Enhancing Video Steganography through Genetic Algorithm

1. Tarak Bharambe, B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India
2. Jui Thule, B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India
3. Abhishek Chaudar, B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India
4. Sejal Raotole, B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India
5. Mrs. Pradnya Kasture, Professor, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Pune.

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*

I 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 cloaked 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 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.

Section 2 of this research article presents an analysis of the relevant literature; Section 3 explains the research approach; Section 4 discusses the experimental assessments; and Section 5 closes with suggestions for further study in the future.

II RELATED WORKS

A mechanism that might deliberately inject the pixels was devised by S. Kumar and his colleagues [4] in order to hide content. The noise foundation that was produced as a consequence is ordinary and doesn't trigger any warning bells. The histogram of the stego picture displays very tiny variations from the underlying cover image, which is confirmation of the stego picture's improved image fidelity in compared to the standard approach of using the least significant bytes. Whenever the hidden information is incorporated into an image, it produces very minimal deformation, that may be quantified by the peak signal-to-noise ratio. This strategy works better than the usual method of substituting the least significant bytes. This included distortion component should automatically mirror what the picture acquires from either the transmission medium in regards of the way it behaves because of the relationship between the two. As a result, the noise introduced by the transmission channel increases the likelihood that the image irregularity, regardless of how minor it may be, found by the steganography technique will be overlooked. In additional to the discriminating requirements that have been specified for the technique, just one bit per pixel is altered; as a result, there is not much of an impact on the overall dimensions of the picture.

Rajkumar and his colleagues suggested the use of videos. [5] Steganography provides an additional layer of safety to a systems when it is used in conjunction with encryption. The proposed method will resulting in the data being encrypted and then embedded directly inside the video files itself. Each image conceals three separate components of data when seen in sequence. Regarding the movie that is going to be made, steganography is tested using video as well as secret data of varied sizes. The fidelity of the encoded video is shown not to have been considerably compromised by the approach that was presented. This video's quality is on par with the one it was ripped from. The person who is in possession of the key to decode the stego video is the receiver of the stego video. It is hard to determine for definite whether or not there are information that has been concealed. As a result, there is no need to worry about the information being sent to its ultimate destination. The Data Encryption Standard technique is the encrypted communication technique that is now in use that is the least complicated and most easy. In spite of the fact that it is uncomplicated and makes use of strategies that are generally used, it offers a way of data transport that is both speedy and safe.

The method of data concealment that was proposed by S. Shakeela and her colleagues is efficient and risk-free at the same time. Because this method uses a twofold coding scheme, the steganography is incredibly safe, and it will be challenging to uncover the material that has been concealed because of it. That whenever a wavelet transform approach is utilized, the steganographic video may be displayed with just a little reduction in quality brought on by the reduction. It is remarkable that the proposed technique is still able to protect a significant amount of secret information from certain compaction attack provided that it is public knowledge that compaction eradicates unnecessary features from the media format. Nevertheless, the proposed approach does maintain to save this hidden data. If the information in issue is sound and it is recovered from a film, it will not sound precisely like the soundtrack or audio data that have been initially put in the footage [6]. This is because the concealed content was inserted in the film after the fact. Basic functionality of the sound data is needed in order to obtain an audio experience that is nearly similar. This is necessary since rounding, various processing steps, and compression methods may all potentially add distortion. As a result, the scientific and technological advancement might significantly benefit from the implementation of this plan. More effort is required to make enhancements to already existing techniques as well as to identify flaws in confidential and secure communications.

A most important bytes-based approach of picture steganography is described in A. U. Islam et al[7] .'s research. This technique is rooted in the fact that perhaps the cover image is encrypted using the differential between the bits of two pixels. The elements that are going to integrated into a pixel are the five and sixth ones in its representation. The magnitude of the discrepancy among bits 5 and 6 is determined by the bit that indicates the entry of confidential info. Bit 5 may be kept unaltered if the differential among bits five and six is the same as the secret bit that is being received. In the event that the differential between bit 5 and bit 6 does not reflect the value of the entering bit, bit 5 is reversed such that both values are equal. Switching to using the most significant bytes instead of the least significant bytes improves the system's protection since steganographic algorithms often concentrate their efforts on the least significant bytes. In particular, the approach that was presented has a greater peak signal noise ratio compared to the other ways that were being used, which shows that the method is effective via the use of comparison. The proposed approach is able to hide more content inside a single cover picture, and its actual quantity is also higher than that of the solutions that are already in use.

Convolutional neural networks were used to construct the one-of-a-kind encoder-decoder structure that was introduced by Rehman et al. [8]. This technology was used for picture steganography. In comparison to earlier methods, which only

implemented a binary illustration as payload, the current proposed approach combines a couple of encoder-decoder channels to incorporate an image information as payload as well as vigorously recover it from an provided cover picture. This is accomplished by combining a couple of encoder-decoder connections. Extensive testing has shown that the proposed approach is effective, and the considerable actual quantity has led to great results across a range of exotic datasets. This was shown by the fact that the testing was carried out.

Using an encrypted communication scheme methodology and a shifting algorithm predicated on steganography, as well as the assistance of a visual encryption algorithms, S. Chavan et al. [9] suggested a methodology that tends to make use of a visual encryption algorithms. This technique also makes utilization of a data encryption arrangement technique. It is possible to accomplish the same degree of success with steganographic as well as visual encrypting as one would with traditional picture security. As a result, every effort to decipher the authentic information that has been preset becomes more impossible.

The security features of steganographic methods may be significantly improved by employing the least significant bit handling through out shifting technique as well as the rest of the process. The intended technology is capable of producing the best greyscale result, which not only renders it more useful in the implementation of real life but also makes it resilient to RS assault.

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. [10]. They demonstrated, by making use of several of the industry-standard procedures available to them, that not only does their approach function well numerically, but it is also impervious to steganography. The current proposal extends oneself to the several natural attachments and advancements, such as the integrating of extra information in the cushions, the online visibility of other kinds of media including such pictures, message, sound recording, and so on, and the extension of antagonistic loss for greater resistance to steganography. These extensions and improvements are all possible thanks to the model's adaptability. An information revolution that the authors intend to collaborate on is the reoccurring repository of private documents in the cover of the canister in both geographical and temporal areas. This is aimed at avoiding issues that can be caused by improper utilization of the canister, including the emergence of noise, the compaction of video, or the trimming of video, amongst other things.

Younus et al. [11] established a novel strategy for video steganography that takes use of a suggested key function technique to encrypt a concealed message. This strategy was designed with the intention of making the system more secure. The recommended method makes use of a major feature for encryption that consists of an organization of parameters associated and allows for the numbers to be changed with each transaction. This helps to increase the method's efficiency as well as its robustness. In regards, the knight trip is employed to enhance the least significant bytes methodology that is used for storing the information from within the image sequence. This is accomplished by selecting the encoding pixel value at unexpected times rather than in a serial style, as is accomplished with the conventional least significant bytes. This prevents hackers from determining whether the pixels encompass the classified data. The results of the experiments indicate that the proposed method is superior to the current state of the art in regards to peak signal noise ratio, average square error, and security.

A binary attention process approach to image steganography is presented by Yang et al. [12], with the intention of reducing the impact of steganography on the functions that are automatically performed by neural networks. The first proposed technique is the picture texture sophistication concept, which assists in locating the locations of the pixels as well as their capacity for modification without becoming detected by the visual system of humans. Rebuilding feature maps is the focus of the following model, which is known as the reducing feature deformation model. This model works to reduce the impact of embedding. This study also proposes a significant amount of attention be paid to fusing and fine tune methods to better the accuracy of both hidden information retrieval and privacy. In this study, the proposed methodology effectively illustrates the marginalization of confidential info by illustrating that integrated images may avoid detection using a diverse range of steganography methodologies. Specifically, the approach shows that the cloaking of classified material is achieved by hiding the images within the text.

III PROPOSED METHODOLGY

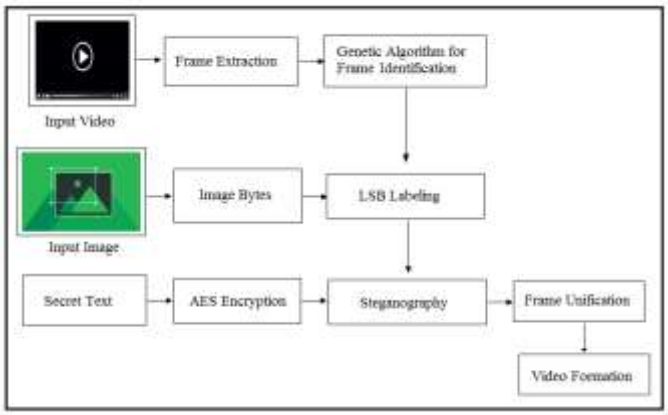

Figure 1: Proposed Methodology

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.

Cross Over and Mutation- The procedure of crossover, mating, and breeding is the next. Crossover describes the process through which some genes from both parent chromosomes are positioned next to one another, jumbled together, or swapped to create new children. Because of the crossing of the parent chromosomes, the baby possesses traits from both parents. Three techniques can be used to perform crossover during the encoding process of a video file.
The entire content of the input text files is read into a stream of bytes at the crossover step of the genetic algorithm. The output stream is then crossed every 8 bytes to create the encoded video file.

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.

The whole process of embedding image and text into the video files is depicted in the flowchart of figure 2.

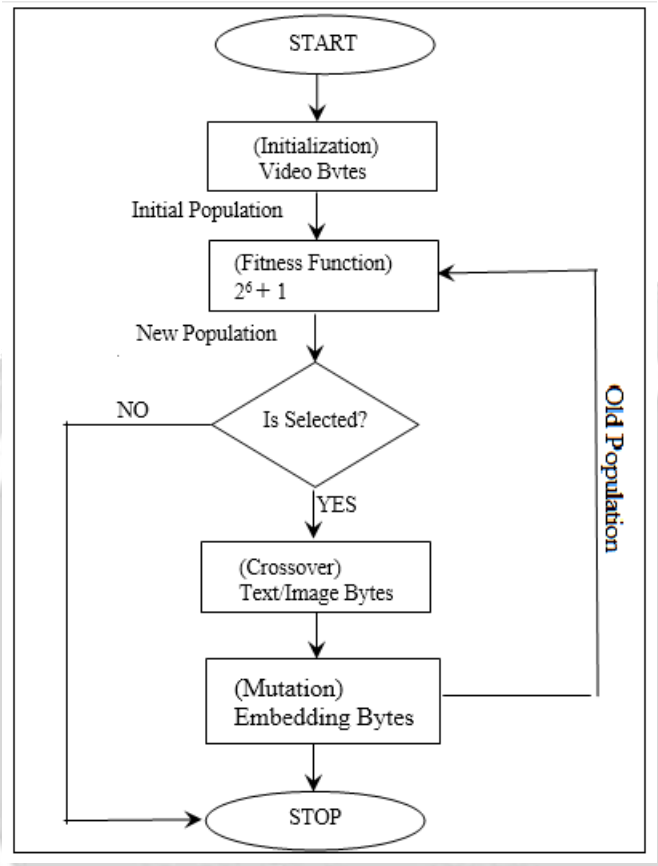

Figure 2: Flowchart for Genetic Algorithm

IV RESULTS AND DISCUSSIONS

The designed method was created using the Java programming language with the aim of performing good steganography on video data. The solution that is being given makes use of the NetBeans IDE to implement the methodology's programming and the MySQL database as an addition to handle the capabilities for handling data storage. The development machine features a typical setup with a Core i5 processor and 8 GB of RAM.

When comparing the original video to the encoded video, the Peak Signal Noise Ratio (PSNR) metric is employed to evaluate the quality of the video. The Peak Signal-to-Noise Ratio (PSNR), an indicator for evaluating the original and compressed versions of a video in terms of pixel or video component color value, is used to determine the degree of image fidelity.

The pixel color values may change during the process of reconstructing an image after steganography. Peak signal-to-noise ratio (PSNR) measurements can be used to determine how much the video quality has declined. There is a broad and dynamic range in the signals. Therefore. The PSNR values are mathematically represented using a logarithmic scale, and their measurement is done in decibels.

The Peak Signal-to-Noise Ratio (PSNR) technique, which provides an objective measure of the similarity between videos, is successfully expressed by the use of the decibel scale. A reliable measure for precisely describing the visual discrepancy between two images is the peak signal-to-noise ratio (PSNR).

In order to evaluate performance and distinguish between perceived differences in quality, the quantification of video processing techniques and strategies is of great value. By evaluating the mean square error (MSE) between two videos, the peak signal-to-noise ratio (PSNR) statistically assesses the extent to which two videos differ from one another. The squared disparities between the pixel values of two videos are averaged out to get the mean squared error (MSE), which is a measurement.

The mean Squared error (MSE) must first be computed in order to use the PSNR approach. The Peak Signal-to-Noise Ratio (PSNR) equation is then used to calculate the Mean Squared Error (MSE) value. Equations 1 and 2 provide for the mathematical description of the PSNR approach-based evaluation of the suggested methodology.

$$MSE = \frac{\sum[I_1(m,n) - I_2(m,n)]^2}{M*N} \text{ ---------- (1)}$$

Where,

I_1 = Original video.
I_2 = Steganographed video.
M = Number of bytes in the video.
N = Number of bytes in the video.

$$PSNR = 10 \log_{10} \frac{R^2}{MSE} \text{ ---------- (2)}$$

Where,
R = is the maximum fluctuation in the input video.
MSE = Mean Square Error.

The Peak Signal-to-Noise Ratio (PSNR), which is determined, is used to evaluate the effectiveness of the videos produced from the input dataset. The aforementioned videos are used to demonstrate the process in line with the categorization shown in the preceding table.

Using the aforementioned formulae, the PSNR of both the original and steganographed videos is calculated. To compare the input video with the steganographed output video produced by the methodology, the PSNR approach is used. The average PSNR figures obtained for five videos are shown in Table 1 below.

Video Number	Average PSNR
1	31.12494911
2	30.26255445
3	29.77764613
4	28.76464615
5	30.9794645

Table 1: PSNr for obtained Experiment

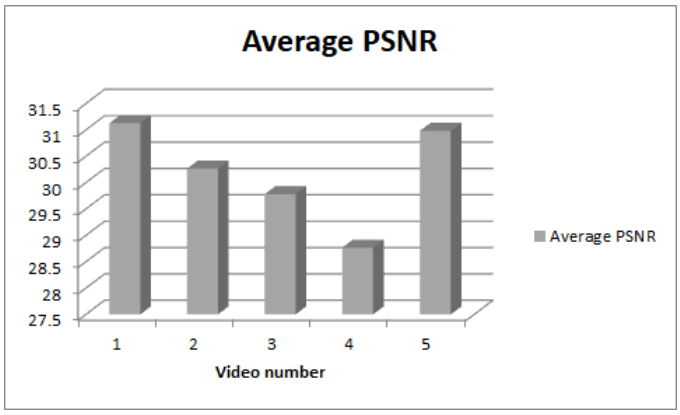

Figure 3: Average PSNR for Different Video

According to their PSNR scores, the aforementioned figure illustrates the methodology's efficacy. The Peak Signal-to-Noise Ratio (PSNR) scores show how well the offered technique performed steganographically. The high Peak Signal-to-Noise Ratio (PSNR) of 30.181 obtained shows how significantly improved the method is. In the context of steganography, a higher PSNR number denotes very little change in the final video. This demonstrates that the approach is working as expected and that the results are as expected.

V CONCLUSION AND FUTURE SCOPE

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.

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

REFERENCES

[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.

[8] Rehman, Atique & Rahim, Rafia & Nadeem, Muhammad & Hussain, Sibt. (2017). End-to-end Trained CNN Encode-Decoder Networks for Image Steganography.

[9] S. Chavan and Y. B. Gurav, "Lossless Tagged Visual Cryptography Scheme Using Bit Plane Slicing for Image Processing," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), 2018, pp. 1168-1172, DOI: 10.1109/ICIRCA.2018.8596778.

[10] Islam, Saiful & Nigam, Aditya & Mishra, Aayush & Kumar, Suraj. (2019). VStegNET: Video Steganography Network using Spatio-Temporal features and Micro-Bottleneck.

[11] Younus, Zeyad Safaa and Younus, Ghada Thanoon. "Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data" Journal of Intelligent Systems, vol. 29, no. 1, 2020, pp. 1216-1225. https://doi.org/10.1515/jisys-2018-0225

[12] Wu, Pin & Chang, Xuting & Yang, Yang & Li, Xiaoqiang. (2020). BASN—Learning Steganography with a Binary Attention Mechanism. Future Internet. 12. 43. 10.3390/fi12030043.