is used to generate covering movies that simulate transportation channel matching. Programming devised by Bose, Chaudhuri, and Hocquenghem has made it possible to eradicate error bits once and for all. To confirm the coherence and sustainability of the strategy that has been offered, in-depth investigations are carried out on locally imitated channels, as well as on YouTube as well as Vimeo. The results of the experiments provide convincing proof that the proposed method is resistant to video transcoding. When compared to other options, conducting hidden conversation via websites such as YouTube as well as Vimeo is an approach that is both more secure and much more reliable. VStegNET is an initiative that was first of its kind in the annals of the development of video steganography. VStegNET and other algorithms that rely on two-dimensional Convolutional Neural Networks have had their functionality evaluated and contrasted by Islam et al.

SCOPE OF THE PROJECT

Scope of Secure Video Steganography for Multi-Variant Files is explained below

3.1 Nevon Project: Secure data transfer using video steganography

This project consists of an implementation of video stenography technique performed on a lossy compression applied video file. This allows user to transfer a quite high amount of secret data over insecure networks. This process is based on a compressed wavelet technology in accordance with an innovative technique known as (BPCS) bit-plane complexity segmentation data hiding. In most of the video compression techniques that make use of wavelet dependent technology like the 3D and 2D set partitioning in hierarchical trees (SPIHT), the wavelet variables that lie in the processed wavelet transformed video data file are then converted using a quantizer to a bit-planed form and therefore this BPCS steno-data is formed. This can be used over the wavelet projects area.

Reference : https://nevonprojects.com/video-steganography/

3.2 ProQuest: Forensic analysis of video steganography

Steganography is the art and science of hiding information in plain sight. By ensuring that data is hidden from casual observers, a stego-system aims to reduce any suspicion that a third party may have over occurring communication. This can be a valuable resource where free speech is not guaranteed. In this and many other related contexts, steganography provides an ideal solution which makes it possible to avoid censorship (Krenn, 2004). An ideal stego-system should typically allow for highly sensitive information to be securely exchanged without the knowledge of others.

Reference:https://www.proquest.com/docview/1956791137?sourcetype=Scholarly%20Journals

METHODOLOGY

The methodology for Secure Video Steganography for Multi-Variant Files is developed under waterfall model architecture as shown in the below figure 1.

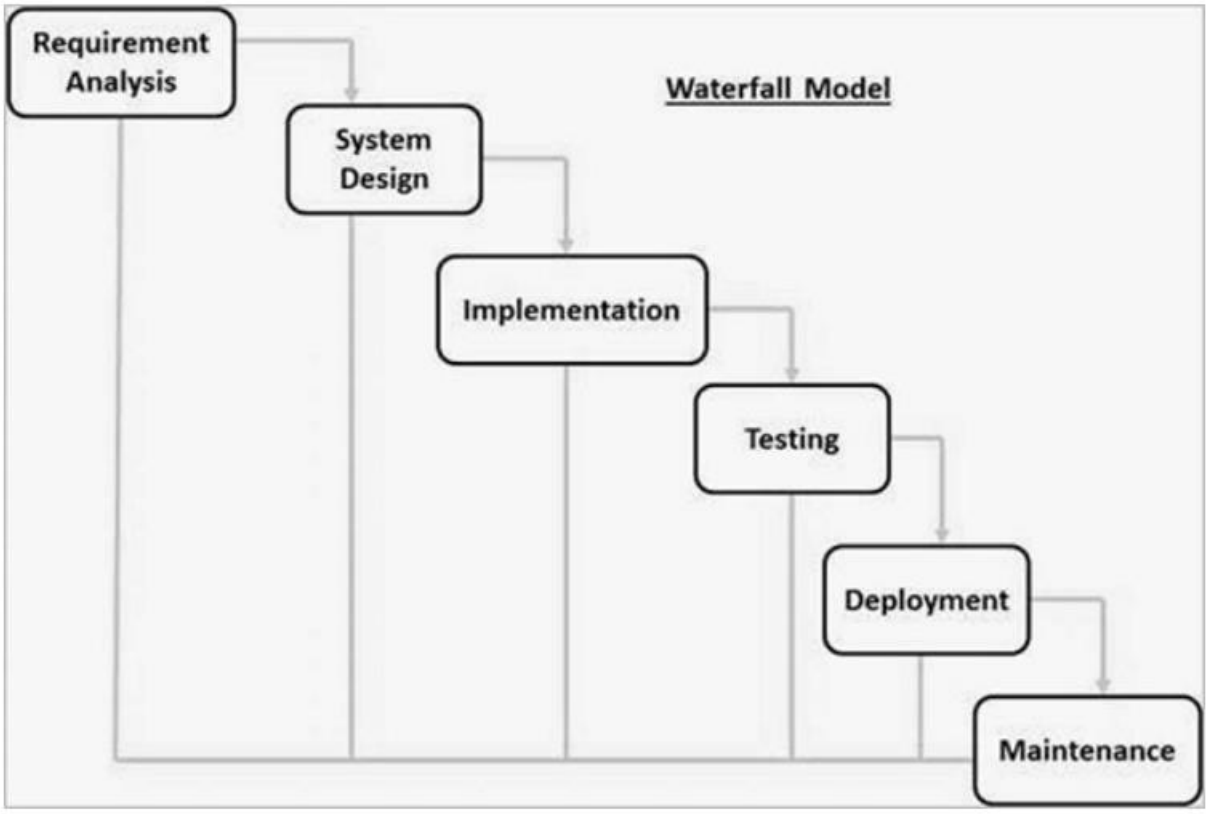


Fig 1 : Water fall model Architecture

The sequence phases in water fall model according to our project are mentioned below.

4.1 Requirement Analysis – Here requirement analysis are done based on following points

- ✓ Base paper for Secure Video Steganography for Multi-Variant Files.
- ✓ Study the Genetic Algorithm

4.2 System Design: The System of Secure Video Steganography for Multi-Variant Files is designed by using the following hardware and software

Minimum Hardware Specification:

- CPU : Core i5
- RAM : 8 GB
- HDD : 500 GB

Software Specification:

- Coding Language : Java
- Development Kit : JDK
- Front End : Swing Freamework
- Development IDE : Netbeans 8.2
- Database : MySQL 5.0

4.3 Implementation:

Proposed system is designed by using the following modules

4.3.1 Module A: Generic Algorithm

- Initial Population
- Mutation
- Cross Over
- Frame Selection

4.3.2 Module B: LSB

- Pixel Matrix
- Byte Estimation
- Byte Comparison
- LSB Byte List

4.3.3 Module C: Text Byte Array

- Plain Text
- Transformation
- Key Padding
- Cipher Text

4.3.4 Module D: Encoding

- LSB List
- Byte List
- Byte Embedding
- Normalization

4.5 Deployment of the system:

The developed software is deployed in the laptop of above mentioned configuration with the help of the mentioned software.

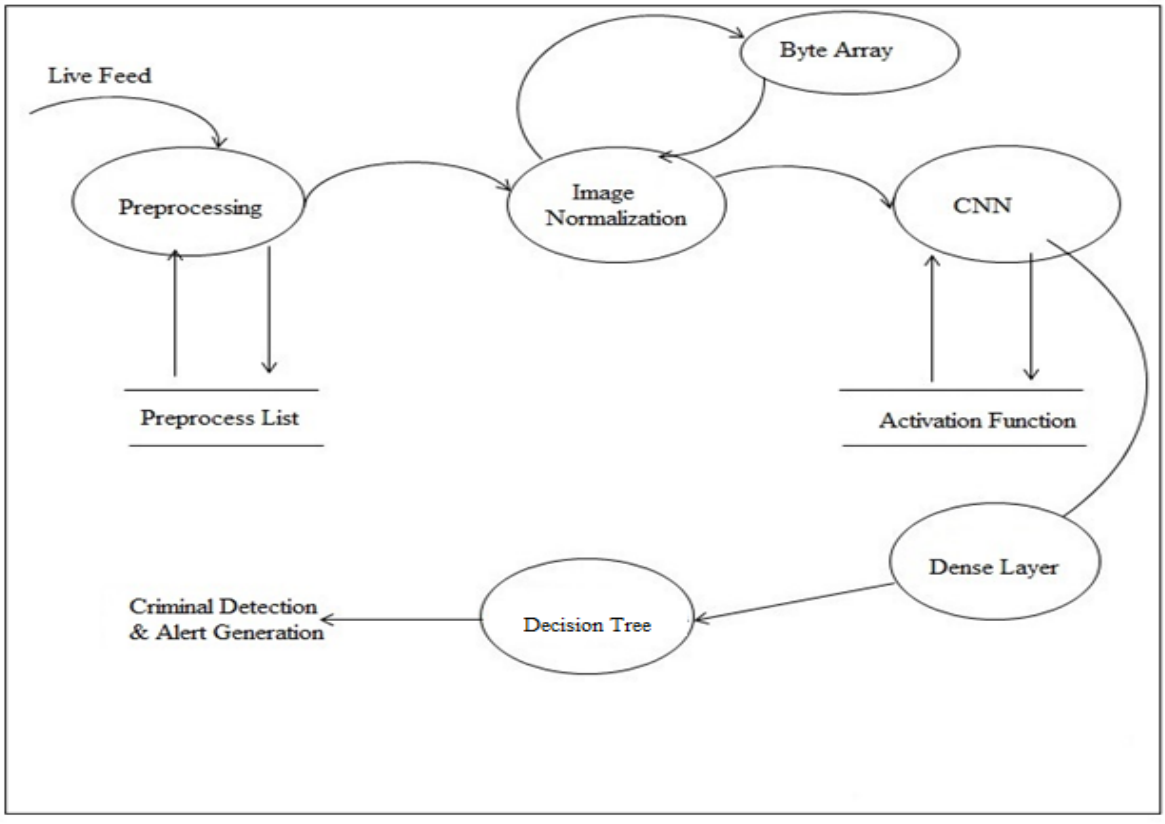
4.6 Maintenance of the system:

As this software is tested for the quick recovery, so maintenance of the system is not a challenging task. This is because the tools and the software used are open source, so there is no question of licensing the required software.

DETAILS OF DESIGN, WORKING AND PROCESSES

1 DETAILS OF DESIGN

2 WORKING AND PROCESSES



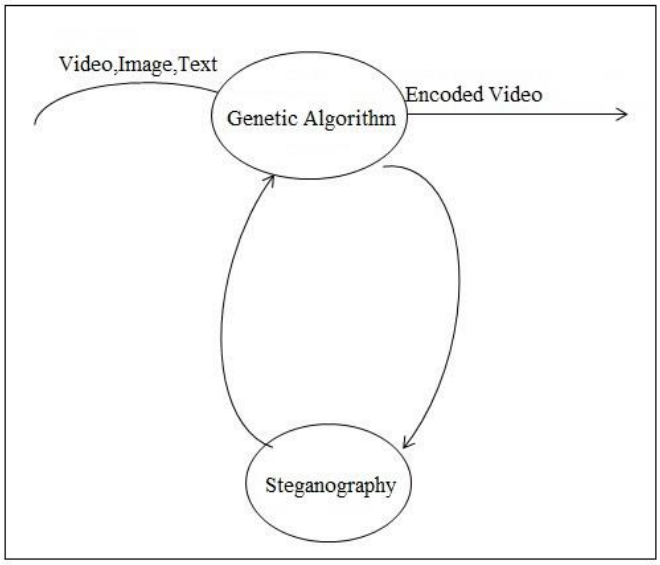


Fig 2 DFD level 0

The DFD 0 diagram for the data flow diagrams describes the flow of the approach. The DFD diagram provides the simplest flow where in the frames of the video, image and Secret Text are provided and the Genetic Algorithm is implemented and encoded video is realized using Steganography.

5.1.1.2 DFD level 1

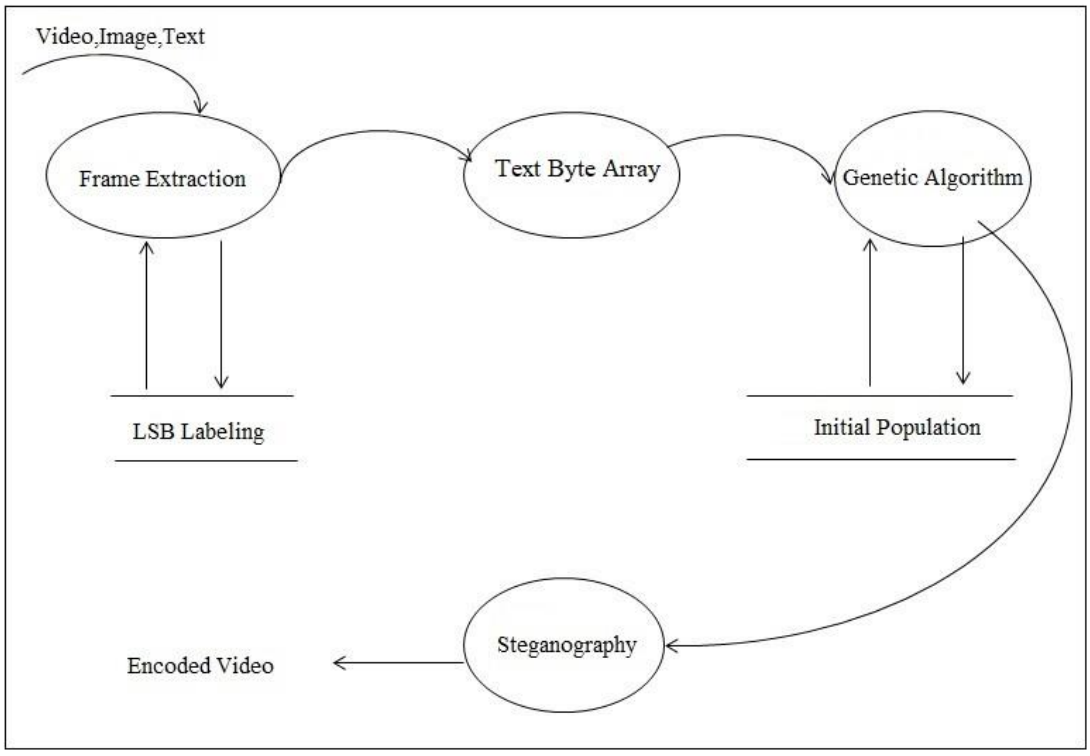


Fig 3 DFD level 1

The DFD 1 diagram provides even more details wherein the user provides the video, image and secret text from which the frames are extracted and the LSB labeling is performed. The Genetic Algorithm is utilized and the initial population is formed after which the steganography technique is applied and the encoded video is achieved.

5.1.1.3 DFD level 2

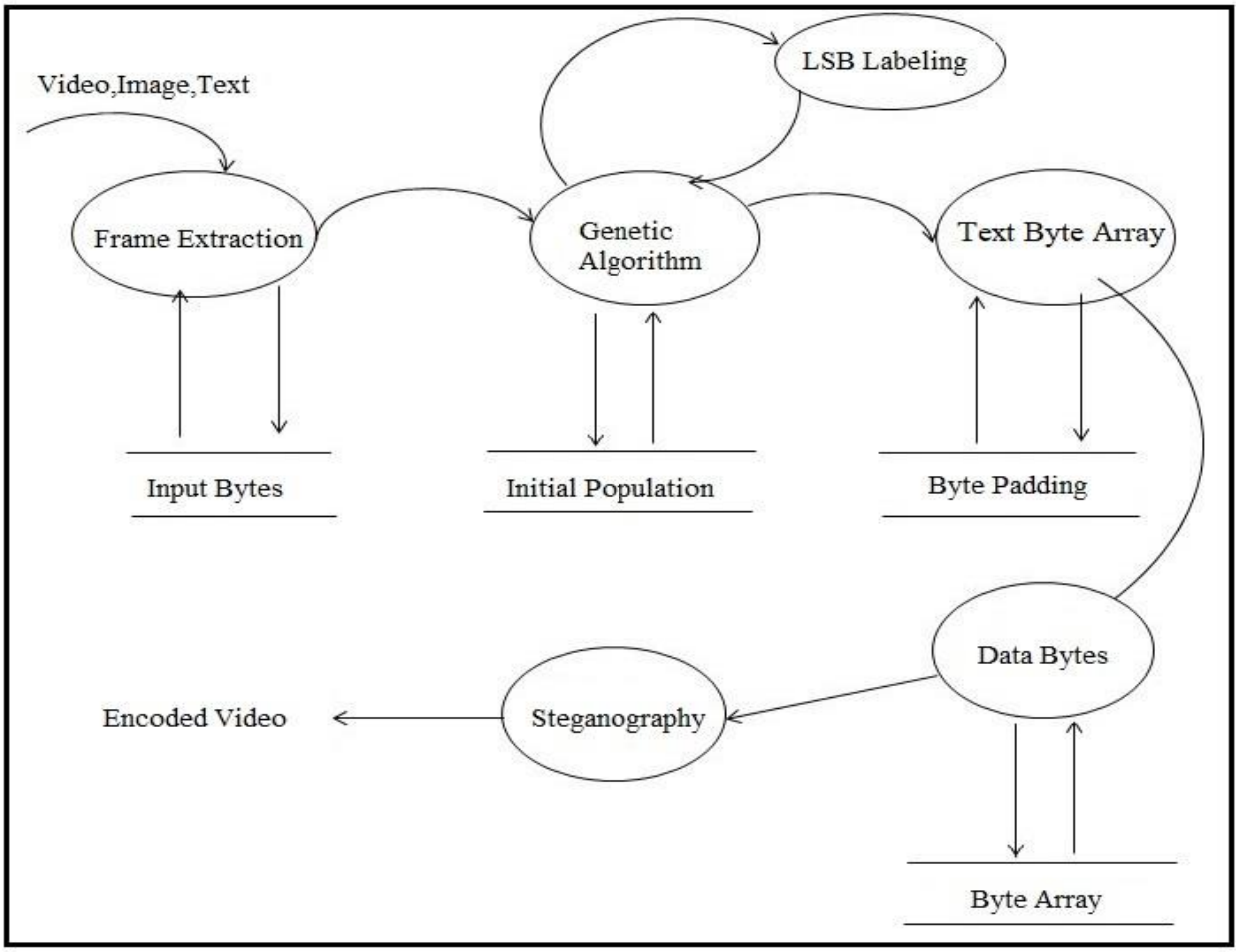


Fig 4 DFD level 2

The DFD 2 diagram is the most detailed wherein the user provides the video, image and Secret Text from which the frames are grabbed and the input bytes are extracted. The Genetic algorithm is utilized through LSB labeling and the initial population is formed after which the Text byte array technique is applied with byte padding. The resultant data bytes are utilized in a byte array to perform video steganography which results in the encoded video.

5.1.2Activity Diagram

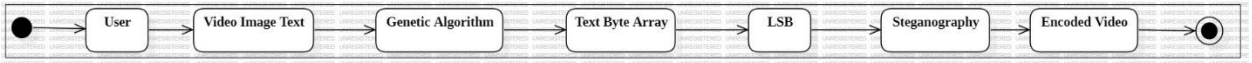


Fig 5.1 Activity Diagram

The activity diagram lists the various activities that are performed in the proposed methodology, the start state is initiated and the user provides the video, along with image or text, after which the genetic algorithm is initiated, the Text byte array follows, the Least Significant Bit calculation that leads to Steganography and results in the Encoded Video.

5.1.3 Usecase Diagram

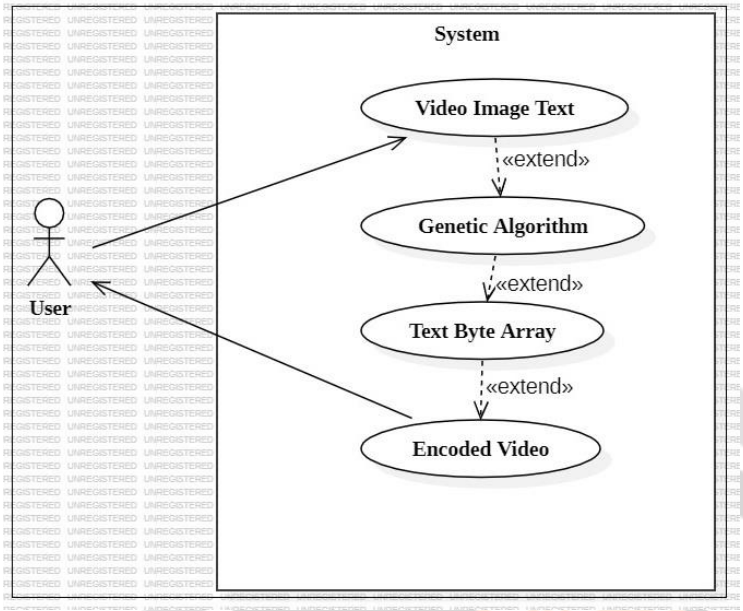


Fig 6 Usecase Diagram

The Use case Diagram depicts the various use cases that are performed by the user in the proposed model. The use cases include, feeding video, image and secret text, Genetic Algorithm, Text Byte Array and finally views the Encoded Video.

5.1.4 Sequence Diagram

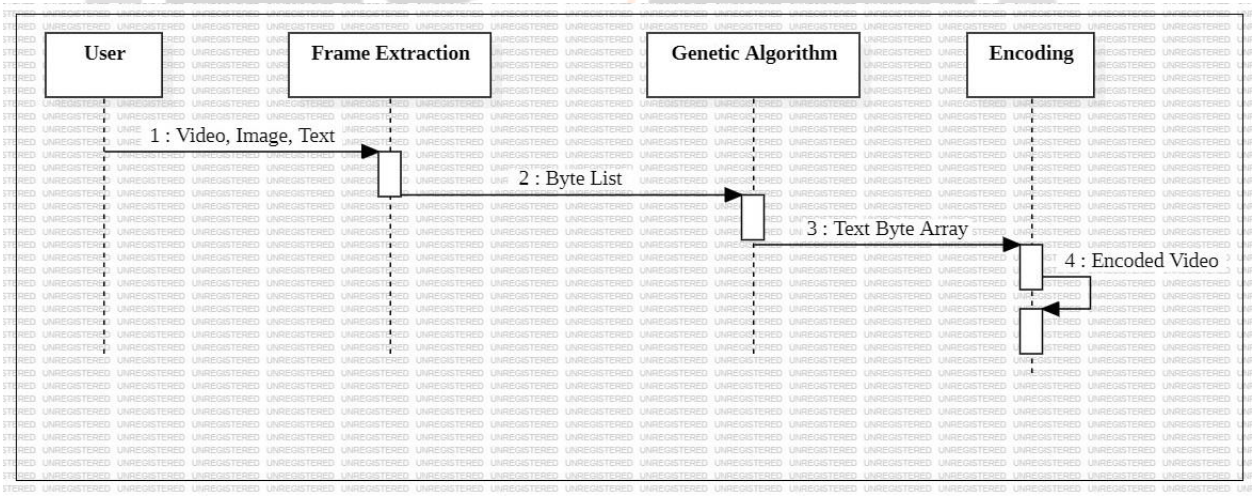


Fig 7 Sequence Diagram

The sequence role diagram provides a sequence of the approaches as well as the various roles performed in the intermediate. In this approach the video, image and secret text is provided to the system and frame extraction is performed. The byte list module is initialized which initiates the genetic algorithm. The text byte array is then used to achieve the encoded video.

5.2 WORKING AND PROCESSES

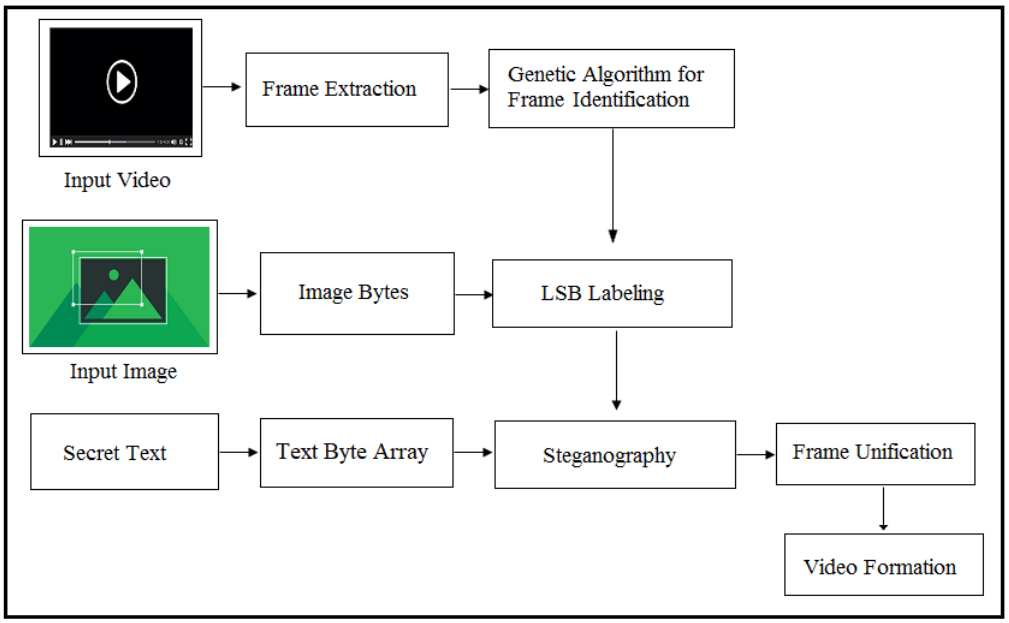


Figure 13 System Overview

The proposed methodology for video steganography is narrated in this section with the below mentioned steps.

Step 1: User Registration and Login: The user must register with the system before they may access it. The user is presented with a form with different fields that collect user information like as name, username, mobile number, email address, etc. Upon registering on the swing platform, the user can log into the system after these details have been entered and verified by the system. The user may begin the steganography process by choosing the proper choice for encoding an image or text file in the video after the user login has been completed.

Step 2: Video Encoding: The user must select the video file in.mp4 format along with the text file to encode in it. This process also takes the key and the encoded file name in which the video is going to be stored after the encoding process. The steps of genetic algorithm undertaken for encoding the image or text file in the video can be seen in detail in the below mentioned points.

Initial Population- The first step of the genetic algorithm is to form the initial population of the bytes are formed by reading the input video files. The video file is being read in buckets of 8 bytes, so an iteration is being run to read all the bytes of the video file. In each iteration, 8 bucket bytes are being fetched and written on a file output stream object.

Fitness function- In genetic algorithm, the fitness function is a function that evaluates how ”fit” or ”good” a candidate solution is in relation to the problem under discussion. It accepts a candidate solution as input. The calculation of fitness value must be quick enough because it is performed repeatedly in a genetic algorithm. A genetic algorithm may be negatively impacted and become excessively slow due to a slow computation of the fitness value. Since the goal is to either maximize or minimize the specified objective function, the fitness function and the objective function are typically the same. However, an algorithm designer may decide to use a different fitness function for harder problems with numerous goals and constraints.

Then a fitness function is picked for the value of 1 byte with the difference of the last bytes written of the initial population to write the linear sequence of the space to hide the message in at 26 + 1 bytes.

Selection - A small percentage of the current population is chosen to breed a new generation in every generation that follows. A fitness-based selection approach is used to choose individual solutions. Since we are in generation 0, we have no offspring. We pick parents from the text or image input file bytes that the user has provided for encoding the video for the resulting population. In this phase of the genetic algorithm, the file name of the text file to be encoded is chosen. The filename bytes are then read into an 8-byte array of instances and written into that array. The encoded video files are then sent through email to the recipients using the built-in Gmail host API key in step five, data transmission. This is accomplished at the swing framework’s intended user interface to improve the edge of the created application. On the other side, the recipient will utilize the encoded information to reverse the process using decoding choices once he receives the file and key by email in order to recover the concealed message

CONCLUSION

In this methodology, the suggested methodology for producing steganography for video has been fully clarified. A video file can be the input carrier file. These are the cover files that will protect the hidden content, such as a secret message or secret data. These files contain an input video file that is efficiently processed by separating out the video's constituent frames. The genetic algorithm is used to implement the process of identifying the bytes that can be used for steganography. The use of the genetic algorithm enables the theory of evolution to be used for the goal of choosing the right frame from the video that will be the best for hiding. For LSB labeling, these bytes are used in conjunction with the video's specified bytes. Once the steganography is complete, the data is reformed and the frames are united to create the original file, which is free of any traces of the hidden information. Utilizing experimental assessment, the approach has been thoroughly evaluated with incredibly successful outcomes.

Future Work

The cloud platform can be used in the future to implement an efficient steganography method that is portable and simple to use.

REFERNCES AND BIBLIOGRAPHY

[1] P. A. Shofro, K. Widia, D. D. A. P. Astuti, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, ”Improved Message Payload and Security of Image Steganography using 3-3-2 LSB and Dual Encryption,” 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018, pp. 158-162, DOI: 10.1109/ISRITI.2018.8864285.

[2] H. Mathur and S. Veenadhari, ”Blended Vector Matrix on Different Channels of Image Encryption with Multi-Level Distinct Frequency Based Chaotic Approach to Prevent Cyber Crimes by Using Affine Transformation,” 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 650-656, DOI: 10.1109/ICICCT.2018.8473235.

[3] Fan, Pingan & Zhang, Hong & Zhao, Xianfeng. (2022). Robust video steganography for social media sharing based on principal component analysis. EURASIP Journal on Information Security. 2022. 10.1186/s13635-022-00130-z.

[4] S. Kumar, N. K. Singh, A. Majumder, and S. Changder, ”A Novel Approach to Hide Text Data in Colour Image,” 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2018, pp. 577-581, DOI: 10.1109/ICRITO.2018.8748390.

[5] Rajkumar, Gat & Malemath, Virendra. (2017). Video Steganography: Secure Data Hiding Technique. International Journal of Computer Network and Information Security. 9. 38-45. 10.5815/ijcnis.2017.09.05.

[6] S. Shakeela, P. Arulmozhivarman, R. Chudiwal, and S. Pal, ”Double coding mechanism for robust audio data hiding in videos,” 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2016, pp. 997-1001, DOI: 10.1109/RTEICT.2016.7807979.

[7] A. U. Islam et al., ”An improved image steganography technique based on MSB using bit differencing,” 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 2016, pp. 265-269, DOI: 10.1109/INTECH.2016.7845020.