iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** VIII **Month of publication:** Aug 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.55251

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com*

# Video Steganography Based on Modified Data Protection Scheme

Snehal D. Khandare[1], Dr. Shubhada S. Thakare[2]
[1]*Mtech Student,* [2]*Assistant Professor, Electronics and System Communication Engineering, Government College of Engineering, Amravati, India*

***Abstract:*** ***Since last few years, communication technology more focus about significance over information security during sharing on different platform by using internet service. Also in this world of computer we see everyone is exchange their personal as well as other type of information through the web. The main factor is that how to keep information unchanged while verifying it also keep it safe up to reaches the recipient. One component of the solution to these kind of problems is cryptography. Also steganography can be used security purpose to keep data safe. By Using mathematical techniques and the stego keys the issue how to store them safely.***

***As the video steganography is dynamic in nature this makes difficult to detection of hidden data than other techniques. This combines cryptography and steganography by encrypting the secret text before hiding it with public key encryption system is named after initials of its co-founders Rivest – Shamir – Adleman (RSA) . The goal of cryptography is to prevent unwanted access to or modification of data. Most often, traditional cryptology is used to prevent data from being manipulated, but decoding requires complicated computation. This method analyzed the both Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).***

***This technique is convert plain text to cipher text and encode it in video frame up to two least significant bits (LSB). According to study on different papers as compared to the other methods of steganography techniques this implementation technique is provides the strong embedding capacity also boosts security and robustness as well as improved the imperceptibility of stego-videos.***

***Keywords: LSB technique, Cryptography, MSE, RMSE, PSNR, SSIM.***

## I. INTRODUCTION

Steganography is the technique in which the secret message is hiding in data (cover) and then transmitting to the receiver. At the receiver side, receiver can decode that data and separate the original data and secret message from it. The secret information and the original data mixed together known as ”stego objects”. The human visual system is not able to see the negligible amount of changes occurred in the cover data. It is beneficial to take the video as a cover during hiding process because it provides high concealing capacity, more potential to hide information from attackers, Non-discrimination of cover video and the stego-video is the major concern for any steganography techniques. However if we combine steganography and cryptography techniques it may increase complexity of the resultant technique.

Complexity is measure on the basis of total time taken to embed the secret data. If the hardware devices are increases then the cost of the technique also get increases. Video files have their application in various fields like banking, social sites, medical, education, business etc. As video has large size and it has dynamic nature due to which it is difficult to detect the hide data which gives height to the robustness property against different types of attacks.

The video steganography consist of two phases in which first phase contain the embed secret data in video files and second phase is the extraction of secret message from video files. During work on this technique here firstly select the MP4 or AVI video format file as a cover video.

And separate the frames from that video and choose the desired frame for data hiding purpose. Here the data can embed in selected frames by using LSB technique. Also before hiding the secret text this text is converted into cipher text using cryptography technique.

The original frame and stego frames are collected together to form the video and this video is known as stego video. At the receiver side the extraction of secret data done by following the vice versa process. Following Fig. 1 shows the basic block diagram of video steganography and there working process using systematic way.

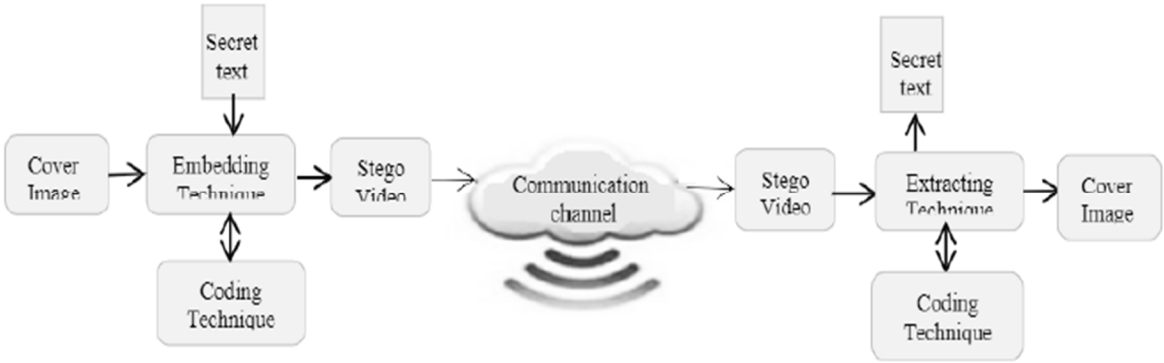



*Figure 1: steganography with video image*

## II. LITERATURE REVIEW

In this section some of the steganography techniques are reviewed. Researchers done lot of study on the steganography techniques, here are some work done by different author

Ellappan Venugopal et al [1] used structure a modified CNN- based stegonalyzer for images applying as a one kind of inserting key. In this it implement the less convolutions having bigger channel in last convolutional layer. It can manage bigger image and lower payloads. Jaladi Vivek et al [2] proposed the video steganography by introduced the chaos with enhanced mapping technique to reduce computational complexity and fast encoding. In this the position of each pixel of secret video frame is calculated by the ELSB technique. The existing LSB technique is not taken into account which leads to high video distortion. The authors Zahid Iqbal Nezami et al [3] used the technique that converts the plain text to ciphertext and encode it in cover data using up to four least significant bits (LSB) based on hash code. The human eyes can't see the difference between the initial and resulting image after modification occured. K.Jayasakthi velmurugan et al [4] uses the combination of hybrid neural networks and hash function for determining the essential bits in cover video to embed the secret data in it. For embedding process the cover video and secret data will first uploaded and then the hash algorithm and neural network are applied for extracting the data the vice versa process can be done and for this here the MATLAB 2016 software is used. Urmila Pilania et al [5] proposed the integer wavelet transform technique also the JPEG (Joint Photograph Expert Group) compression to perform the steganography technique. Video is use as a cover file and JPEG compression technique is improve the concealing capacity because it has intrinsic properties. And the Integer Wavelet Transform is improved the imperceptibility and robustness. The paper published by Manohar N. et al [6] proposed that there are many methods used for video steganography but they will not provide different types of formats, security and quality of the results. So this paper used the steganography method by using the secure based LSB, Fuzzy logic, and Neural Networks also check the PSNR and MSE. The paper published by Yiming Huang et al [7] proposed that the novel video steganography scheme based post-quantum cryptography technique .this technique provide the extraordinary security character which makes it different from others. Also it has excellent visual invisibility and large amount of message inserting capacity. The paper published by Asha Durafe et al [8] proposed the steganography technique by using Raspberry pi and GSM module. In this the image can be hidden by using steganography and the password is protected using QR code. Also the two files are zipped using password and mailed to the receiver using Raspberry Pi. And GSM module is used to send OTP. Murat Hacimurtazaoglu et al [9] used a poly-pattern key block matrix (KBM) as a key in LSB based video steganography. Also for detection of the imperceptibility the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are calculate. Pingan Fan et al [10] proposed robust video steganography against video transcoding to construct the hidden communication on social media. To select robust embedding regions new strategy based on principal component analysis is used. Proposed method provides stronger robustness and reliability over media channel, better security performance against other existing methods.

The paper published by S. Suganthi et al [11] used the steganography as well as cryptography technique for hiding secret data to enhance the security system. To avoid the hacking issues the proposed method used RC7 encryption for encrypting secret text data into cipher text .also in this paper Chaos Algorithm, RC7 Algorithm, and LSB Algorithm are used. Ramadhan J. Mstafa and Khaled M. Elleithy et al [12] used video steganography algorithm based on linear block code. Here the image is used as a secret message and cover data is nine uncompressed video sequences. To improve the system security the pixel's positions of secret data and cover data are randomly reordered by using private key.

For add more security before embedding the secret message it is encoded by applying Hamming code (7, 4). Again the result of encoded message is added with random generated values by using XOR function. The paper published by Laxmi Gulappagol et al [13] proposed the RSA algorithm is used to hide the secret image into a cover video. The data is shuffled by using the Fisher Yates algorithm. After that the Discrete Cosine Transform is applied to generate 8*8 blocks. T. Aravinda Babu and K.S.R.S Jyothsna et al [14] proposed video steganography technique by using DWT-BCH method. In this firstly video is separated into sets of image and then DWT is applied to each image. By converting the secret key into binary data BCH coding is perform. Then BCH coded data is embedded into DWT image. Cho Do Xuan et al [15] used BPCS (Bit Plane Complexity Segmentation) method for improving the efficiency of steganography technique. For improving more, the complexity formula of the bit planes are used. It helps to improving the thresholds in the bit planes to find more planes hiding secret information but also keep their safety. Dhandapani Samiappan and PR. Buvaneswari et al [16] proposed the three secure steganography algorithms that embed a bit stream of the secret message into approximation coefficients of the integer wavelet transform (IWT), DWT and to form stego-video LBP method is used. The paper published by Rawaa Abd Alhakem and Mohammed Abdullah Naser et al [17] proposed combined methods cryptography and steganography by encrypting the secret text before hiding it using RSA algorithm. In addition for increase the extra layer of security the hased based least significant bit mechanism are also used. Katarzyna Koptyra and Marek R. Ogiela et al [18] proposed the multi-steganographic system for the Internet of Things. For data input it uses two user friendly sensors i. e. thumb joystick and touch sensor. This method is beneficial because it has low complexity hence it is easy to implement. Minghui Li et al [19] proposed VVC (versatile video coding) steganographic algorithm based on coding units (CUs). To embed secret information the proposed steganography uses Chroma CUs. To reduce bit rate of stego video a novel convolutional neural network (CNN) are used. Minkyung Kwak and Youngho Cho et al [20] proposed the video steganography based on social network service (SNS) platforms. To embed much more secret data than existing tools they can use the two open tools VirtualDub and Stegano also design a new payload approach based video steganography method(DECM: Divide-Embed-Component Method).

## III. PROPOSED METHOD

### *A. Embedding Procedure*

On the sender's side, the embedding procedure consists of several steps, the most important of which is to encrypt the secret message using data encryption algorithm. Choosing the cover video file that will be used in hiding and then collecting information from it after which the cover video frame are separated from each other. And this frame are used to hide the data. In the proposed work having the several steps which are as follows as per reference of Fig 4.1

*1)* First here select the cover video having MP4 or AVI format
*2)* Here collect the required information from video
*3)* And separate the frames from the original video
*4)* After separating the frames the frame selection are done for data hiding purpose
*5)* Selected frames are used for data hiding and remaining frames are kept as it is
*6)* The data is hide in selected frame by using LSB embedding technique
*7)* The secret text message is hided in that selected frames but before hiding it the secret text is converted into cipher text using cryptography technique and for additional security purpose here added one codeword data
*8)* After hiding the secret message in selected frame the output is stego frames and it will added in other frame of original video and it get stego video which is send at receiver side.

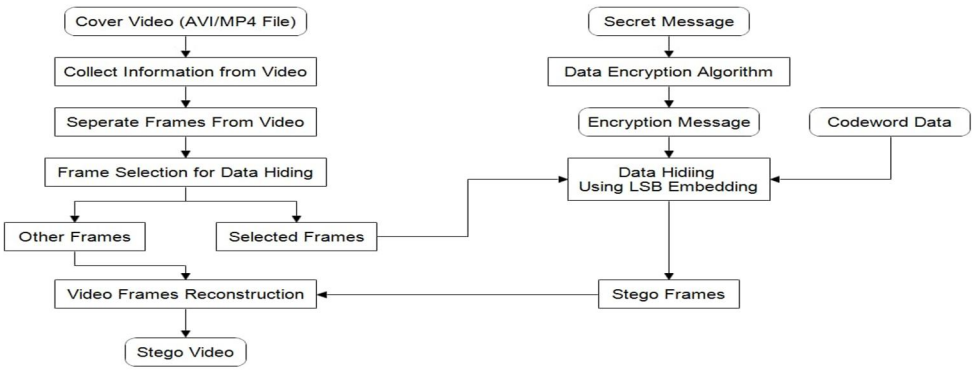



Fig 2 Block diagram of Embedding Process of Data Protection Scheme

*B. Extraction Procedure*

On the receiver's side, the extraction procedure consists of several steps which as per shown in Fig 4.2 to decrypt the secret data, choosing the stego video file carries the secret message and the collecting information from it after which the stego frames are separated from other frames .The suggested (LSB) method was used to extract the encrypted secret message from the selected stego frames. To decrypt the secret data, the receiver will use the Data decryption technique to decrypt the secret data. The proposed work has used the following extraction steps

*1)* First the stego video is collected
*2)* Then the required information collect from that video and separate the frames
*3)* After separating the frames the frames are selected for further data decoding process
*4)* Selected frames are used for data extraction process using LSB embedding techniques and other frame are kept as it is
*5)* The vice versa process of embedding are done for extraction of secret data by using data decryption algorithm the secret data are recovered from it and also before decryption the codeword data is apply to that secret message containing frames for security purposed
*6)* After recovery of secret data the remaining frames are added with other frames and the original video are obtained.

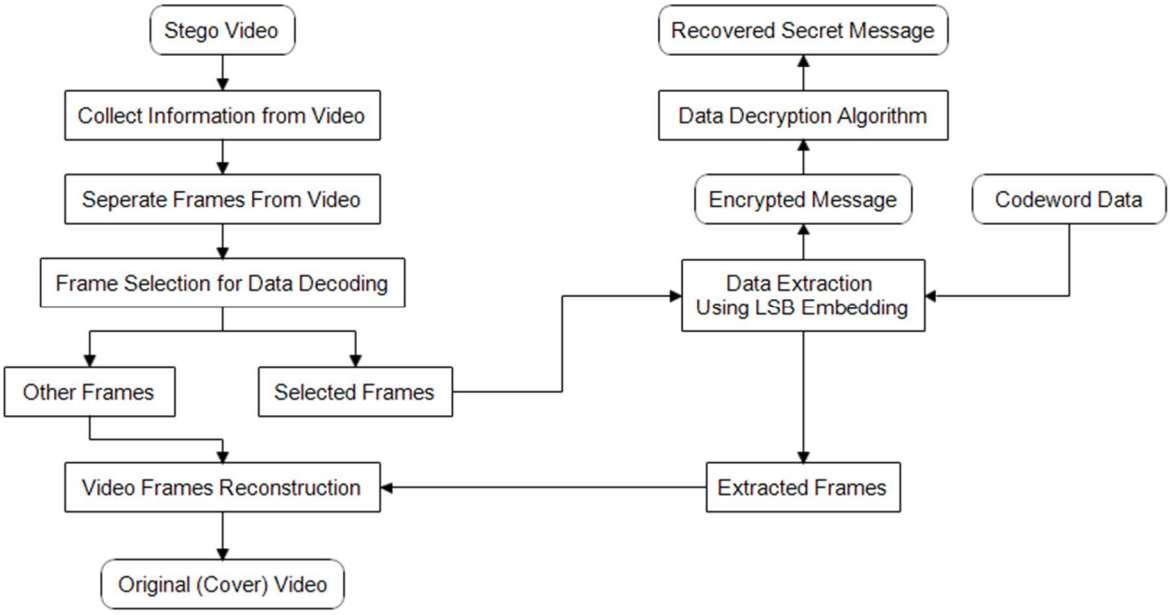



Fig 3 Block diagram of Extraction Process of Data Protection Scheme

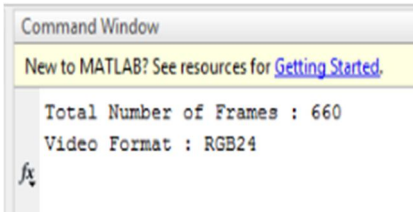
## IV. RESULTS

*A. Analysis 1: Data Protection Scheme*

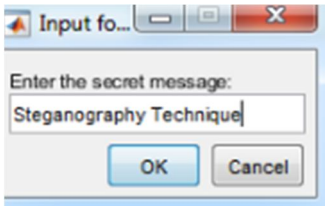
*1) Case I*

Test case 1 Video format: MP4

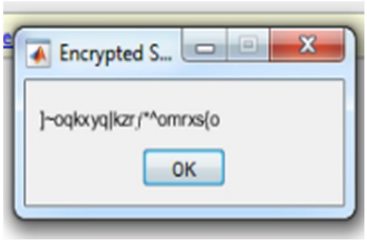
The following output images shows the result of the data protection scheme by using video steganography process. Also calculate the parameter like MSE, RMSE, PSNR and SSIM.



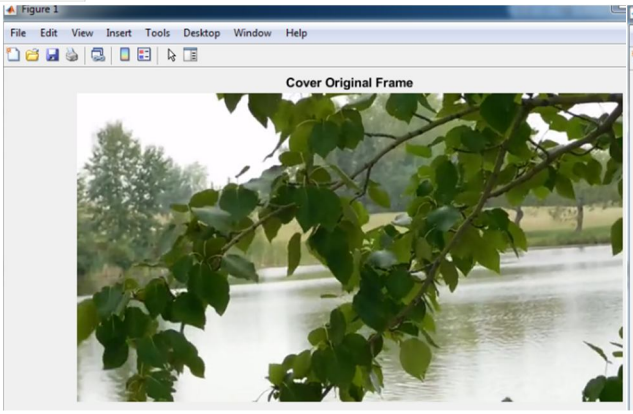

Frame format



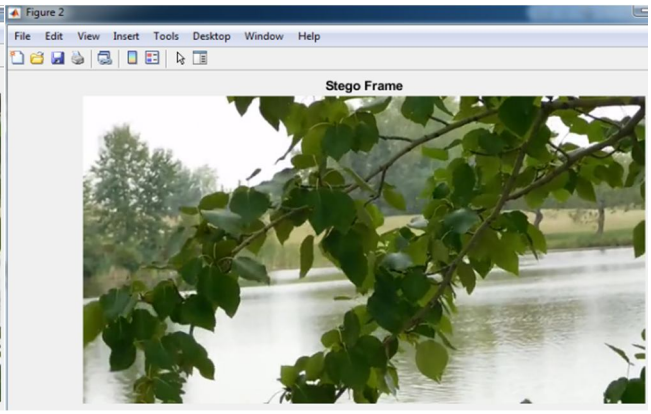

Secret Message



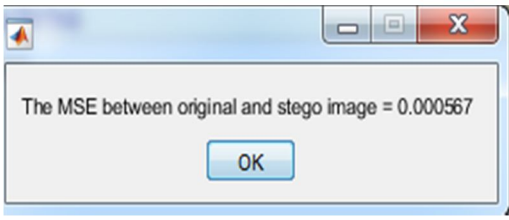

Encrypted secret message



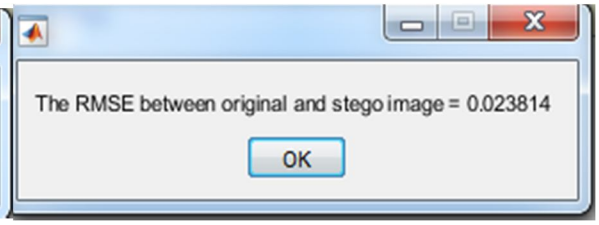

Original cover Frame



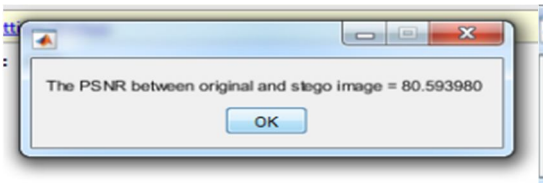

Stego Frame



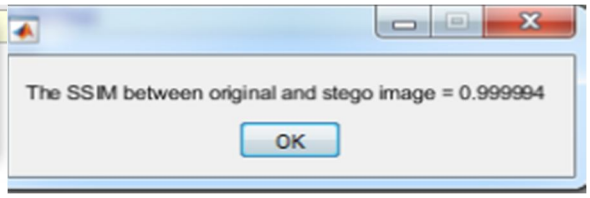

MSE parameter



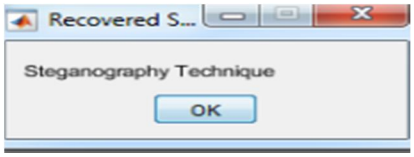

RMSE parameter



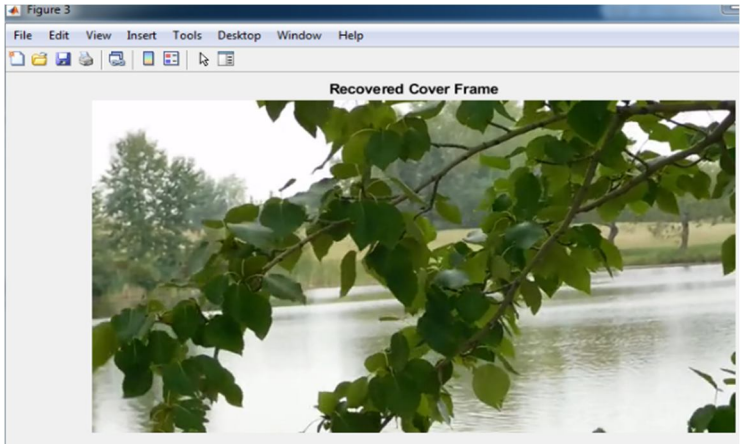

PSNR parameter




SSIM parameter




Recovered secret message



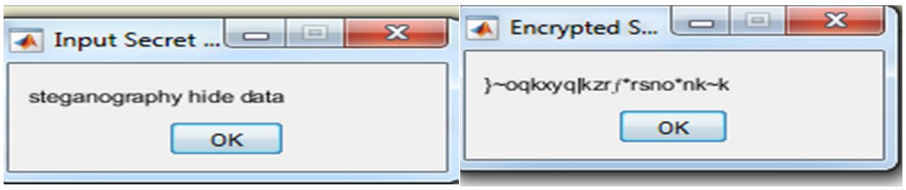

Recovered Cover Frame

In above case 1 the codeword data of authentication and extraction stage are same due to which the original cover frame and the secret message are recovered at receiver side. If the codeword data are different at authentication and extraction stage then there is impossible to recover the original cover frame and secret message at receiver side which is shown in next case.

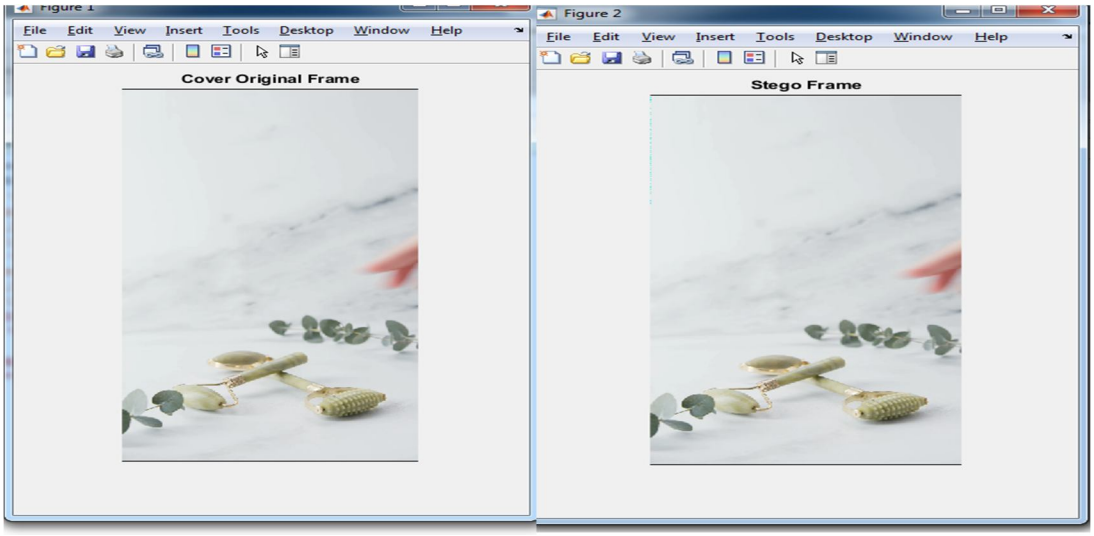
*2) Case II*

- Test case II Video format: MP4

As we see the case I results, the case II result output is different from the case I. If we make any changes in the code word data of both sender and receiver side then there is error occurred. It means that if the code word data at authentication and the extraction side are not matched then the error will be occurred during recover the secret message and the original cover video. It cancan shows as follows:

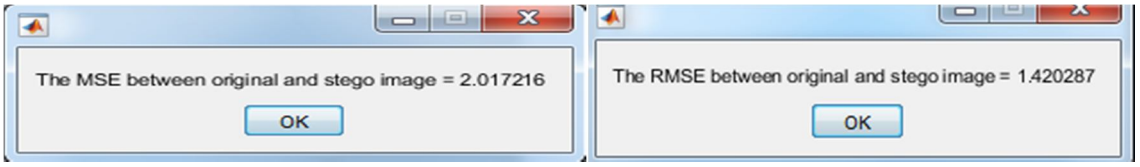



Secret message Encrypt secret message

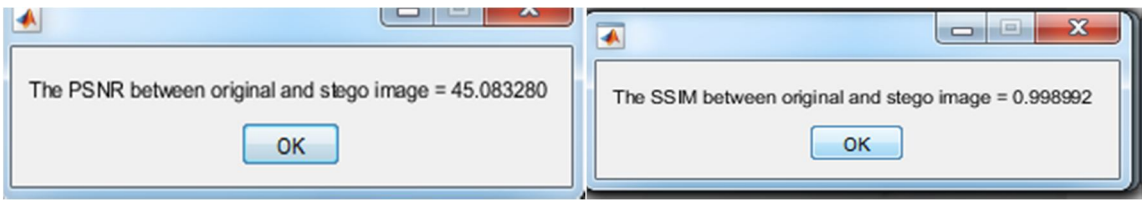



Cover original frame Stego frame

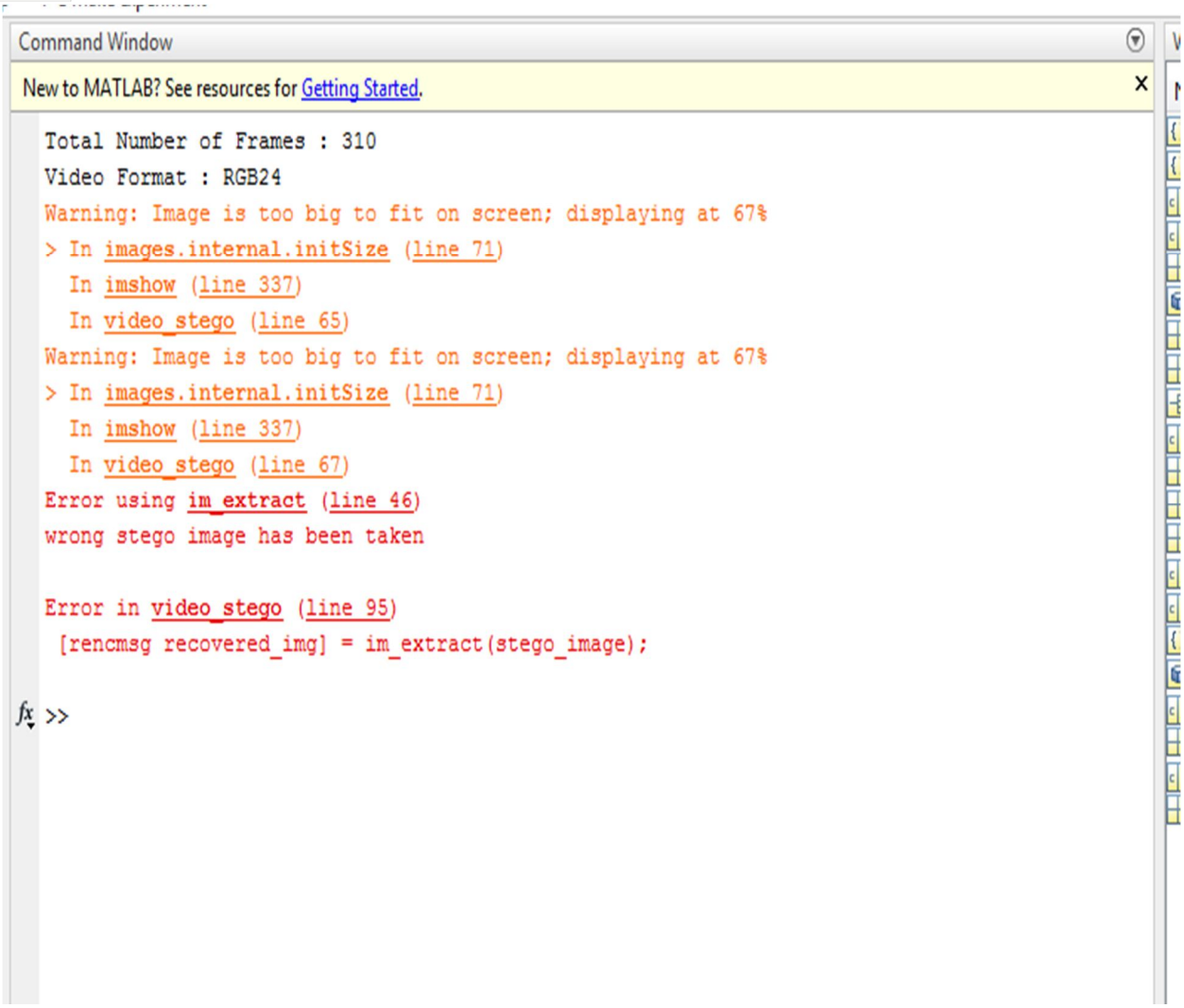
The parameter calculated for this MP4 video during the video steganography process is as below




MSE parameter RMSE parameter




PSNR parameter SSIM parameter




Error occurred due to mismatch the codeword data

*B. Analysis 2*

Observing parameters values for MP4 and AVI video format for different LSB positions

For MP4 and AVI video format by inserting different LSB position and keeping other factor same the parameter changes as follows:

Table 2.1 Parameter changes for MP4 and AVI video having different LSB position

| Sr. No. | Video Format | Total NO. of Frames | LSB Position | Secret message | MSE | RMSE | PSNR | SSIM |
|---|---|---|---|---|---|---|---|---|
| 1 | MP4 | 171 | 2 | Steganography | 0.365534 | 0.604550 | 52.0501521 | 0.999954 |
| 2 | MP4 | 171 | 4 | Steganography | 0.365574 | 0.604576 | 52.301050 | 0.999954 |
| 3 | MP4 | 171 | 8 | Steganography | 0.365595 | 0.604594 | 52.501521 | 0.999954 |
| 4 | MP4 | 171 | 16 | Steganography | 0.367825 | 0.604612 | 52.651723 | 0.999954 |
| 1 | AVI | 171 | 2 | Steganography | 0.000035 | 0.005893 | 92.724728 | 1.000000 |
| 2 | AVI | 171 | 4 | Steganography | 0.000037 | 0.006107 | 92.414386 | 1.000000 |
| 3 | AVI | 171 | 8 | Steganography | 0.000040 | 0.006314 | 92.124749 | 1.000000 |
| 4 | AVI | 171 | 16 | Steganography | 0.000034 | 0.005838 | 92.805907 | 1.000000 |

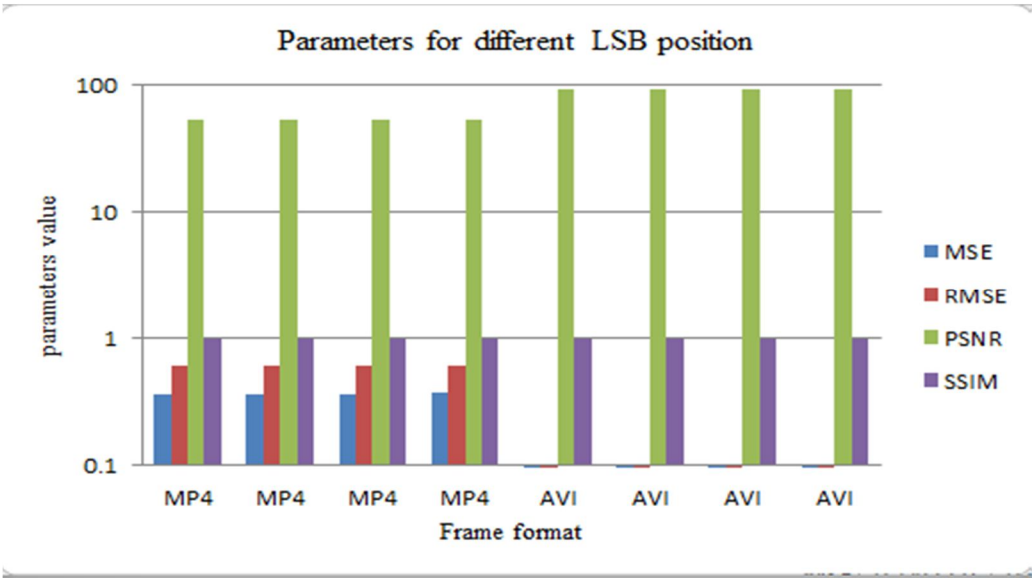



Fig 4 Various parameters for different LSB position

*C. Analysis 3*

Observing Processing Time for MP4 and AVI video format having same frame rate

For MP4 and AVI video format the processing time changes shown as follows:

Table 3.1 Processing time for MP4 and AVI video format

| Sr. No. | Video Format | Total No. of Frame | Secret Message | Processing Time | |
|---|---|---|---|---|---|
| | | | | T1 (sec) | T2 (sec) |
| 1 | MP4 | 310 | Steganography | 31.81 | 0.0724 |
| 2 | AVI | 310 | Steganography | 58.37 | 1.69 |
| 3 | MP4 | 161 | Steganography | 9.80 | 0.05 |
| 4 | AVI | 161 | Steganography | 13.03 | 0.25 |
| 5 | MP4 | 171 | Steganography | 12.61 | 0.04 |
| 6 | AVI | 171 | Steganography | 18.33 | 0.08 |

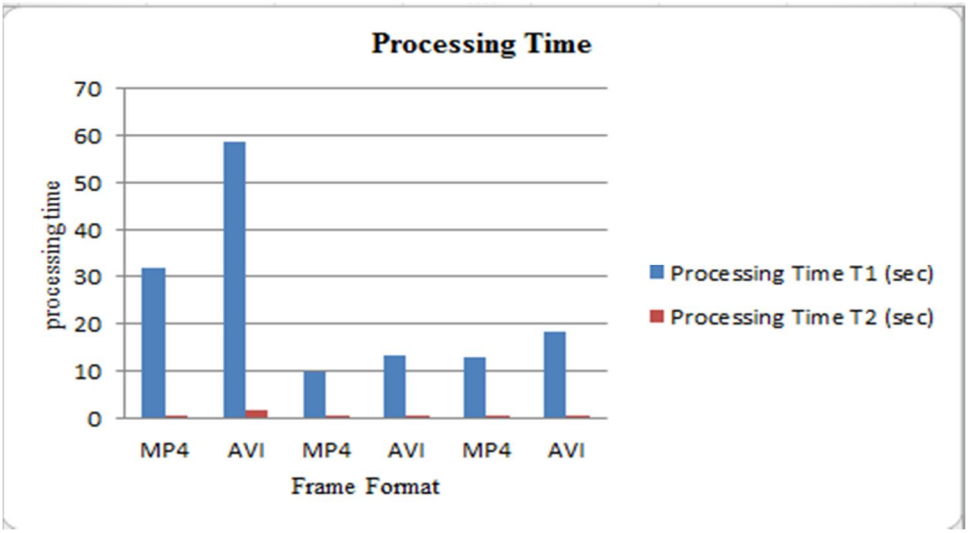


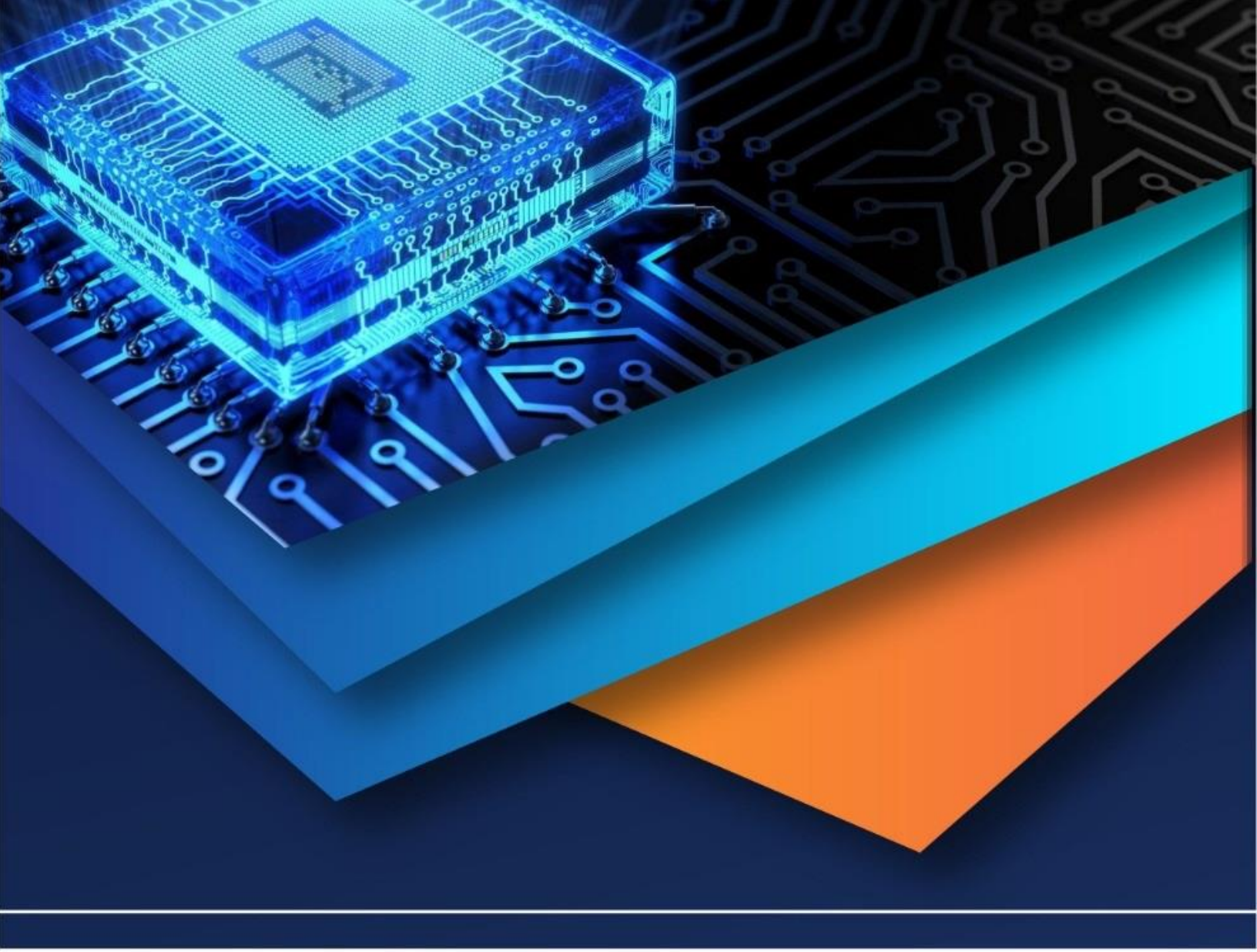

**Fig 5** Processing Time parameter of MP4 and AVI format

## V. CONCLUSION

According to the virtual research on cryptographic scheme it is found that the cryptography technique is simpler to implement without needing any complicated keys. In order to reduce the computation and furthermore secure the data, steganography technique used for hiding data that allow reliable storage without any risk and improve security. Video steganography technique are useful because they allow for more secure storage of highly sensitive data, including encryption keys, missile launch codes, and numbered bank accounts. By distributing the data, there is no single point of failure that can lead to its loss. Proposed technique provides security, reliability and convenience. The proposed method can encrypt the secret text message. The steganography method that (LSB) that implemented for text embedding is stronger in terms of reliability, capacity, security, imperceptibility as well as performance and computing complexity than standard embedding procedures. This proposed method can be robust "steganalysis process" for encrypts the secret message.

## REFERANCES

[1] Ellappan Venugopal, Selvarasu Ranganathan, V. Velmurugan, TadesseHailu,(2020)."Design and implementation of video steganography using Modified CNN algorithm"
[2] Jaladi Vivek Baswaraj Gadgay (2021). "Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding"
[3] Zahid Iqbal Nezami, Hamid Ali,Muhammad, Asif,Hanan Aljuaid, Isma Hamid and Zulfiqar Ali (2022). "An efficient and secure technique forimage steganography using a hash function"
[4] K.Jayasakthi velmurugan and S.Hemavathi (2019). "Video Steganography by Neural Networks Using Hash Function"
[5] Urmila Pilania, Rohit Tanwar, Mazdak Zamani, and Azizah Abdul Manaf (2022). "Framework for Video Steganography Using IntegerWaveletTransform and JPEG Compression"
[6] Manohar N, Peetla Vijay Kumar (2020). "Data Encryption & Decryption Using Steganography"
[7] Yiming Huang, Zhongkui Lei, Zhufu Song, Yueru Guo, Yihang Li (2021). "A Video Steganography Scheme Based on Post-Quantum Cryptography"
[8] Asha Durafe and Ritika Desai (2020). "Steganography for Public Security"
[9] Murat Hacimurtazaoglu and Kemal Tutuncu (2021). "LSB-based pre-embedding video steganography with rotating & shifting poly-pattern block matrix"
[10] Pingan Fan, Hong Zhang and Xianfeng Zhao (2022). "Robust video steganography for social media sharing based on principal component analysis"
[11] R. BanuPriya, J. Deepa and S. Suganthi (2019). "Video steganography using LSB algorithm for security application"
[12] Ramadhan J. Mstafa and Khaled M. Elleithy (2014). "A Highly Secure Video Steganography using Hamming Code (7, 4)"
[13] Laxmi Gulappagol and K. B. Shiva Kumar (2020). "Application of Fisher Yates Data Shuffling and RSA Encryption in Transform Domain Video Steganography"
[14] T. Aravinda Babu and K.S.R.S Jyothsna (2021). "Performance Analysis of video steganography using DWT-BCH method"
[15] Cho Do Xuan (2021). "A Proposal to Improve the Bit Plane Steganography based on the Complexity Calculation Technique"
[16] Dhandapani Samiappan and PR. Buvaneswari (2019). "Video Steganography using IWT, DWT, LBP Methods and its Research"
[17] Rawaa Abd-alhakem and Mohammed Abdullah Naser (2021). "Video steganography based on modified embedding technique"
[18] Katarzyna Koptyra and Marek R. Ogiela (2023). "Steganography in IoT: Information Hiding with Joystick and Touch Sensors"
[19] Minghui Li, Zhaohong Li and Zhenzhen Zhang (2022). "A VVC Video Steganography Based on Coding Units in Chroma Components with a Deep Learning Network"
[20] Minkyung Kwak and Youngho Cho (2021). "A Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger"
[21] Farah Qasim Alyousuf and Roshidi Din (2019). "Review on secured data capabilities of cryptography, steganography, and watermarking domain"
[22] Maisa'a Abid Ali Khodher (2021). "Suggested Video Steganography Algorithm Based on Power Low Transform (PLT) Using IoTs"
[23] Shree Shradha S and Vaishnavi Poul (2020). "IJARCCE Video and Image Steganography"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY