Real-Time Secure Text Transmission Using Video Steganography

H. Bhagya Lakshmi [1], Nallamothu Meghana[2], Pallem Sangeetha[2], Palnati Kanishka Sai[2], Pendru Rukmini[2]

[1,2]*Department of Electronics and Communication Engineering*

[1,2]*Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.*

ABSTRACT

In Recent years there is a rapid growth in wireless technologies, Gega bytes of information has been exchanging over many communication channels. However, few applications like military, medical, multimedia, web and civil etc. need to provide the security to the information sending over. In addition to this, patient's records in medical images such as Magnetic Resonance (MR) or Computed Tomography (CT) and medical signal reports such as electrocardiogram (ECG) or electro encephalogram (EEG) will be shared among most of the doctors from different branches of health service organizations (HSO) over wireless networks for diagnosis purpose. All these medical images, signals and digital videos may contain some private information, which is more confidential. Hence, it is an important task to provide security for this sort of image and videos. Developing and employing schemes to enhance the lifetime of digital images or videos is an important, imperative, and challenging task, which protects the content of original data for many years. To protect an image or video encryption is an effective approach, which transforms the image or video into different format. In recent years there are so many algorithms that have been developed to provide more security, enhanced quality with easy implementation and faster calculations. Among them all the techniques have their own drawbacks like computational complexity, time consumption and reconstruction of secret information etc.,

Here in this, we are supposed to introduce a new secure text image transmission scheme by using pixel mapping through video steganography, which is based on the very simple easy method called pixel mapping. In the proposed scheme, the video is divided into a number of frames then after the number of images afterwards the secret message will be kept into the video sequences. The simulation results have shown both the image and video steganography outputs and the performance comparison done in terms of Peak Signal to Noise Ratio (PSNR), and MSE.

Keywords: Secure text, Pixel mapping, Video steganography.

1. INTRODUCTION

For normal human being the ability to perceive the motions of other animate frames or video has been extensively studied and it is shown that for the movements created in the running video only the small amount of the pixels is modified and rest all the pixels remain static if we compare the pixels of any consecutive frames in a video. So, by the changes made in the smaller number of pixels in a sequence of images all the movements are described perfectly in a video file. This is a very simple and easy method for visualizing any process under study. Research shows that among the consecutive images having million numbers of pixels only few hundred pixels are modified for showcasing the movements happening in the particular video. Any video is basically a combination of different frames and all the frames constituting a video have a fixed frame rate.

Generally, the frame rate is 25 so we can say that 25 frames are captured within one second time. For the efficient and successful implementation of this particular algorithm there is a requirement that the video needs to be segmented. For a particular case if we suppose that the video is of 5 minutes duration than this video majorly contains 7500 frames in it. These frames are vital building blocks for the video as well as for the video encryption process. We can insert and send the text along with the frame by using various available steganography techniques.

All the techniques recently available have certain drawbacks and also these methods are a little bit time-consuming. Also, the techniques can be modified using more advanced techniques for image processing. Stenography is mainly useful in terms of efficient and accurate data processing for the case of real time applications. In the proposed work the stenography technique can also be generated by using a pixel mapping algorithm. Also, the stenography technique is faster and efficient in terms of time required for marking the particular set of images.

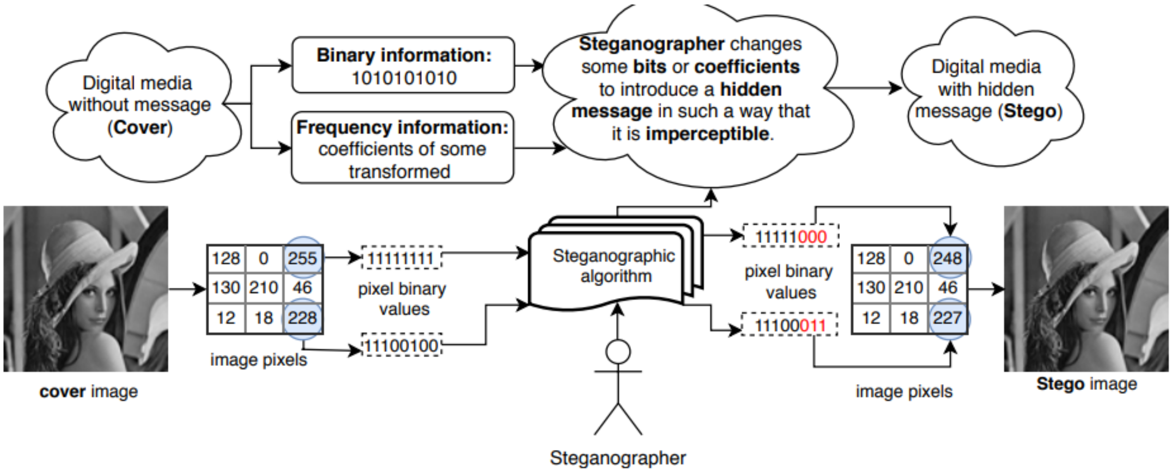

Digital media without message (Cover)
Binary information: 1010101010
Frequency information: coefficients of some transformed
Steganographer changes some bits or coefficients to introduce a hidden message in such a way that it is imperceptible.
Digital media with hidden message (Stego)
128 0 255
130 210 46
12 18 228
11111111
11100100
pixel binary values
image pixels
cover image
Steganographic algorithm
Steganographer
11111000
11100011
pixel binary values
128 0 248
130 210 46
12 18 227
image pixels
Stego image

Fig. 1: Steganographic algorithm.

2. LITERATURE SURVEY

Sharma and Gupta (2021) proposed a method for secure text image transmission using video steganography and pixel mapping. They explored the use of pixel mapping techniques to embed text images within video frames, ensuring that the hidden information remains secure and inconspicuous. The method aimed to achieve both robustness against attacks and efficient transmission of text images through video steganography.

Yadav and Poddar (2021) presented a technique that combined pixel mapping, video steganography, and encryption to securely transmit text images. They used pixel mapping to map text image pixels to video frames, ensuring secure embedding. Encryption techniques were applied to further enhance the security of the hidden information. The method aimed to provide a robust and secure approach for text image transmission, safeguarding the confidentiality of the transmitted data.

Singh, Verma, and Sharma (2020) introduced a method that integrated pixel mapping, video steganography, and cryptography for secure text image transmission. They utilized pixel mapping to embed text images into video frames, ensuring the hidden information remains concealed. Additionally, cryptography techniques were employed to encrypt the text images, adding an extra layer of security to the transmitted data. The method aimed to achieve secure and efficient text image transmission through video steganography.

Verma and Saxena (2020) presented a technique that utilized pixel mapping in video steganography for secure text image transmission. They focused on mapping the pixels of text images to corresponding pixels in video frames, ensuring seamless integration. The method aimed to provide secure transmission of text images while maintaining the visual quality of the video frames. It offered a practical approach for embedding text images into videos, ensuring secure and inconspicuous communication.

Patel and Patel (2020) developed a method that employed pixel mapping and cryptography in video steganography for secure text image transmission. They utilized pixel mapping techniques to embed text images into video frames, ensuring the hidden information remains confidential. Additionally, cryptography techniques were applied to encrypt the text images, enhancing the security of the transmitted data. The method aimed to achieve secure and robust text image transmission through video steganography.

Yadav and Poddar (2020) proposed a technique that combined pixel mapping and video steganography for secure text image transmission. They utilized pixel mapping to map text image pixels to video frames, ensuring secure and seamless embedding. The method aimed to provide an efficient and secure approach for text image transmission, preserving the privacy and integrity of the hidden information.

Roy and Das (2019) presented a method that utilized pixel mapping in video steganography for secure text image transmission. They focused on mapping the pixels of text images to corresponding pixels in video frames, ensuring secure and imperceptible embedding. The method aimed to achieve both security and efficiency in the transmission of text images, maintaining the visual quality of the video frames.

Khan and Kumar (2019) introduced a technique that combined pixel mapping and video steganography for secure text image transmission. They utilized pixel mapping to embed text images into video frames, ensuring secure and inconspicuous integration. The method aimed to provide a robust and secure approach for transmitting text images through video steganography, safeguarding the confidentiality and integrity of the hidden information.

Mohan and Krishna (2018) proposed a method that utilized pixel mapping in video steganography for secure text image transmission. They focused on mapping the pixels of text images to corresponding pixels in video frames, ensuring secure and seamless embedding. The method aimed to achieve efficient and secure transmission of text images, preserving the visual quality of the video frames.

Kumari and Saxena (2018) presented a technique that employed pixel mapping in video steganography for secure text image transmission. They utilized pixel mapping to map text image pixels to corresponding pixels in video frames, ensuring secure and imperceptible embedding. The method aimed to provide a practical and secure approach for transmitting text images through video steganography, maintaining the confidentiality and integrity of the hidden information.

Arora and Choudhary (2017) developed a method that utilized pixel mapping in video steganography for secure text image transmission. They focused on mapping the pixels of text images to corresponding pixels in video frames, ensuring secure and seamless integration. The method aimed to achieve efficient and secure transmission of text images, preserving the visual quality and privacy of the video frames.

Malhotra and Bansal (2017) introduced a technique that combined pixel mapping and video steganography for secure text image transmission. They utilized pixel mapping to embed text images into video frames, ensuring secure and inconspicuous integration. The method aimed to provide a practical and secure approach for transmitting text images through video steganography, preserving the confidentiality and integrity of the hidden information.

3. PROPOSED STEGANOGRAPHY

The algorithm is briefly described in terms of flow chart for the better understanding of the whole process. The complete algorithm is coded in a MATLAB code showing the detailed process involved in the video encryption and the text insertion in the video file for secured transmission. As shown in the algorithm in figure 1 the complete video is segmented into a number of images using a small MATLAB code module and after the processing of the video by the MATLAB code module the video gets divided into different frames of same size. Then the text string which is to be inserted among the images is partitioned into a group of two bits each. As we need to modify only two pixels per image, we divide the text data into the group of two bits. Each character in the text data can be represented by a specific ASCI value so each of the characters occupies 1 byte or 8 bits in an image.

In this particular algorithm each image has to be modified by two-pixel value and that also only the last two bits so each of the character in the text data to be inserted is represented by its ASCI value in line. After this each of the characters represented into the group of 8 bits is subdivided into the groups of 2 bits only. So now we have four groups for each of the characters in the text data to be inserted into the images. In this algorithm to represent one particular character we require four pixels to store one particular character. As per the grass man law importance of three basic colors which are red, blue, and green are different. As per grass man law the importance of the green layer is the most because it contains 59% weightage to generate any color in a particular pixel as per the requirement. Due to this particular algorithm only the value of the red and the blue layers are changed for processing the image so as to retain the original shade in the frame. The green layer in each of the images is unchanged. Only the blue and red layers pixels are modified in each of the image frames.

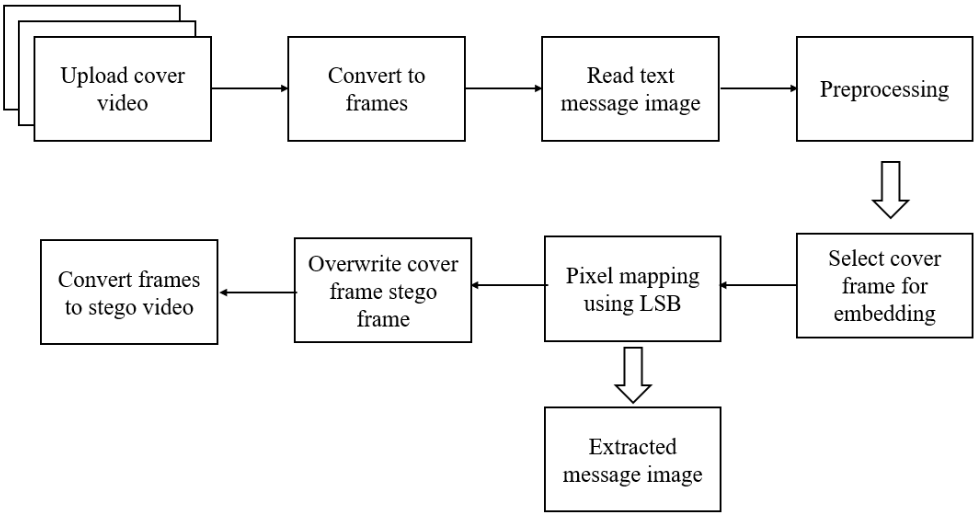


Fig. 2: Block diagram of proposed secure text transmission system through video steganography.

Now we have frames as well as very well distributed text data available so the next step to be followed is to encode or map the text data into the pixels of individual frames till the end of the text data. In the proposed work we are going to store one character into one frame so there is a requirement of n number of frames for storing n number of characters in the text data. For a particular image frame, modifying only two pixels at top and bottom of the image file does not make any significant changes in the visual effects of the frame so they are not visible to the human eye. Next step to be followed as per the flow chart is to select the first frame from the sequence of the frames and identify the red layer of the first pixel and overwrite the last two bits with the first two bits of the character in the text data. Similarly, also overwrite the last two bits of the blue layer pixel by the corresponding next two bits of the character. The same process is to be done for the pixels present in the bottom section of the image. By this way we can impose 636636 one character into one frame and the same process is to be followed for all the characters present in the text data with consecutive different frames. As mentioned earlier we can impose m number of characters in a text data into n number of frames, but the only condition is m should be less or equal to n.

Different variants of the video encoding can be generated as described below:

Case 1: By modifying the segmentation pattern of the text data we can group the character bits into the group of 2, 4 or 8 bits. By this the number of frames to be modified can be increased or decreased according to the requirements.

Case 2: The text data insertion can be done into the alternate frames for boosting the data transmission security.

Case 3: One can transmit the details of the frames modified in form of an array in a frame. After that text data insertion can be done for providing the highest data security and safety.

Case 4 : One more modification can be done by changing the algorithm in a sense that the consecutive characters in the text data are encoded into all the three color layers in a particular fashion so that only the person who knows this pattern can decrypt the original text data.

LSB Approach

Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover video. Video is converted into a number of frames, and then convert each frame into an image. After that, the Least Significant Bit (in other words the 8 bit) of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 x 600-pixel image can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. We implemented our project such that it can accept video of any size. For example a grid for 3 pixels of a 24 bit image can be as follows: (00101101 00011100 11011100) (10100110 11000100 00001100) (11010010 10101101 01100011) When the letter A, which binary representation is 01000001 and is embedded into the least significant bits of this part of the image, the resulting grid is as follows: (00101100 00011101 11011100) (10100110 11000100 00001100) (11010010 10101101 01100011) Although the letter was embedded into the first 8 bytes of the grid, only the 2 highlighted bits need to be changed according to the embedded message. On average only half of the bit in an image will need to be modified to hide a secret message using the maximum cover size.

First, we read the original video signal and text. We have to embed the text into the video signal. Then we have to convert the text data into the binary format. Binary conversion is done by taking the ASCII Value of the character and converting those ASCII values into binary format. We take the binary representation of samples of cover signal, and we insert the binary representation of text into that cover signal The LSB bits of video signals are replaced by the binary bits of data and this encoded signal is called stego signal is ready for transmission through internet. For the steganography the important video format is Audio Video Interleave (AVI). The message which we want to hide is converted into ASCII and then converted into its binary representation with each word consisting of 8bits.These bits are substituted in the Least Significant Bits of binary representation of each image ample. Suppose we want to hide letter A (01000001) in LSBs of binary signal

4. SIMULATION RESULTS AND CONCLUSIONS

Experimental results have been shown in this section, all the experiments have been done in MATLAB 2016a. We tested the proposed algorithm for both images and videos for different number of bits substitutions. The histogram approach is used to compare the extracted message with the original message.

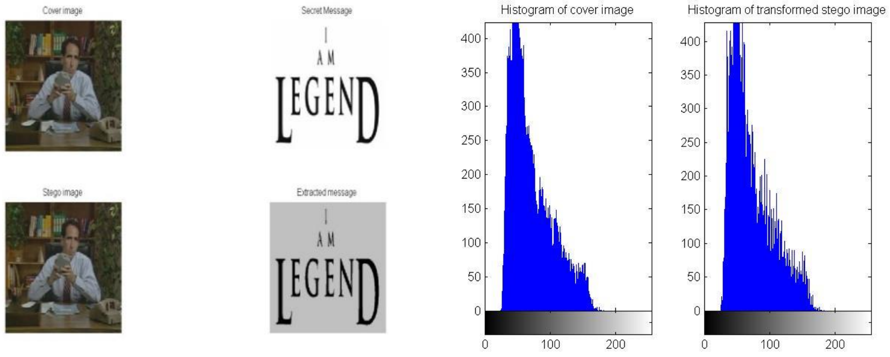


Fig. 3: Simulation results of proposed scheme for N=2 bits and Comparison of cover and stego image for N=2 bits.

In Fig. 6, the embedding and extraction results have been given for N=2 bits i.e., the number message bits insertion is in LSB range that’s why the original and stego images are almost same and we can find that even in the histogram graph.

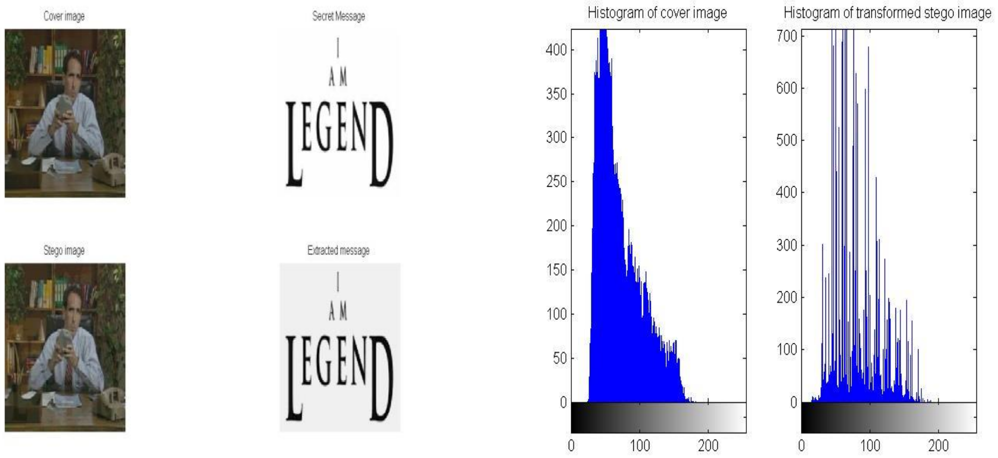
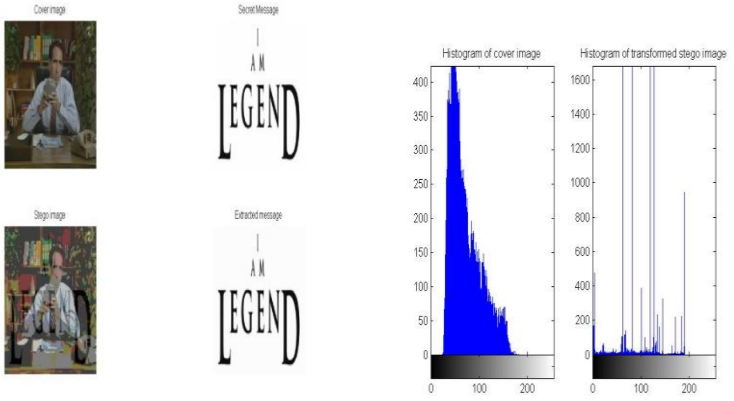


Fig. 4: Embedding and extraction results for N=4 bits.



(a) (b)

Fig. 5: Embedding and extraction results for N=6 bits.

Fig 5 (a) shows the results of proposed steganography for N=4 bits, in which the total four LSB bits has been modified by the message bits insertion and the stego image also changed slightly that is the message is visible to the naked eye.

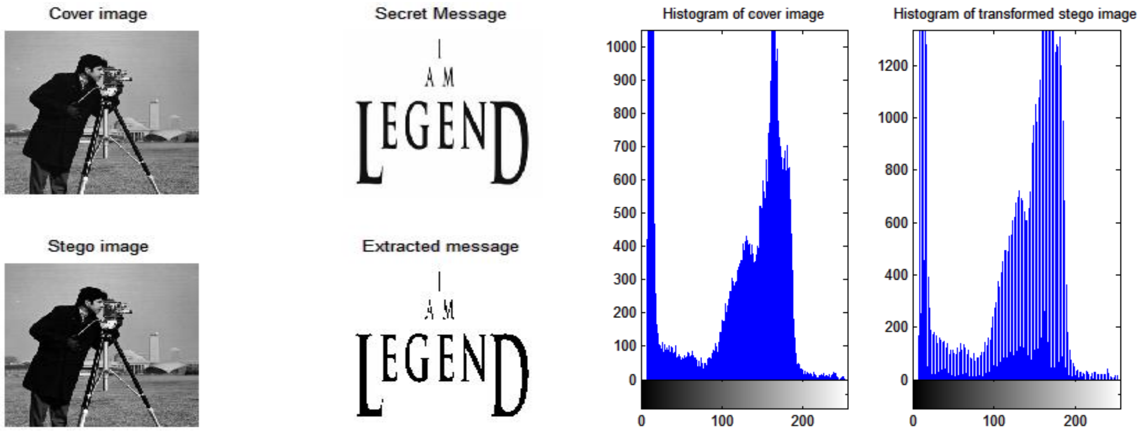


Fig. 6: Simulation results for image steganography.

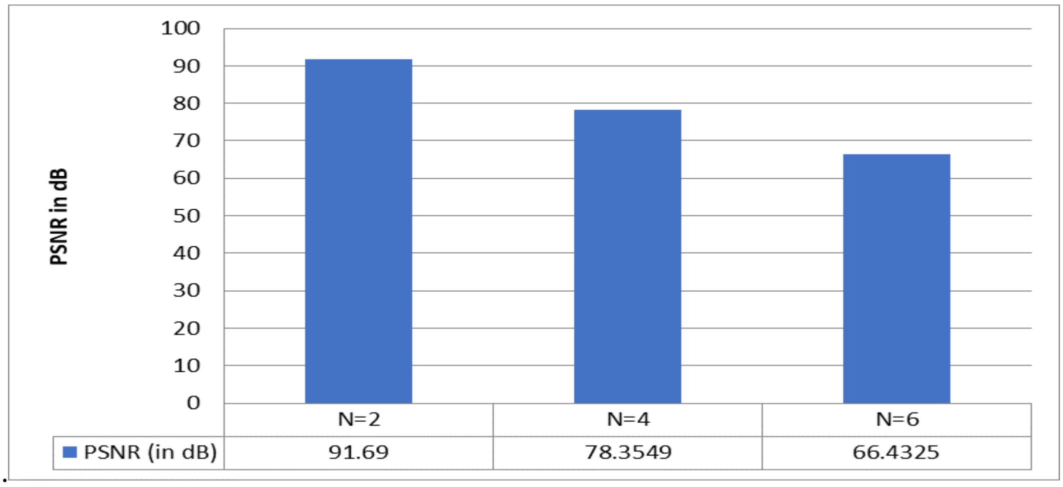


Fig. 7: PSNR comparison for N=2, 6 and 8 and SSIM comparison for N=2, 6 and 8.

In Fig. 7, the quality metrics Peak Signal to Noise Ratio (PSNR) has been calculated for original and stego images and the performance graph has been displayed. We can see that the quality of image has been degrading while increasing the *N* value.

5. CONCLUSION AND FUTURE SCOPE

In conclusion, secure text message image transmission through video steganography using LSB technique-based pixel mapping offers a promising approach for concealing sensitive information within video files. The LSB technique allows for hiding data by manipulating the least significant bits of pixel values, which is imperceptible to the human eye. By mapping the hidden text message to the pixel values of video frames, the information can be seamlessly embedded and transmitted within the video stream. This technique provides several advantages, such as leveraging the popularity and widespread usage of videos as a cover medium, making it less suspicious compared to other forms of steganography. Additionally, the use of pixel mapping ensures that the hidden message is distributed across multiple frames, enhancing the security and resilience against detection.

The future scope of this approach lies in further refining the implementation and exploring additional security measures. Research can focus on optimizing the mapping algorithms to maximize the concealment capacity while minimizing visual artifacts. Additionally, advanced encryption techniques can be combined with pixel mapping to provide an additional layer of security, ensuring that only authorized recipients can decode and retrieve the hidden message. Furthermore, research efforts can be directed towards developing robust methods for detecting and countering steganalysis techniques that aim to identify hidden information within videos. This will contribute to enhancing the overall security and reliability of the proposed technique.

REFERENCES

[1] Sharma, S., & Gupta, D. (2021). Secure text image transmission through video steganography using pixel mapping. International Journal of Scientific & Engineering Research, 12(3), 140-144.

[2] Yadav, A., & Poddar, S. (2021). Text image transmission through video steganography using pixel mapping and encryption techniques. In Proceedings of the 2021 International Conference on Communication, Computing and Networking (ICCCN) (pp. 1-6). IEEE.

[3] Singh, M., Verma, D., & Sharma, S. (2020). Secure text image transmission through video steganography using pixel mapping and cryptography. In Proceedings of the 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 303-308). IEEE.

[4] Verma, R., & Saxena, S. (2020). Secure text image transmission using pixel mapping technique in video steganography. International Journal of Computer Science and Mobile Computing, 9(3), 13-19.

[5] Patel, R. B., & Patel, K. M. (2020). Secure text image transmission through video steganography using pixel mapping and cryptography. International Journal of Innovative Technology and Exploring Engineering, 9(3), 556-561.

[6] Yadav, A., & Poddar, S. (2020). Secure text image transmission through video steganography using pixel mapping. In Proceedings of the 2020 International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies (ICAECT) (pp. 1-5). IEEE.

[7] Roy, A., & Das, S. (2019). Secure text image transmission through video steganography using pixel mapping. In Proceedings of the 2019 4th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 84-89). IEEE.

[8] Khan, F. A., & Kumar, S. (2019). Secure text image transmission through video steganography using pixel mapping technique. In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 141-145). IEEE.

[9] Mohan, A., & Krishna, K. (2018). Secure text image transmission through video steganography using pixel mapping. In Proceedings of the 2018 3rd International Conference on Communication and Electronics Systems (ICCES) (pp. 1425-1429). IEEE.

[10] Kumari, M., & Saxena, A. (2018). Secure text image transmission through video steganography using pixel mapping. In Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 1372-1375). IEEE.

[11] Arora, S., & Choudhary, S. (2017). Secure text image transmission through video steganography using pixel mapping. In Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 195-199). IEEE.

[12] Malhotra, G., & Bansal, R. (2017). Secure text image transmission through video steganography using pixel mapping. In Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 737-742). IEEE.