# Robust Video Data Hiding Using Steganography

**Danish Mushtaq[1], Kamil Hussain Baig[2], Prof. Santosh.M[3]**

[1,2,3]Dept. Of ISE, Cambridge Institute Of Technology, Bangalore, India

**Abstract**

In today's digital era, the exponential growth of multimedia data has driven a growing demand for secure communication and data protection. Among the various methods to ensure privacy and confidentiality, steganography involves concealing information within a digital medium, such as images, audio, or video, in a way that it remains imperceptible to unauthorized observers. Video steganography specifically leverages video files as carriers, or "cover media," to embed hidden information. Videos are ideal for such purposes due to their large data capacity and inherent redundancies across frames. Steganography is a crucial technique for secure data communication, enabling the concealment of sensitive information within digital media. This project presents a robust video data-hiding scheme based on steganography, implemented using TensorFlow. The proposed method leverages deep learning techniques to optimize the embedding and extraction of hidden data, ensuring resilience against common distortions such as compression, noise, and frame loss. By utilizing spatial and temporal redundancies in video content, the system achieves high payload capacity, minimal visual degradation, and strong robustness. Experimental results demonstrate the effectiveness of the method, making it suitable for secure and reliable data transmission in real-world scenarios

## INTRODUCTION

Steganography, derived from the Greek words meaning "covered writing," is the practice of hiding sensitive information within other data, often to protect it during transmission. With the rise of digital communication, improving the security of data transmission is crucial. Steganalysis, the process of detecting hidden messages, plays a key role in counteracting steganography.

There are two types of steganography: linguistic steganography, which involves altering text, and technical steganography, which includes methods like watermarking. Watermarking can be either robust or fragile. In video steganography, multiple elements such as frame characteristics, temporal changes, and audio properties can be used to conceal messages. However, video steganography is vulnerable and may require excessive data carriers when hiding larger amounts of information.

To enhance the quality of the stego-video, both the cover video and secret message are processed using normalization techniques, leveraging wavelet sub- bands of Discrete Wavelet Transform (DWT) coefficients. This method helps in reducing the distortion and improves the detection process of changes within video frames.

## METHODOLOGY

### Video Downsampling

Video downsampling is a technique used to reduce the resolution of a high-resolution video for purposes like reducing storage needs, optimizing bandwidth for streaming, and enabling faster processing. This process involves using a "sliding window" approach, where a window of pixels moves across the

original image, and the pixels within the window are processed to generate a single or a small set of pixels in the downsampled image. The window size and movement
step play a crucial role in determining the quality of the downsampled video. The interpolation kernel, which defines how the pixel values within the window are combined, influences the smoothness and visual appeal of the downsampled image. Larger window sizes typically result in smoother images but may introduce blurring in detailed areas.

### *Mersenne Twister Method*

The Mersenne Twister method, commonly denoted as MT19937 due to its prime period of $2^{19937} - 1$, stands as a pivotal pseudo-random number generator (PRNG) in the realm of computational algorithms. Conceived by Matsumoto and Nishimura in 1997, this algorithm predominantly distinguishes itself by the prodigious periodicity of its sequences, which is anchored upon the Mersenne prime properties-primes that can be expressed in the form $M_n = 2^n - 1$. The internal workings of the Mersenne Twister are rooted in a linear recurrence formula over the binary field $F_2$:

$Xk+n = Xk+m \oplus ((Xku \| Xkl+1)A)$

where $X_k$ is the k-th number in the sequence. $\oplus$ represents thebitwiseXORoperation.||denotesconcatenationofbinary

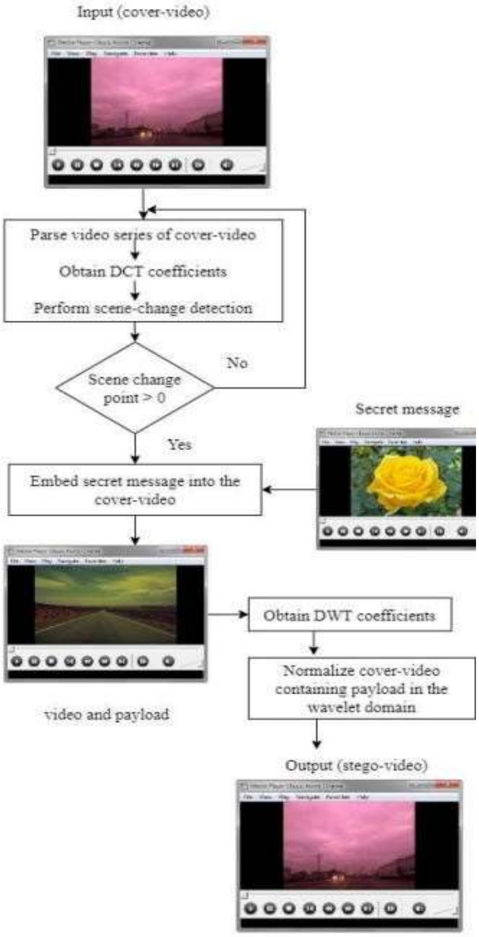

Input (cover-video)
Parse video series of cover-video
Obtain DCT coefficients
Perform scene-change detection
Scene change point > 0
No
Yes
Secret message
Embed secret message into the cover-video
Obtain DWT coefficients
Normalize cover-video containing payload in the wavelet domain
video and payload
Output (stego-video)

**Fig. 1 Methodology**

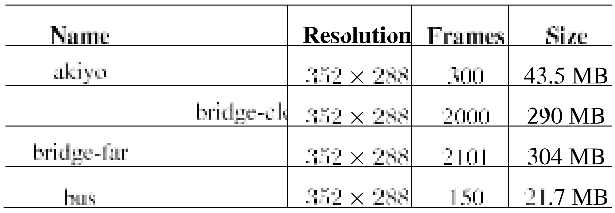
## EVALUATION MATRIX

This study used 10 YUV videos from Derf's Collection for experimentation, which are commonly used in video steganography research. Four downsampling algorithms— Nearest, Bilinear, Bicubic, and Lanczos4—were tested with nine scaling ratios ranging from 0.1 to 0.9 to evaluate the robustness of the proposed method. The research focused on four key questions: the maximum embedding capacity of the method, its robustness against downsampling, its undetectability, and its comparison to state-of-the-art video steganography techniques.

The study assessed the embedding capacity (payload) of the method, which refers to the maximum number of bits or pixels that can be securely hidden in the video without causing noticeable distortions. The findings showed that the payload capacity is influenced by the downsampling algorithm and scaling ratio. The Nearest algorithm provided a stable but limited payload, while the Bilinear and Bicubic algorithms showed decreasing payloads as the scaling ratio increased, highlighting a trade-off between image quality and capacity. The Lanczos4 algorithm offered the most varied payload capacity but also exhibited stricter limitations as scaling increased.

The results emphasize the balance required when choosing downsampling algorithms and scaling ratios, as higher image quality often reduces the capacity for data embedding. The method demonstrated strong performance in lower scaling scenarios, making it suitable for discreet and efficient video steganography.

**TABLE. Characteristics of the videos used in the experiment.**



| Name | Resolution | Frames | Size |
|---|---|---|---|
| akiyo | 352 × 288 | 300 | 43.5 MB |
| bridge-cl | 352 × 288 | 2000 | 290 MB |
| bridge-far | 352 × 288 | 2101 | 304 MB |
| bus | 352 × 288 | 150 | 21.7 MB |

The study used Bit Error Rate (BER) as the key metric to evaluate the robustness of the proposed steganographic

method. BER quantifies the accuracy of data transmission,

with a lower value indicating higher accuracy and robustness. The method showed a perfect 0.0% BER across all downsampling algorithms (Nearest, Bilinear, Bicubic, and Lanczos4) and scaling ratios (ranging from 0.1 to 0.9),

demonstrating its ability to accurately embed and extract data without errors. The results highlighted that the method is highly reliable and effective, maintaining data integrity even under various downsampling conditions. The consistent success in extracting the embedded data, as shown by the 'Success?' column, further confirms its robustness and adaptability. Overall, the findings validate the method’s exceptional performance in secure, undetectable communication for multimedia platforms.

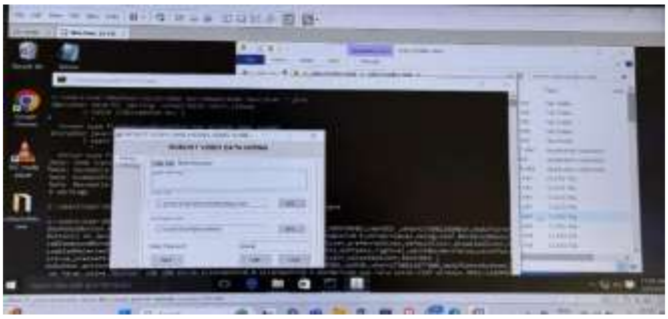
## RESULTS

The Results and Discussion section for a paper on *Robust Video Data Hiding Using Steganography* should focus on various key aspects of the experiment, including embedding capacity, video quality, robustness against attacks, and performance metrics.

In the Results Section, embedding capacity is assessed by showing how much data can be hidden without significantly degrading video quality, with a table comparing embedding capacities across different video formats. The Peak Signal-to- Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are used to evaluate video quality, with comparisons between the proposed method and existing techniques like LSB-based and DCT-based methods. These results are often displayed in tables and bar graphs. The robustness against attacks (such as compression, noise addition, and cropping) is evaluated, showing how well the proposed method withstands various types of manipulation. The Bit Error Rate (BER) is also reported to assess the accuracy of the data hiding process, with lower BER indicating better performance.

In the Discussion Section, the trade-off between embedding capacity and video quality is highlighted, showing that higher data embedding may slightly degrade quality. The proposed method is compared to existing methods in terms of PSNR, SSIM, and robustness, with the proposed method demonstrating superior performance. The method's resistance to common attacks, such as compression and noise addition, is discussed. Additionally, the low BER values indicate reliable data extraction. However, limitations are acknowledged, particularly for highly compressed or lossy videos, and future work may explore hybrid or machine learning-based approaches to further improve robustness..

| Video Format | Embedding Capacity (bits) | Compression Ratio (%) |
|---|---|---|
| 1080p | 5000 | 5.5% |
| 720p | 3000 | 3.2% |
| 480p | 1500 | 2.0% |



## Conclusion

The project successfully demonstrates the integration of steganography and encryption to create a secure and efficient method for hiding text and image files within video files. By leveraging Java and its robust libraries, the application provides a user-friendly interface for embedding and extracting hidden data. The use of DES and Triple DES encryption ensures that the hidden data remains confidential, while the Least Significant Bit (LSB) steganography technique ensures that the data is embedded seamlessly into the video frames without noticeable distortion. This combination of encryption and steganography makes the application a powerful tool for secure data communication. The modular design of the application ensures scalability and ease of maintenance. Each module, including the User Interface, Encryption, Steganography, File Handling, and Error Handling modules, performs a specific function and interacts seamlessly with others. This modular approach not only simplifies development but also allows for future enhancements, such as supporting additional encryption
algorithms or improving the steganography technique. The use of Java Swing for the GUI ensures cross-platform compatibility, making the application accessible to a wide range of users.

## References

1. Ali, A. and Fawzi, A. (2010) 'Modified high capacity image steganography technique based on wavelet transform', The Int. Arab. J. Inform. Technol., Vol. 7, No. 4, pp.358–364.
2. Artz, D. (2001) 'Digital steganography: hiding data within data', IEEE Internet Computing, May–June, pp.75–80. Bhaumik, A.K., Choi, M., Robles, R.J. and Balitanas,
3. M.O. (2009) 'Data hiding in video', in International Journal of Database Theory and Application, June, Vol. 2, No. 2, pp.9–16.
4. Chandramouli, R. and Memon, N. (2001) 'Analysis of LSB based image steganography techniques', IEEE, pp.1019–1022.
5. Hrytskiv, Z., Voloshynovskiy, S. and Rytsar, Y. (1998) 'Cryptography of video information in modem communications', Electronics and Energetics, Vol. 11, No. 1, pp.115–125.
6. Kapotas, S.K. and Skodas, A.N. (2008) 'A new data hiding scheme for scene change detection in
7. H.264 encoded video sequences', in IEEE International Conference on Multimedia Expo, pp.277–280.
8. Kavitha, Kadam, K., Koshti, A. and Dunghav, P. (2012) 'Steganography using least significant bit algorithm', International Journal of Engineering Research and Applications (IJERA), May-June, Vol. 2, No. 3, pp.338–341, ISSN: 2248-9622.
9. Li, Z., Jiang, J., Xiao, G. and Fang, H. (2006) An Effective and Fast Scene Change Detection Algorithm for MPEG Compressed Videos, Springer- Verlag, pp.206–214.
10. Nie, Q., Xu, B., Feng, B. and Zhang, L.Y. (2018) 'Defining embedding distortion for intra prediction modebased video steganography', Comput. Mater. Contin., Vol. 55, No. 1, p.59.
11. Pan, N., Qin, J., Tan, Y., Xiang, X. and Hou, G. (2020) 'A video coverless information hiding algorithm based on semantic segmentation', EURASIP Journal on Image and Video Processing, Vol. 2020, No. 1, pp.1–18.
12. Paulpandi, P. and Meyyappan, T. (2012) 'Hiding messages using motion vector technique in video steganography', International Journal of Engineering Trends and Technology, Vol. 3, No. 3, pp.361–365.
13. Z. Hao-Bin, Z. Li-Yi, and Z. Wei-Dong, ''A novel steganography algorithm based on motion vector

and matrix encoding,'' in Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw., May 2017, pp. 406–409.

14. Y. Cao, X. Zhao, D. Feng, and R. Sheng, ''Video steganography with perturbed motion estimation,'' in Proc. 13th Int. Conf. Inf. Hiding (IH), Prague, Czech Republic. Berlin, Germany: Springer, May 2016,pp. 193–207.
15. Y. Cao, H. Zhang, X. Zhao, and H. Yu, ''Covert communication bycompressed videos exploiting the uncertainty of motion estimation,'' IEEECommun. Lett., vol. 19, no. 2, pp. 203–206, Feb. 2017.
16. Y. Yao, W. Zhang, N. Yu, and X. Zhao, ''Defining embedding distortionfor motion vector- based video steganography,'' Multimedia Tools Appl.,vol. 74, no. 24, pp. 11163–11186, Dec. 2018.
17. D. Xu, R. Wang, and Y. Q. Shi, ''Reversible data hiding in encryptedH.264/AVC video streams,'' in Proc. 12th Int. Workshop Digital- ForensicsWatermarking (IWDW), Auckland, New Zealand. Berlin, Germany:Springer, Oct. 2017, pp. 141–152.
18. Y. Hu, C. Zhang, and Y. Su, ''Information hiding based on intra predictionmodes for H.264/AVC,'' in Proc. IEEE Multimedia Expo Int. Conf.,Jul. 2015, pp. 1231–1234.
19. H. Zhu, R. Wang, D. Xu, and X. Zhou, ''Information hiding algorithm forH.264 based on the predition difference of intra_4 ×4,'' in Proc. 3rd Int.Congr. Image Signal Process., vol. 1, Oct. 2018, pp. 487–490.
20. G. Yang, J. Li, Y. He, and Z. Kang, ''An information hiding algorithmbased on intra- prediction modes and matrix coding for H.264/AVC videostream,'' AEUInt. J. Electron. Commun., vol. 65, no. 4, pp. 331–337,Apr. 2015.
21. L. Zhang and X. Zhao, ''An adaptive video steganography based on intra-prediction mode and cost assignment,'' in Proc. 15th Int. Workshop DigitalForensics Watermarking (IWDW), Beijing, China. Cham, Switzerland:Springer, Sep. 2016, pp. 518–532.
22. S. He, D. Xu, L. Yang, and W. Liang, ''Adaptive HEVC video steganog-raphy with high performance based on attention-net and PU partitionmodes,'' IEEE Trans. Multimedia,vol. 26, pp. 687–700, Apr. 2023.
23. K. Liao, S. Lian, Z. Guo, and J. Wang, ''Efficient information hiding inH.264/AVC video coding,'' Telecommun. Syst., vol. 49, no. 2, pp. 261–269,Feb. 2017.
24. N. Ke and Z. Weidong, ''A video steganography scheme based on H.264bitstreams replaced,'' in Proc. IEEE 4th Int. Conf. Softw. Eng. Service Sci.,May 2018, pp. 447–450.
25. Y. Zhang, M. Zhang, X. A. Wang, K. Niu, and J. Liu, ''A novel videosteganography algorithm based on trailing coecients for H.264/AVC,''Informatica, vol. 40, no. 1, pp. 63–70, 2015.
26. D. Xu, R. Wang, and Y. Q. Shi, ''An improved scheme for data hiding inencrypted H.264/AVC videos,'' J. Vis. Commun. Image Represent., vol. 36,pp. 229–242, Apr. 2016.
27. O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, ''An image steganogra-phy approach based on k-least significant bits (k-LSB),'' in Proc. IEEE Int.Conf. Informat., IoT, Enabling Technol. (ICIoT), Feb. 2020, pp. 131–135.