Steganography Mechanism for Image Data Hide In Video with Data Encryption

Kiruthika E, Mr.M.Kamalanathan,M.E.,
PG student, Assistant Professor M.E-VLSI DESIGN,
Gnanamani College of Technology, Namakkal,
Tamil Nadu, India

ABSTRACT–Because of its growing popularity, digital media has given rise to significant security-related problems. These days, security breaches take many different forms, but often involve eavesdropping, disguising themselves as someone else, and manipulating. One of the newest methods for ensuring security is data hiding, which involves modifying certain unnecessary parts of the host or cover file in order to conceal sensitive information from view within multimedia contents. In data communication, data security is crucial. Since a lot of information is shared online every day between users, there is a greater chance that data will be stolen. An answer to the problem of information security during data transmission is steganography. Bits can be embedded into R's LSB sections to conceal data.G and B color spaces, as well as the method of SVD in divided DWT submatrices. This method can be applied to picture video steganography and is comparable to the sparse representation method. In general, data embedding can be carried out directly onto the data, after the media has been broken down, or by converting them. Data security may be at risk even though there are many different types of data embedding techniques available. This is because these techniques are susceptible to assaults.

Keywords: Convolutional neural networks, Hiding Data, Image Stego, Steganography, Video Stego

I. INTRODUCTION

The internet and digital media are becoming more and more commonplace these days. As a result, the need for secure data transfer has grown. This is the reason that many beneficial strategies have been put out and are currently in use. In this project, secure data transfer via the internet between the sender and the recipient is accomplished through the use of steganography. The technique of covertly inserting data into a data source without affecting its perceptual quality is known as steganography.The Greek words steganos, which literally means "covered," and graphia, which means "writing," are the sources of the word steganography, which refers to covered writing. Steganography is most frequently used to conceal a file inside another file. When data is hidden, it usually means that the original format of the information is no longer maintained. The format is changed to a substitute that is equivalent.multimedia files, such as pictures, movies, or photos. This is concealed within still another item. A method for hiding any type of file inside a carrying video file is called video steganography. Because of its size and memory needs, the usage of video-based steganography may be more appropriate than that of other multimedia files. One key method for embedding information in a carrier file is the least significant bit (LSB) insertion. The information bit is hidden using the least significant bit (LSB) insertion technique, which works on the media file's LSB bit. In this project, a data concealing system using RDH techniques will be created to conceal information in particular video frames and locations by substituting LSBs.

II. LITERATURE SURVEY

2.1 Steganographic Approach for Data Hiding using LSB Techniques The art and science of composing secret messages so that only the intended receiver is aware of their presence is known as steganography. Bits of unneeded or worthless data are replaced in order for steganography to function. This concealed data may take the shape of graphics, cipher text, or plain text. Sometimes, when encryption is prohibited, steganography is utilized. Alternatively, and this is more typical, steganography is added to encryption. Even if the encrypted file is decrypted, the concealed message will remain hidden since steganography allows an encrypted file to conceal information. Using steganography, the goal is to conceal a secret message in a cover material so that others are unable to identify its existence. To put it simply, steganography technically refers to concealing a piece of information inside another. Steganography makes use of the ability to conceal data at both the network packet and digital multimedia file levels. Steganography, which means "covered writing," originated in ancient Greece. There, common methods included tattooing a messenger's head after he had shaved it, allowing it to grow back, and then shaving it again when he reached his contact point. A Steganography communication will typically look like another message, such as the cover text, an image, an article, or a shopping list. Traditionally, it might be concealed by writing on garments or by smearing invisible ink in between the lines of seemingly innocent documents. In order to conceal data, one of three three things: the capacity to add a sequence that contains the data, change an already-existing, harmless sequence, or identify redundant information in an already-existing sequence and use it to conceal data. Because individuals frequently send digital pictures via email and other Internet communication, modern steganographic systems use multimedia artifacts like images, videos, etc., as

cover media. In the contemporary technique, there are five different types of steganography based on the type of cover object.

2.2 Frame Selected Approach for Hiding Data within MPEG Video Using Bit Plane Complexity Segmentation- This paper introduces a novel approach to highly secure video steganography. This method's basic idea is to use the digital video as individual frames and choose which frames to conceal the content within. Since the experiment's findings demonstrate that the hidden data within the chosen frame is successful, take data from the order of the frames, these features work without degrading the video's quality. This framework invites the largest size cover file among multimedia files, which is the video, to circumvent the steganography approach's limitation. With video steganography, we can choose to encrypt specific frames to increase system security or to encrypt the entire video to conceal a significant quantity of data. Owing to security concerns, the author chose one frame from among all the frames in the buffer; this decision was made to ensure data protection. The author likes to show the outcome on the digital device's frame because it is more difficult to portray the result as a video stream on paper.video file with each frame's histogram included. Here, we can observe that, particularly when considering the human visual system, there are not many distinctions between the two sets of frames. This indicates that the technique can be successfully applied to video frames. It may also be used to observe divergences on the frames before and after data is hidden, and to validate the process using the histogram. The histogram for each single frame shows that there are no variations between the two sets of data before and after the data was hidden, indicating that the algorithm was successful in hiding the data inside the frames without impairing the ability of the human visual system to detect it.

2.3 Video Data Hiding Through LSB Substitution Technique- These days, hacking activities are increasing daily, and hackers can simply steal crucial data and Security alone won't keep hackers at bay. Although the level of security has increased, the main disadvantage of the new security status is that it has become quite expensive. Therefore, we need more affordable, high-security options that are also better. When sensitive or vital information is provided in a regular manner, there is a potential that it could be misused. The method by which the data in the BMP image files is concealed. Current transactions are regarded as "un-trusted" because to their low security, meaning that hackers can easily compromise them. Additionally, we must take into account that sending a lot of data over the network wouldmistakes made throughout the transfer. The systems that are currently in use only have one level of security. As we discussed in the problem domain, the current security methods are insufficient to stop hacking, and the new methods are quite expensive. Then, a different, more effective method that offers a higher level of security is required. Through the use of image masking, we are decreasing the amount of hacking activity carried out by hackers. Image video interleave, or AVI, is what we produce. Even though the AVI videos are huge, they can be securely processed using Data Hiding and Extraction procedures and converted into twenty equal grayscale photos before being sent over a network from the source to the destination. grayscale pictureuse 8 bits per pixel, allowing it to display 256 distinct colors or shades of gray. We create text information for sets 1, 2, and 3, each of which has 20 bmp data images. We then apply one, two, or three LSB replacements to each set. The final steps encrypt the AVI video before sending it by the sender. Decryption is applied at the receiver end.

III. EXISTING SYSTEM

Phases of data extraction/image recovery, data embedding, and image encryption comprise the current approach. A separable reversible data concealing in an encrypted image is used in this study. According to the suggested plan, a data-hiding key is used to embed the extra data into the encrypted image after the original image has been encrypted using an encryption key. Even though the recipient is unaware of the contents of the encrypted image, he can still extract the additional data from it if he just possesses the data-hiding key. With just the encryption key, the recipient can decrypt the data and create an image that resembles the original, but he won't be able to retrieve the extra data that is embedded. Using an encryption key, the content owner encodes the original uncompressed image to create an encrypted picture. Then, using a data-hiding key, the data hider compresses the encrypted image's least significant bits (LSB) to produce a sparse space that can hold the extra data. According to the data-hiding key, the data contained in the produced space can be readily retrieved at the recipient side from the encrypted image including additional data. An image that is identical to the original can be obtained by decrypting it using the encryption key because the data embedding only alters the LSB.

Drawbacks:

- Tough to manage massive data hiding in pictures
- The current mechanism makes it hard to hide data reversibly depending on videos.
- Increase the number of hidden LSB panels.

IV.PROPOSED SYSTEM:

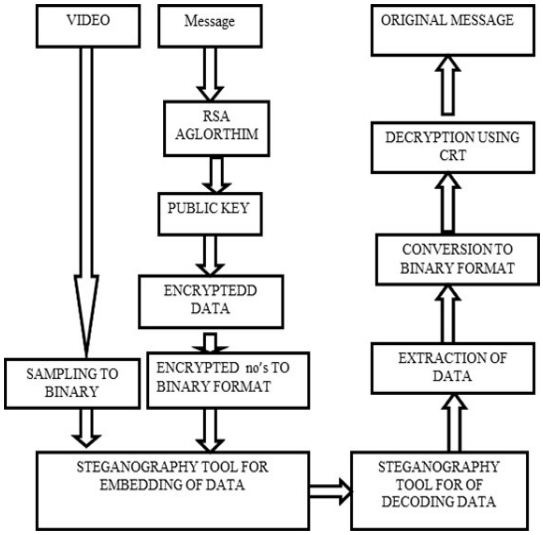
Modern transactions are regarded as "un-trusted" in terms of security, meaning that hackers can easily exploit them. We also need to take into account that sending a lot of data over a network will always result in transfer failures. The systems that are currently in use only have one level of security. Another issue with the current

system is that hacking activity is increasing daily, making it easy for hackers to obtain sensitive data, and security measures alone are insufficient to prevent hacking. Although the level of security has increased, the main disadvantage of the new security status is that it has become quite expensive. Therefore, we need more affordable, high-security options that are also better. The intended system will offer an effective and safe technique for video steganography. Image video interleave, or AVI, is what we produce. Even though AVI videos are big, they can be safely transferred over a network from the source to the destination by processing the source video using these Data Hiding and Extraction procedures. The suggested technique generates an index for the confidential data, which is then embedded into a video frame. This index helps locate the frames that contain the hidden data. Because of this, during the extraction procedure, the receiving end's index is used to evaluate the frames that contain the secret data rather than the complete movie. When information is steganographed using this technique, the likelihood that an attacker is smaller than with the conventional approach of sequentially hiding information frame by frame. It also shortens the extraction process's computational duration.

Advantages:

- A reduction in the MSE (mean square error)
- The PSNR, or peak signal to noise ratio, is the ratio of the stego frame to the equivalent cover frame. Its value indicates that the frame is transferred without distortion or loss.

4.1 System architecture



V.MODULES

- Video and image acquisition
- Double Coding Mechanism
- Embedding the data
- Extraction of the data
- Evaluation criteria

5.1Modules description

5.1.1 Video and image acquisition:

The purpose of the steganography process is to conceal messages within cover messages so that only the intended recipient is aware that they are there. Host message or cover message is the term for the message that is used to conceal hidden message. The modified message is referred to as a stegano message once it has been altered from the host message or cover message. The user has the option to upload both the cover video and the picture that is hidden within it in this module. After that, video is converted to an image as a signal format, frame decomposition, and pixel format. Any kind of image or video can be uploaded.

5.1.2 Double Coding Mechanism:

This project uses a double coding process, wherein morse codes are generated after pseudo random codes generated by a linear feedback shift register (LFSR) are utilized. Data security will increase with this method. One noteworthy aspect of Morse code is that each code has a different or unique unpredictability. The distinctive feature adds even more significance to the steganographic process; there is no particular method for creating such codes. Morse code is a method of transmitting text data that appears as an on-off sound tone and a sequence of lights that can be received and decoded to provide data. The "Dots" and "Dashes" sequence are known as Morse codes. There are Morse codes for prosigns, digits, and alphabets.

5.1.3 Embedding the data:

Choose the values for the detailed and approximation coefficients in this module. Next, conceal the image within the second plane's approximation coefficients. We call this procedure "image encryption." Using this model, we will Utilize the double coding method to transform the image and offer a high level of protection. And once an image is ready to be sent, this info is saved in it. The shares are recovered and stacked together to restore the original image on the receiving end. Next, use the inverse method to obtain the stegano video. After that, the Stegano video is transformed to RGB and YUV formats.

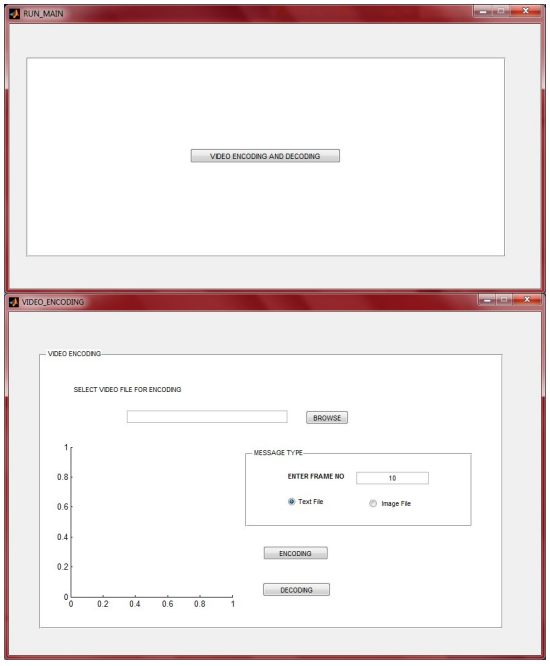
5.1.4 Extraction of data:

This module extracts original images and videos in a more efficient way. The stego video may be read, converted to YUV and RGB format, and its inverse sub bands can be obtained. After that, decode the Stego movie to obtain the encrypted image. To obtain the original image, use decryption. We can obtain the image's binary values.to translate into values in decimal. Finally, cover video and picture are extracted using the inverse lifting wavelet transform.

5.1.5 Evaluation criteria:

In this module, we use Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) to assess the system's performance. Squared Pearson Correlation Coefficient (SPCC) and Signal to Noise Ratio (SNR) are used to quantify the quality of the derived secret picture signal.

VI.SCREEN SHOT



VII.CONCLUSION

The suggested data concealing method offers strong security and efficiency. Due to the twofold coding strategy used in this method, the steganography becomes resilient and the hidden data will be difficult to identify. The transform domain approach makes the stego video less susceptible to the effects of compression methods. Although it is commonly known that compression eliminates superfluous information from media, the suggested approach protects a sizable amount of concealed data from these kinds of attacks.Our proposed systems use the clustering modification methods approach to incorporate picture in image.When the secret media image is taken out of the video, it will not precisely match the embedded image that was there in the first place. Compression algorithms, rounding, and other processing stages can distort the media.To obtain an almost identical image, processing of the image data will be required. Thus, there are several uses for this approach in the advancement of science and technology.

REFERENCES

[1] Aniruddha, K., & Chandramore, K. (2014). Automatic toll collection system using RFID. International Journal of Electrical and Electronics Research, 2(2), 67-72.

[2] Bröring, A., Remke, A., & Lasnia, D. (2011, December). Sense Box–a generic sensor platform for the web of things. In International Conference on Mobile and Ubiquitous Systems: Computing, Networking, andServices(pp. 186-196). Springer, Berlin, Heidelberg.

[3] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[4] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.
[5] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
[6] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
[7] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.
[8] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.
[9] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756
[10] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749
[11] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
[12] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
[13] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019
[14] Buch, N., Velastin, S. A., & Orwell, J. (2011). A review of computer vision techniques for the analysis of urban traffic. IEEE Transactions on Intelligent Transportation Systems, 12(3), 920-939.
[15] Kelemen, M., Virgala, I., Kelemenová, T., Miková, L'.,Frankovský, P., Lipták, T., & Lörinc, M. (2015). Distance measurement via using of ultrasonic sensor. Journal of Automation and Control, 3(3), 71-74.
[16] Kianpisheh, A., Mustaffa, N., Limtrairut, P., & Keikhosrokiani, P. (2012). Smart parking system (SPS) architecture using ultrasonic detector. International Journal of Software Engineering and Its Applications, 6(3), 51-58.
[17] Liu, J., Han, J., Lv, H., & Li, B. (2015). An ultrasonic sensor system based on a two-dimensional state method for highway vehicle violation detection applications. Sensors, 15(4), 9000-9021.