



IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.569



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

Investigation of Image Steganography for Security Application

Dr R Prem Kumar¹, K Reddy Meghana², G Ramya Sree³, M Rahul⁴, T Sai Kumar⁵,
S Mohammad Sultan⁶

Department of Electronics and Communication Engineering, Siddharth Institute of Engineering & Technology, Puttur,
Andhra Pradesh, India¹²³⁴⁵⁶

ABSTRACT: Steganography is the domain of secreting data and a push to cover the presence of the embedded data. It's anything but a superior way of getting messages, not the presence of the message. Unique messages are being covered up inside a transporter such that the progressions so happened in the Carriers are not discernible. Video Steganography assumes a critical part in media applications to get and confirm advanced pictures. This work presents a thorough investigation of different video Steganography procedures and heuristic based picture Steganography strategies. This paper uses the concept of video Steganography, where the data is hidden behind the frames of videos. This paper provides two level of security to the data i.e. Steganography and cryptography. First the data is encrypted using cryptography algorithm, next the encrypted data is embedded into frames of videos. The Shuffling technique used to embed the data. It is the most common technique, but can hide large amount of data in most simplest and efficient way.

I. INTRODUCTION

Innovation has rapidly scaled over the previous year's prompting a wide utilization of mixed media for moving information, particularly Web of Things (IoT). Generally, the exchange occurs over shaky organization channels. Specifically, the web has acquired sped up notoriety for trading advanced media also, people, privately owned businesses, organizations, governments utilize this mixed media information move techniques for trading information. In spite of the fact that there are various benefits connected with it, one conspicuous detriment is the protection and security of the information. The accessibility of various promptly accessible apparatuses fit for misusing protection, information uprightness and security of the information being sent has made the chance of indicative dangers, snooping and other incendiary exercises. Steganography, which is utilized to shroud the data in plain sight, permits the utilization of a wide assortment of the restricted Intel structures like picture, text, sound, video and files. Advanced watermarking is another technique where private data is installed to guarantee possession. Cryptography is the mainstream utilized for data covering up, yet, Steganography is acquiring prevalence as of late [1].

Video pressure is the answer for managing the tremendous number of pieces engaged with video transmission. Since network assets are restricted, a video is compacted to previous transmission or capacity. Be that as it may, for security purposes, Steganography and watermarking procedures are utilized to accomplish secrecy and trustworthiness separately. Steganography is the craftsmanship that manages concealing a mysterious message into a guiltless transporter medium shaping a stego medium. This stego medium ought not to uncover the presence of the covered-up secret message. Watermarking is another concealing technique, however at the point when the object is honesty and licensed innovation data being traded [2], [3].

As per the implanting area, video Steganography could be arranged into two principal classes [4]: uncompressed space video Steganography and compacted area video Steganography. For uncompressed-area Steganography calculations [5], [6], information implanting happens before the video coding measure. Hence techniques for this kind are dependent upon the deficiency of covered up information brought about by video pressure. With respect to packed area video Steganography strategies, sentence structure components of packed video are controlled for information installation. Generally utilized grammar components incorporate movement vectors [24],[25], intra expectation modes [7], [8], entomb forecast modes [9], [10], quantization boundaries (QPs) [11], [12], and quantized change coefficients (QTCs) [13],[14]. Steganography infuses given data into a cover media like advanced pictures, sound signs or recordings, to shroud its reality. In this way, Steganography accomplishes data stowing away in such a manner that nobody can

perceive the presence of information aside from the collector. Though, if there should arise an occurrence of cryptography, the presence of data isn't covered up yet its qualities are clouded [15].

II. RELATED WORK

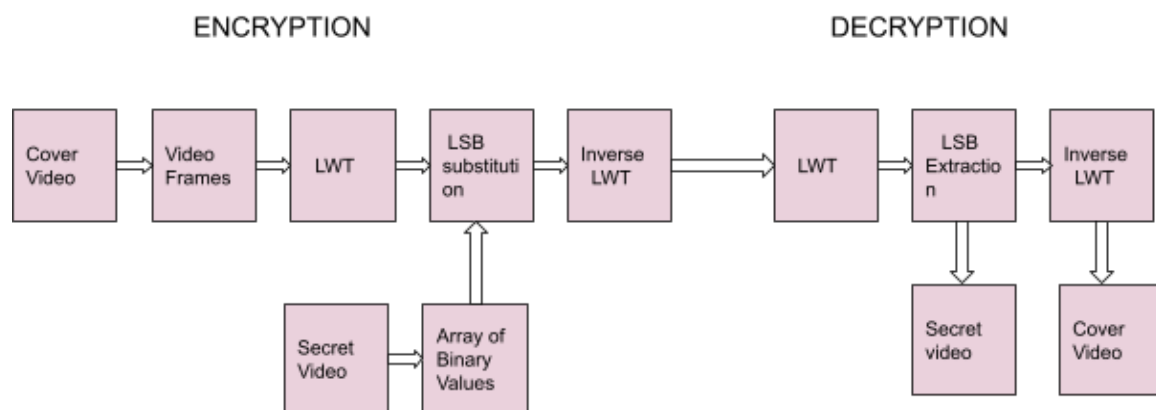
Steganography injects given information into a cover media like progressed pictures, sound signs or chronicles, to cover its world. Along these lines, Steganography achieves information stowing away in such a way that no one can see the presence of data beside the authority. However, on the off chance that there ought to emerge an event of cryptography, the presence of information isn't concealed at this point its characteristics are blurred [15].

In encryption, the technique called the AES algorithm has used. Along with the AES algorithm pixel swapping technique is also used to embed the message into the videos. Encryption has been done using AES algorithm. Embed this encrypted message into the pixels to enhance the double level security. The concept of PSNR value calculation is used in this paper to compare the original and stego image. PSNR is Peak Signal-to-Noise Ratio. Both the PSNR values are compared, if we get the more value in the stego image, then we can say the proposed system is secured [5].

Steganography Imaging System (SIS) provides the two levels of security In this system cryptography is not used for first level of security instead Username and password is used to provide the login security. Here the secret key is used only to retrieve secret message from the image not for the encrypting purpose. In the proposed system, first the secret message is transferred to text file. Then the text file is compressed to zip file. At the next level the zip file is converted into binary codes to embed the message into image. The purpose of using zip file is that zip file is more secure than the normal text file [7].

III. SYSTEM DESIGN

A. Preparing the Secret Message



In the first place, the mysterious message is composed with the English alphabetic. From that point forward, the mysterious message is encoded to build the security. In this interaction, the mysterious message is encoded using a key that is learned by Equation 1

$$\text{key} = \text{round}(\text{sum}(u)) / 2 \quad (i)$$

Where u means a set of random values calculated using Eq. (2):

$$u = \text{rand}(1, 5) \quad (ii)$$

Here, the capacity key produces a bunch of arbitrary qualities, which gives a serious level of safety for the mysterious message. In each phase of execution, the worth of the key will differ as per arbitrary qualities that will be produced, and by applying Eq. (3), the mysterious message will be encoded:

$$E = \text{sm} + \text{key} \quad (iii)$$

B. Embedding Process

During this stage, the encoded secret message is installed inside video outlines by using the knight visit calculation and the LSB technique. Here, the video is parted into outlines and changed over into a bunch of pictures. From that

point forward, the casings used as a cover are picked arbitrarily. Thereafter, the pixels inside the picked outline used for concealing the information inside it are picked arbitrarily using a knight visit calculation. Then, at that point, the LSB strategy is used to shroud the scrambled mystery message inside the picked pixels. Afterward, this interaction was applied on the arrangement of pictures until the scrambled mystery message was finished. Then, at that point, the arrangement of pictures was changed over to the edges. Finally, the video outlines are converged to get the stego video.

i. *Preparing the Cover Video*

This cycle addresses the arranging interaction for the cover video to implant the data inside it. Here, soundvideo interleave (AVI) is used as a cover for concealing the restricted data. AVI is a sort of video record contained a social occasion of pictures and sounds and called outlines. AVI has a significant size, and the chief benefit of using concealing the colossal proportion of data can be implanted inside it. Additionally, it very well may be communicated from sender to beneficiary over the organization after the installing cycle [2], [13]. At first, the video is divided into outlines. From that point onward, the casing utilized for implanting is arbitrarily chosen. Then, at that point, the knight visit calculation is used to pick a particular pixel of the picked edge to insert the information using the LSB technique.

ii. *Knight Tour Algorithm*

One of the deficiencies of the LSB technique is the sequential determination of the pixels. Therefore, discover techniques that utilization an irregular determination. One of these strategies is the knight visit calculation. It's anything but a progression of moves of a knight on a chessboard so much that the knight visits each square only one time. Ensuing to isolating a video into outlines, as per this technique, the picked outline is addressed as a chessboard and as indicated by the development of the knight on the chessboard, which is one line and two segments or two lines and one segment in arbitrary manners like the letter (L) in English [3], [8], to pick the pixels used for installing the information. This cycle is used to build the power of the proposed technique and to beat the impairment of the LSB strategy that applies the sequential decision of the pixels and the weakness against the electronic attacks.

iii. *Least Significant Bit (LSB) Method*

After the way toward picking pixels of casing by using the knight visit calculation, the LSB technique is used to implant an encoded secret message inside it. The LSB strategy is viewed as an acclaimed and simple technique in steganography [28]. In this strategy, a video outline managing is done by changing the most un-critical pieces 7 and 8 to implant the restricted information to make the cycle of progress in the video outline hard to perceive by the natural eye. Eq. (4) is used to figure the pixel esteem after the inserting interaction [28]:

$$a_i' = a_i - a_i \bmod 2n + E_i \quad (iv)$$

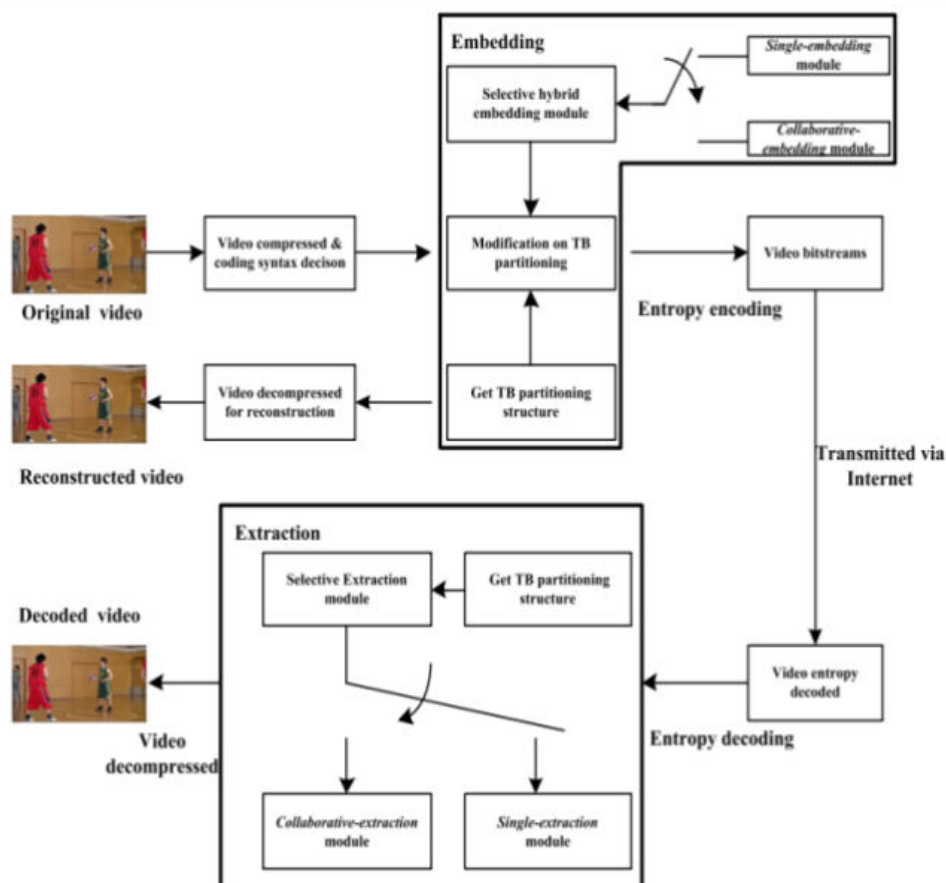
C.Extraction Process

In this stage, after the installing interaction is finished, the sender sends the stego video into the beneficiary. The stego video is masterminded by separating the video into outlines. Thusly, the pixels that have the information inside it are controlled by using the knight visit calculation and applying comparable advances that are used as a piece of the installing interaction. From that point forward, the LSB strategy is used to separate the encoded secret message from the LSB (7 and 8) of the video outline by using Eq. (5) [28].

$$E_i = a_i' \bmod 2n \quad (v)$$

Where E_i addresses the encoded secret message esteems, and a_i' addresses the worth of the pixel of the stego picture. Afterward, the encoded secret message will be decoded to get the mysterious message by using Eq. (6):

$$S_m = E - \text{key} \quad (vi)$$



The proposed video steganography scheme consists of three components, including embedding, carrier bit streams transmitted, and extraction components. First, prior to embedding, the partitioning structures of CB, PB and TB need to be obtained from coding decision of H.265/HEVC, where the partitioning structures are the results, which could achieve the minimum cost of distortion and number of bits with adopting current partitioning structures. And then, selective hybrid embedding modules video bit stream has reached to receiver, the partitioning is established according to different applications. If we need large volume of secret message to be embedded, single-embedding module can meet this demand. If we need high security and perceptual video quality, collaborative embedding module can be applied. Second, when the secret message has been embedded into carrier video, there are two alternative processes. One is ultimately encoded the carrier video to bit stream by entropy coding and enjoyed by the audiences via network transmission. Another is the reconstructed digital video which is constructed for the future prediction process of subsequent PB, with the similar process of the decoder. Finally, when the carrier structures of CB, PB and TB are obtained and analyzed for the search of targeted embedded TBs after entropy decoding. Selective extraction module is confirmed from two alternative extraction modules of Single and Collaborative-extraction. As the result of extraction process, the embedded secret message depended on TB block decision is extracted.

IV. RESULTS

The result of this paper is analyzed with different videos as input. This result provides the double security to any given input. First level security is provided through encrypting the secret information and second level security is provided through Steganography. The Steganography hides the secret information behind the encrypted videos.

There are different algorithms for implementing the encryption of secret data. The one used in this paper is DES encryption algorithm. The reason behind using the DES algorithm is, it is the simplest and fastest algorithm for encryption of data. The secret data is encrypted using the 16 rounds of encryption techniques. These 16 rounds contain P-box, S-box, E-box of operations. Along with this 16 rounds of encryption the 16 round of key substitution is also performed, which provides 16 different subkeys at each step. These subkeys provide better security for encrypting data.

Secret key is the important part of the encryption. Receiver decrypts the secret information using the same secret key provided by sender. A single bit change in the secret key may retrieve the wrong information. At the next level the encrypted data is hidden behind the cover media. The cover media may be audio, video, text, and protocol. This paper is implemented with the video as the cover media.

Figure 6 shows the sample secret message. In this work we have used Shuffle method to generate a key file. This method shuffling the bits in a random order and produces a key file. This file is necessary to retrieve the hidden message. Otherwise it is impossible to retrieve the original file from the encoded one.

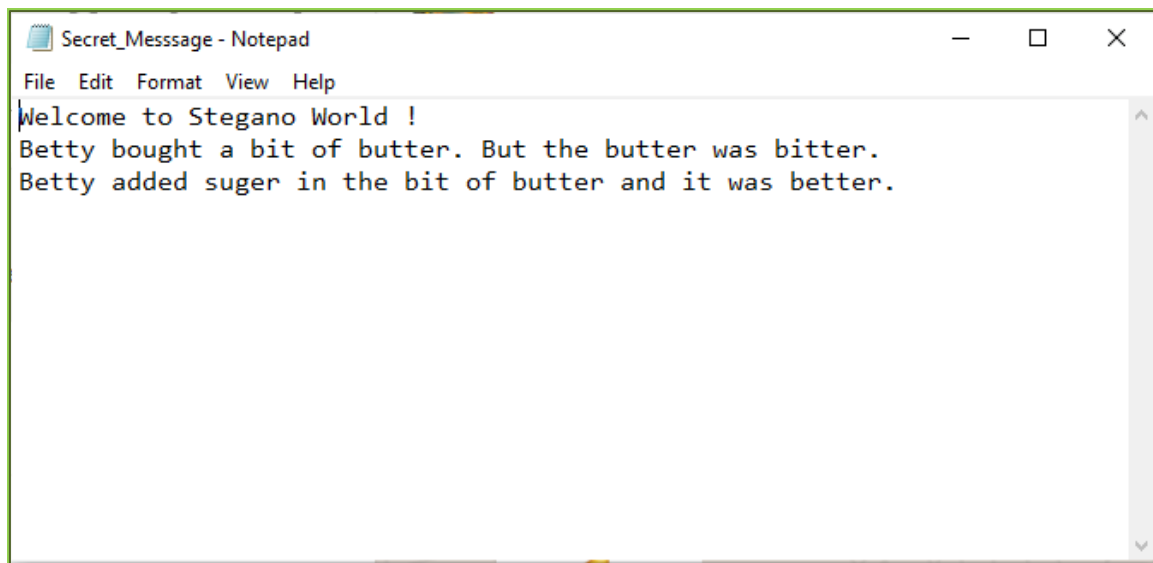
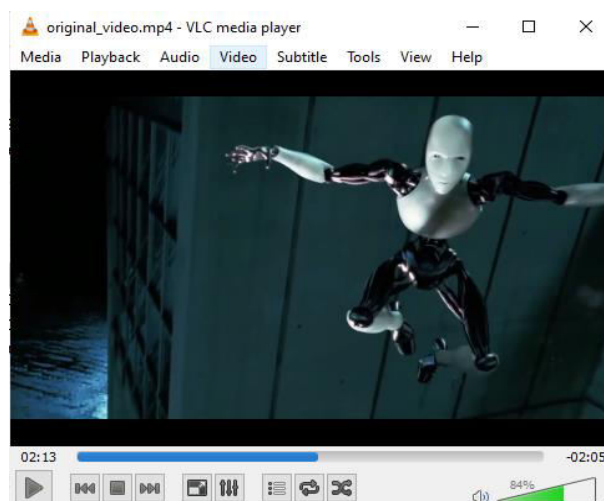


Fig 6: Sample Secret Message



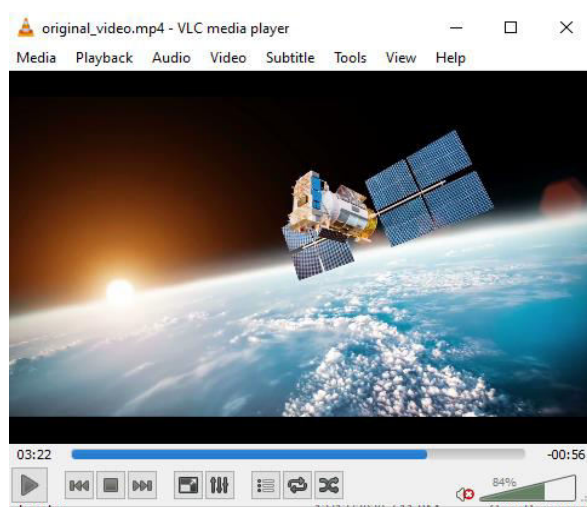
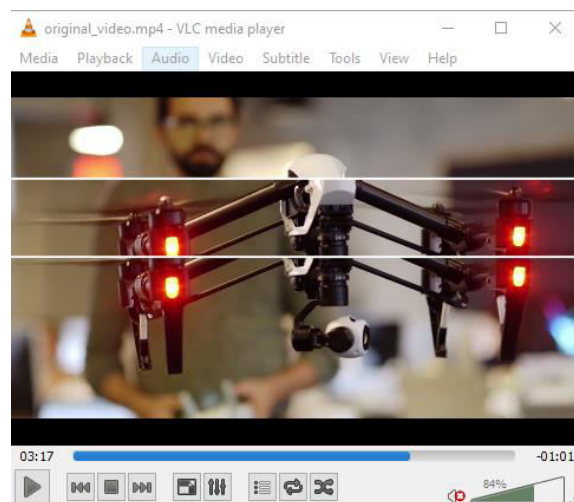
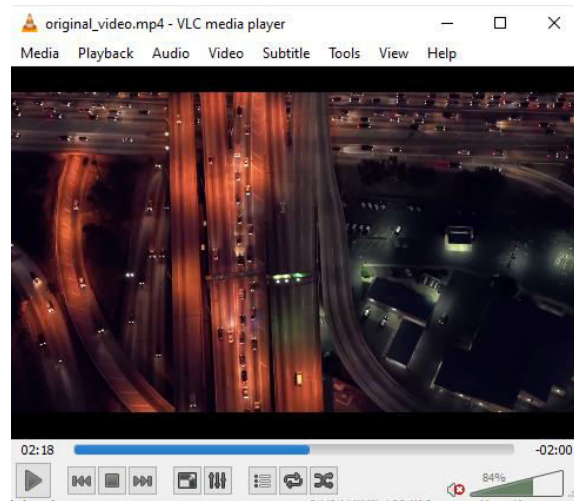
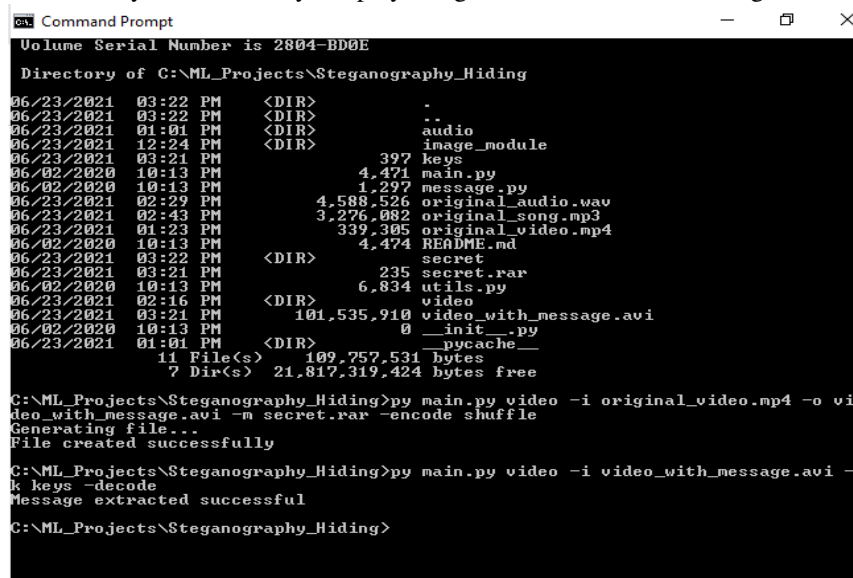


Fig 3 Sample Input Videos

Figure 3 shows the sample input videos which were used in this project. While giving input videos to the system, the secret message will also be given for encoding the videos. The system used the Shuffling method and creates the output videos with secret messages. This method also creates the secret key file while encoding the videos. Figure 4 shows the Encoding process with secret messages and Decoding process with secret key file. The system cannot process the encoded video without secret key file. Secret key file plays a significant role while encoding and decoding the videos.



```

C:\ML_Projects\Steganography_Hiding>dir
Volume Serial Number is 2804-BD0E
Directory of C:\ML_Projects\Steganography_Hiding
06/23/2021 03:22 PM <DIR> .
06/23/2021 03:22 PM <DIR> ..
06/23/2021 01:01 PM <DIR> audio
06/23/2021 12:24 PM <DIR> image_module
06/23/2021 03:21 PM 397 keys
06/02/2020 10:13 PM 4,471 main.py
06/02/2020 10:13 PM 1,297 message.py
06/23/2021 02:29 PM 4,588,526 original_audio.wav
06/23/2021 02:43 PM 3,276,082 original_song.mp3
06/23/2021 01:23 PM 339,305 original_video.mp4
06/02/2020 10:13 PM 4,474 README.md
06/23/2021 03:22 PM <DIR> secret
06/23/2021 03:21 PM 235 secret.rar
06/02/2020 10:13 PM 6,834 utils.py
06/23/2021 02:16 PM <DIR> video
06/23/2021 03:21 PM 101,535,910 video_with_message.avi
06/02/2020 10:13 PM 0 __init__.py
06/23/2021 01:01 PM <DIR> __pycache__
11 File(s) 109,757,531 bytes
7 Dir(s) 21,817,319,424 bytes free

C:\ML_Projects\Steganography_Hiding>py main.py video -i original_video.mp4 -o video_with_message.avi -m secret.rar -encode shuffle
Generating file...
File created successfully

C:\ML_Projects\Steganography_Hiding>py main.py video -i video_with_message.avi -k keys -decode
Message extracted successful

C:\ML_Projects\Steganography_Hiding>

```

Fig 4: Encoding and Decoding of input videos with secret messages

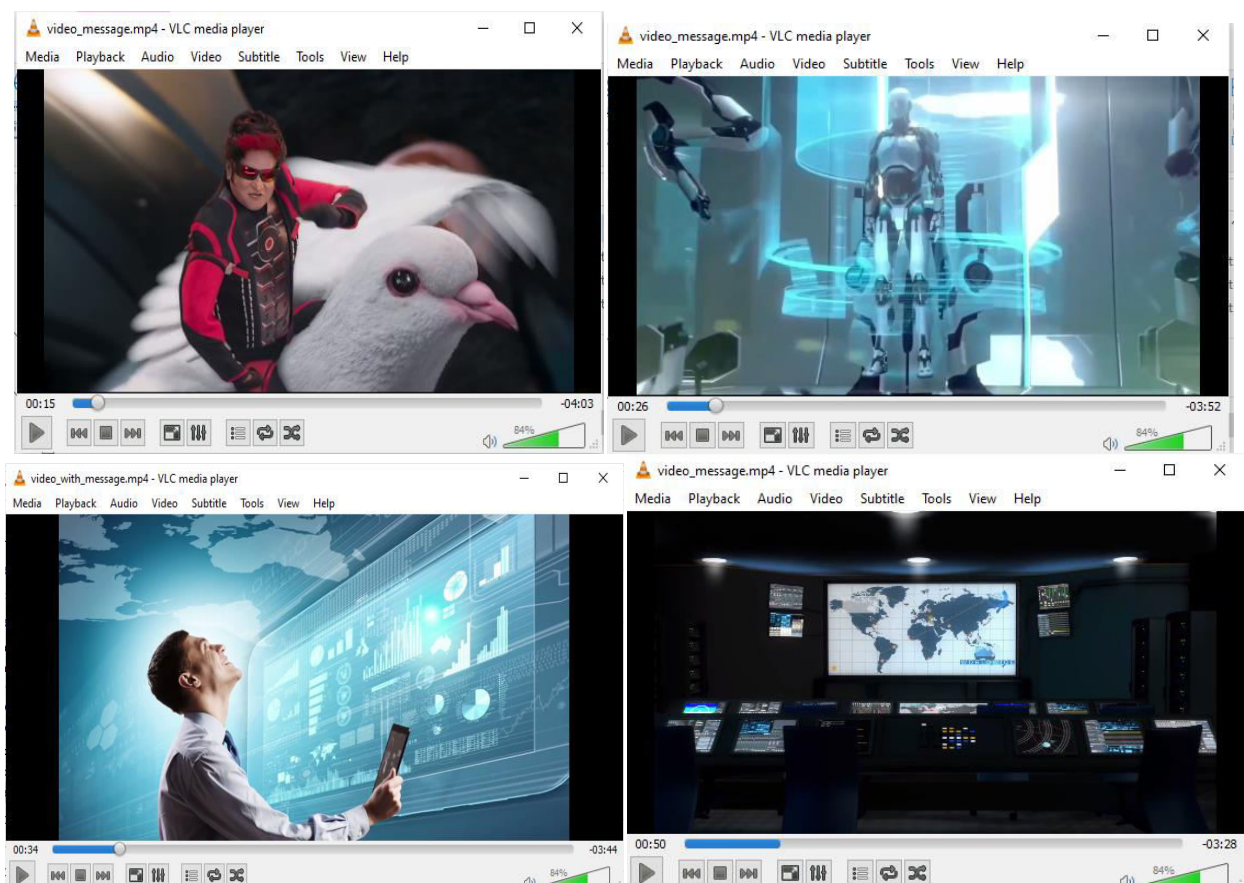


Fig 3 Sample Output Videos with Secret Message



V. CONCLUSION

In this work, we have proposed the video Steganography system. The proposed video steganography scheme consists of three components, including embedding, carrier bit streams transmitted, and extraction components. This system provides two levels of security such as cryptography and Steganography. The proposed system results in hiding the encrypted secret information into the video clips and generates secret key. Each frame hides 3-bits of data. The proposed system was tested by different size of videos and different size of secret message while encoding and decoding the video files. The proposed system shows that there is no noise has occurred in the encrypted videos. It was still similar to that of the original videos. While the decoding process, the encoded video has processed with the secret key. The existence of secret data is incredible to detect. Therefore the data can be transferred safely and securely to the destination. The DES algorithm with Shuffling method used to encrypt the videos. This method is simplest and common. However, it is an inefficient technique for encryption and to transfer data securely. In future work, it's anything but a key, which addresses a bunch of subjective qualities for choosing outlines and inserted picture or sound document inside a video, and it can be utilized as different techniques to choose pixels like the PMM (Pixel Mapping Method) and GLV (Gray level change) strategies.

ACKNOWLEDGMENT

We would like to thank our professor Dr. Prem Kumar sir, who supported & encouraged us to do research regarding our project. And also, we would like to thank our Department Head for giving us this opportunity.

REFERENCES

- 1) N. Subramanian *et al.*: "Image Steganography: A Review of the Recent Advances". vol.9, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3053998.
- 2) X.-L. Liu, C.-C. Lin and S.-M. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047_1055, May 2016.
- 3) M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2131_2153, Sep. 2017.
- 4) R. J. Mstafa and K. M. Elleithy, "Compressed and raw video Steganography techniques: A comprehensive survey and analysis," *Multimedia Tools Appl.*, vol. 76, no. 20, pp. 21749_21786, Oct. 2017.
- 5) R. J. Mstafa and K. M. Elleithy, "A video Steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimedia Tools Appl.*, vol. 75, no. 17, pp. 10311_10333, Sep. 2016.
- 6) R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A robust and secure video Steganography method in DWT-DCT domains based on multiple objects tracking and ECC," *IEEE Access*, vol. 5, pp. 5354_5365, Apr. 2017.
- 7) Y. Hu, C. Zhang, and Y. Su, "Information hiding based on intra prediction modes for H.264/AVC," in *Proc. IEEE Multimedia Expo Int. Conf.*, Beijing, China, Jul. 2007, pp. 1231_1234.
- 8) Y. Wang, Y. Cao, X. Zhao, Z. Xu, and M. Zhu, "Maintaining rate-distortion optimization for IPM-based video Steganography by constructing isolated channels in HEVC," in *Proc. 6th ACM Workshop Inf. Hiding Multimedia Secur.*, Innsbruck, Austria, Jun. 2018, pp. 97_107.
- 9) S. K. Kapotas and A. N. Skodras, "A new data hiding scheme for scene change detection in H.264 encoded video sequences," in *Proc. IEEE Int. Conf. Multimedia Expo*, Hannover, Germany, Jun. 2008, pp. 277_280.
- 10) H. Zhang, Y. Cao, X. Zhao, W. Zhang, and N. Yu, "Video Steganography with perturbed macro block partition," in *Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secure. (IHMMSec)*, Salzburg, Austria, Jun. 2014, pp. 115_122.
- 11) K. Sheik Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 10, pp. 1499_1512, Oct. 2009.
- 12) X. Ma, Z. Li, H. Tu, and B. Zhang, "A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 10, pp. 1320_1330, Oct. 2010.
- 13) P.-C. Chang, K.-L. Chung, J.-J. Chen, C.-H. Lin and T.-J. Lin, "A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames," *J. Vis. Common. Image Represent.* vol. 25, no. 2, pp. 239_253, Feb. 2014.
- 14) Forouzan BA, Mukhopadhyay D (2011) Cryptography and network security (Sie). McGraw-Hill Education, New York.
- 15) O. F. Abdel Wahab, A. I. Hussein, H. F. A. Hamed, and H. M. Kelash, "Hiding data in images using Steganography techniques with compression algorithms," *Telkomnika*, vol. 17, no. 3, pp. 1168_1175, 2019.



- 16) F. Adhanadi, L. Novamizanti, and G. Budiman, "DWT-SMM-based audio Steganography with RSA encryption and compressive sampling," *Telkom -nika*, vol. 18, no. 2, pp. 1095_1104, 2020.
- 17) E. Setyaningsih, R. Wardoyo, and A. K. Sari, "Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution," *Digit. Commun. Newt*, vol. 6, no. 4, pp. 486_503, Nov. 2020.
- 18) Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600_612, Apr. 2004.
- 19) M. Dehshiri, S. G. Sabouri, and A. Khorsandi, "Structural similarity assessment of an optical coherence tomography image enhanced using the wavelet transform technique," *J. Opt. Soc. Amer. An Opt. Image Sci.*, vol. 38, no. 1, pp. 1_9, 2021.
- 20) Li XW, Cho SJ, Kim ST (2014) A 3D image encryption technique using computer-generated integral imaging and cellular automata transform. *Opt Int J Light Electron Opt* 125(13):2983–2990.
- 21) Cao X, Wei X, Guo R, Wang C (2017) No embedding: a novel image cryptosystem for meaningful encryption. *J Vis Commun Image Represent* 44:236–249.
- 22) Mukesh Dalal & Mamta Juneja (2021): A secure video Steganography scheme using DWT based on object tracking, *Information Security Journal: A Global Perspective*, DOI: 10.1080/19393555.2021.1896055.
- 23) Y. Cao, H. Zhang, X. Zhao, and H. Yu, "Video Steganography based on optimized motion estimation perturbation," in *Proc. 3rd ACM Workshop Inf. Hiding Multimedia Secure. IH MM Sec*, Portland, OR, USA, 2015, pp. 25_31.
- 24) B. Zhu and J. Ni, "Uniform embedding for efficient Steganography of H.264 video," in *Proc. 25th IEEE Int. Conf. Image Process. (ICIP)*, Athens, Greece, Oct. 2018, pp. 1678_1682.



**Impact Factor:
7.569**



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details