Secure Sharing Military Information Using Image, Audio and Video With Steganography

M.Ananthi [1], R.Bharathi[2],K. Karthika[3], N. Sasireka[4], S. Yogarni[5]

[1,2] *Assistant Professor, Department of Computer Science and Engineering, Cheran College of Engineering,Karur , Tamilnadu , India.*

[3,4,5]*U.G Student, Departmentof Computer Science and Engineering, Cheran College of Engineering,Karur , Tamilnadu , India.*

[1]*rithu.ananthi@gmail.com,* [2]*bharathimkce@gmail.com,* [3]*karthikacse6363@gmail.com,*

[4]*1605.sasireka@gmail.com,*[5]*yogarni2000krr@gmail.com.*

ABSTRACT

In the dispersed network environment, security is a crucial prerequisite for an information society. Individuals, corporations, and governments are all using various methods to safeguard their personal or military information. This method is also unusual in that the original military data may only be examined by authorised personnel who have the key to decrypt the files and extract the information buried in images, sounds, or videos. This technique used military secret data to safeguard information more effectively than previous methods.

Keywords: Security Information ,Discrete Wavelet Transform (DWT) , Least Significant Bit (LSB) , Steganography.

1. INTRODUCTION

The security of information has been one of the most essential aspects of information technology and communication since the birth of the Internet. Cryptography was presented as a mechanism for ensuring communication confidentiality, and many various methods for encrypting and decrypting data have been devised to keep the information secret. Unfortunately, it is not always enough to keep the contents of information secret; sometimes it is also required to keep the information's existence hidden. Steganography is the term for the method utilised to do this. In this paper, we offer a novel data-hiding system based on a variety of picture, audio, and video-hiding approaches and algorithms. [6]-[7].

Steganography is a kind of encrypted communication that allows for private and secure communication. It has a wide range of applications, including audio-video synchronisation, copyright management, television transmission, military use, and digital watermarking. Broadband internet connections allow for practically error-free data transfer, allowing individuals to share big multimedia files and duplicate them. Sensitive communications and information are sent over the internet in an unsecured format, yet everyone has something to keep hidden. The goal of steganography is to conceal hidden data within the cover medium while maintaining the cover medium's overall quality [8]-[10].

Actual information is not kept in its original format in steganography, but rather changed such that it may be concealed within a multimedia file, such as a picture, video, or music. The modern industries mostly want digital watermarking and audio and video steganography finger printing. We can preserve our secret data since the steganography stays intact throughout transmission and transformation. This is accomplished by converting the picture to a bit stream, which is then embedded in the changing frame. Because cybercrime is now reported so quickly, steganographic solutions must be as effective and safe as possible so that crimes may be reduced. For data and information security, cryptography and steganography should be integrated. [11]-[12].

Video steganography may be accomplished in two ways: by storing data frame by frame or by transforming frames to frequency domain and then storing the result. The first method is similar to spatial domain, whereas the second method is similar to frequency domain. Video steganography may be classed into two forms depending on the technique used for steganography: lossless and lossy steganography. Lossless steganography allows both the hidden information and the original video file to be recovered without error or alteration, while lossy steganography allows the hidden information to be retrieved properly but the original video to have flaws. [13]-[14].

Lossless steganography necessitates the storage of hidden data in a specified area and will take some time to execute the algorithm in order to locate the precise spot where hidden data may be put. As a result, the lossless technique is getting more difficult to apply in real-time applications, and this is dependent on the system requirements. Data must be stored at some LSB position or at particular pixel places in lossy steganography. This is simple to create and may be used in real-time with any standard system specs. The data is hidden using the LSB (Least Significant Bit). The index frame is the initial frame, and it comprises information such as where the information is saved, in what form it is stored, what file type it is stored in, and so on. It is quite straightforward to extract concealed information from steganography video [15] if the first frame is correctly received and the recipient recognises the information.

Because videos have a greater sample number of pixels or the number of transform domain coefficients than still images, they have more capacity and can hold more data. Also, because of their temporal aspects, videos have several qualities that are not seen in pictures, such as perceptual redundancy.

2. RELATED WORKS

Steganalysis technology is being developed using classic picture steganography. Because the hidden embedding approach affects the naturalness of the cover picture, audio, and video, it has certain security flaws. Figure 1 shows a coverless image steganography (CIS) system for selecting hidden pictures to circumvent this challenge. [1]

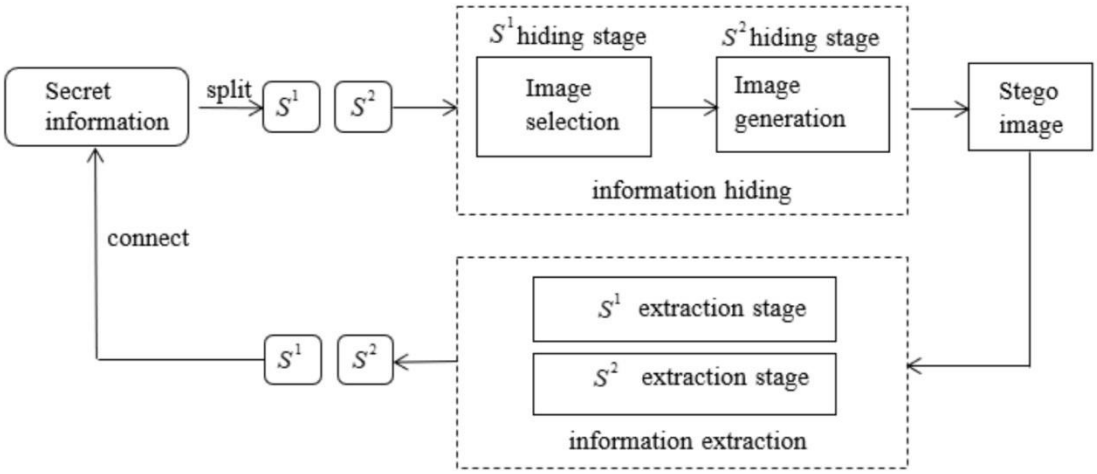


Figure.1.**The Flowchart of the Existing CIS Method.**

Steganography ensures the imperceptibility of secret messages hidden between the covers. Deep learning-based steganography, unlike classical steganography, provides an adaptable and generalised architecture that does not need knowledge in the embedding process. Most steganography algorithms, however, use photos as the cover instead than videos, which are more expressive and widely distributed. An encoder, a decoder, and a discriminator network are used to create a multi scale down-sampling feature extraction structure. Furthermore, a CU (Coding Unit) mask constructed from a VVC (Versatile Video Coding) video is first added to aid the network's learning capabilities. [2]

Steganography has gained popularity in recent decades owing to its capacity to transfer data invisibly. Steganography uses text, picture, audio, and video to hide hidden information. The quantity of hidden information drawn by video steganography is increasing. Also covered is the possibility of encryption systems. Different steganography approaches are classified as early embedding, middle embedding, and delayed embedding, depending on the time data is embedded. [3] Many video steganography algorithms based on the intra-prediction mode (IPM) have recently been developed. The majority of these algorithms are concerned with mapping rules and distortion functions. Because the steganography algorithm must first figure out how much cover is lost. This work proposes a new secure video steganography based on unique embedding algorithms to circumvent this difficulty. Video encoding is paired with video steganography. Then, during intra-prediction encoding, each qualifying block is evaluated and a one-bit message is inserted. Experiments show that our approach provides strong security while having minimal influence on video quality. [4]

To create stego video, we suggested three safe steganography methods that insert a bit stream of the secret message into the approximation coefficients of the Integer Wavelet Transform (IWT), DWT, and the LBP technique. The Mean Square Error (MSE) and PSNR are used to calculate the geometric difference between the cover and stego videos. The new findings reveal that the suggested algorithms may conceal a secret message with a large payload capacity while maintaining a high degree of security and invisibility. [5]

Hybridization of DWT with LSB is employed to determine the optimal bits from the cover movie for inserting the secret data in this study for picture decomposition. This research proposes an end-to-end deep learning network for audio and video steganography to achieve this goal. Artificial intelligence is employed to incorporate the secret data for the development of optimal pixels, and an artificial neural network is used as a classifier to categorise the appropriate areas in the cover data. When compared to previous work, the suggested study has demonstrated to be superior. [6]

3. PROPOSED WORK

The proposed work would use Discrete Wavelet Transform (DWT) compression, Least Significant Bit (LSB) replacement, and AES to hide information in certain frames of the. Because of the enormous size and memory requirements, the suggested technique employs picture, audio, and video based steganography. The text may be hidden in three different ways: picture, audio, and video steganography. Large audio files will be supported by the proposed technology. When uploading huge audio recordings, they will be divided into many parts and hidden in separate cover files. Frames are created from the video. Every 0.05 seconds, frames are divided. The frames are then compressed using the DWT Haar compression method. Select the frame that will be used to conceal the audio data. The audio data is then hidden in the specified frame using the LSB insertion method. The frames are decompressed using inverse DWT compression after data embedding. To create the steganographed video, the frames are reassembled. This video will be identical to the original. However, there will be little modifications. Human eyes are unable to detect this. This will be delivered to the recipient. The receiver may extract several sections of an audio file and combine them into a single audio file. The video will be divided into frames and compressed using DWT compression by the receiver. Each pixel in the steganographed frame will now have its LSB extracted. Gather all of the parts and turn each one into a character. This will separate the concealed audio data from the actual video. The suggested strategy is put into practise in real time, and the performance indicators are assessed. Figure 2 shows an architectural diagram.

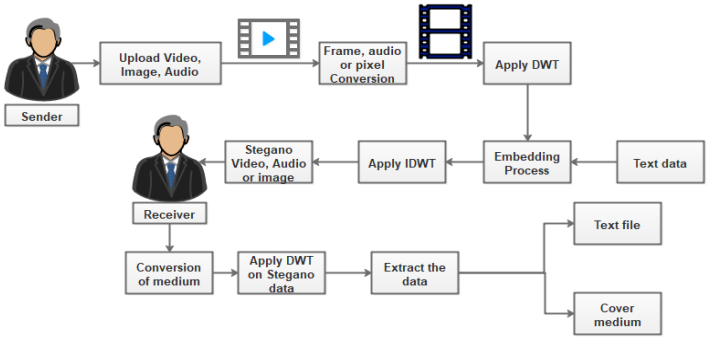


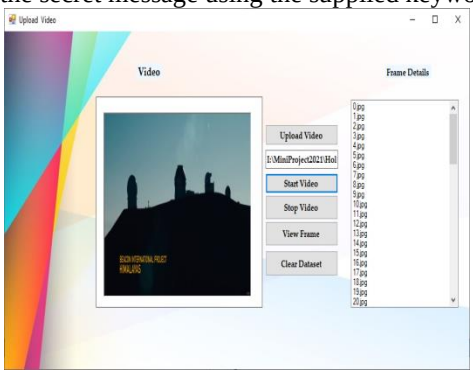
Figure.2. Architecture Diagram

ADVANTAGES

- DWT mechanism assures complete security of the secret image, video and audio.
- LSB achieves high embedding capacity compared with other data hiding techniques.
- Computational complexity is low.

4. RESULT AND DISCUSSION

1. Select the video file and frame to conceal the secret messages, then produce the secret keyword as shown in Figure 3.
2. The receiver gets the video containing the secret message and opens it with the appropriate software, then unhide the secret message using the supplied keyword (see fig. 4).



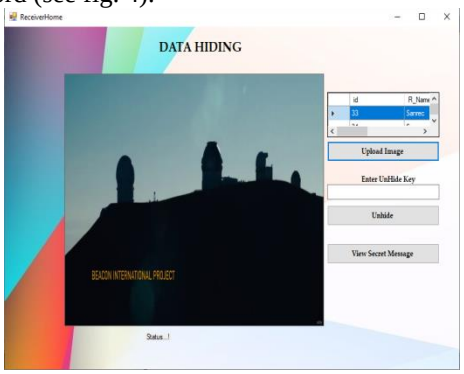


Figure.3. Sender **Figure.4. Receiver**

5. CONCLUSION

To conceal data in picture, audio, or video format, a variety of steganography methods are available. DWT Haar compression and LSB substitution are employed in our method. A large audio file has been divided into many sections. The data is hidden using a special key. That exact key is also used to store data as a frame backdrop. Once the recipient has received the stegno video, combine the shares. The method described above is used to conceal data inside a picture, audio, or video file, resulting in a reliable and secure method of data transport. The suggested embedded video steganography provides a number of benefits, including ease of use, a simple and effective technique for embedding hidden messages, and increased security.

REFERENCES

[1] Xianyi Chen, Zhentian Zhang, AnqiQiu, Zhihua Xia And Neal N. Xiong.“ A novel coverless steganography method based on image selection and StarGAN” . VOL:9, NO:1, JAN-FEB. 1 2022

[2] Huanhuan Chai, Zhohong Li, Fan Li and Zhenzhen Zhang.“ An End-to-End Video Steganography Network Based on a Coding Unit Mask”. 5 APR 2022

[3] Dr. ManjulaG.R ,Sushma R.B . “Video steganography: A Survey of techniques and methodologies” (2021)

[4] Mingyuan Cao, LihuaTian and Chen Li, “A Secure Video Steganography Based on the Intra-Prediction Mode (IPM)”. 14 SEP 2020

[5] DhandapaniSamiappan, PR. Buvaneswari. “Video Steganography using IWT, DWT, LSB Methods and its Research”. VOL:8, SEP 2019

[6] KiranjeetKaur, BaldipKaur. “DWT-LSB Approach for Video Steganography using Artificial Neural Network” . VOL:5JULb 2018

[7] Weiming Zhang, Hui Wang, DongdongHou, and Nenghai Yu. Reversible data hiding in encrypted images by reversible image transformation. *IEEE Transactions on multimedia*, 18(8):1469–1479, 2016.

[8] PauloViniciusKoerich Borges, Joceli Mayer, and EbroulIzquierdo. Robust and transparent color modulation for text data hiding.*IEEE Transactions on Multimedia*, 10(8):1479–1489, 2008.

[9] YousofErfani, RaminPichevar, and Jean Rouat. Audio watermarking using spikegram and a two-dictionary approach.*IEEE transactions on information forensics and security*, 12(4):840–852, 2016.

[10] Thomas Stutz, FlorentAutrusseau, and Andreas Uhl.Non-blind¨ structure-preserving substitution watermarking of h. 264/cavlc inter-frames.*IEEE Transactions on Multimedia*, 16(5):1337–1349, 2014.

[11] Shan-Chun Liu and Wen-Hsiang Tsai. Line-based cubism-like image—a new type of art image and its application to lossless data hiding.*IEEE Transactions on Information Forensics and Security*, 7(5):1448–1458, 2012.

[12] XintaoDuan and Haoxian Song. Coverless information hiding based on generative model.*arXiv preprint arXiv:1802.03528*, 2018.

[13] Donghui Hu, Liang Wang, Wenjie Jiang, ShuliZheng, and Bin Li. A novel image steganography method via deep convolutional generative adversarial networks.*IEEE Access*, 6:38303–38314, 2018.

[14] Zhili Zhou, Huiyu Sun, RohanHarit, Xianyi Chen, and Xingming Sun. Coverless image steganography without embedding. In *International Conference on Cloud Computing and Security*, pages 123– 132.Springer, 2015.

[15] Prabira Kumar Sethy, Kamal Pradhan, SantiKumariBehera, "A Security Enhanced Approach for Video Steganography using K-Means Clustering and Direct Mapping", ICACDOT, 2016, pp: 618 - 622.

[16] R.Bharathi, T.Abirami,” Energy efficient compressive sensing with predictive model for IoT based medical data transmission”, Journal of Ambient Intelligence and Humanized Computing, November 2020, https://doi.org/10.1007/s12652-020-02670-z

[17] R.Bharathi, T.Abirami,” Energy Efficient Clustering with Disease Diagnosis Model for IoT based Sustainable Healthcare Systems”, Sustainable Computing: Informatics and Systems, 23 September 2020, https://doi.org/10.1016/j.suscom.2020.100453