

## A hybrid video steganography technique integrating Knight's Tour Algorithm with 7th-Bit Plane Insertion

Sharath M N \*, Suresha D and Praveen B M

*Department of Computer Science & Engineering, Institute of Engineering & Technology, Srinivas University, Mukka, Mangaluru-574146, Karnataka, India.*

Global Journal of Engineering and Technology Advances, 2026, 27(03), 183–196

Publication history: Received on 10 May 2026; revised on 18 June 2026; accepted on 20 June 2026

Article DOI: <https://doi.org/10.30574/gjeta.2026.27.3.0163>

### Abstract

Video steganography is an effective technique for secure communication that hides confidential information within video files without noticeable visual changes. This paper presents a novel video steganography method that combines the Knight Tour algorithm with a 7th-bit embedding strategy. The Knight Tour algorithm selects embedding locations in a random and unpredictable manner, improving security against unauthorized access. Secret data is embedded using the 7th bit of the selected pixel and its adjacent pixel, ensuring efficient data hiding while preserving video quality. The performance of the proposed method is evaluated using PSNR, MSE, SSIM, and embedding capacity metrics. Experimental results show that the technique achieves high imperceptibility, improved robustness, and increased payload capacity compared to conventional video steganography methods.

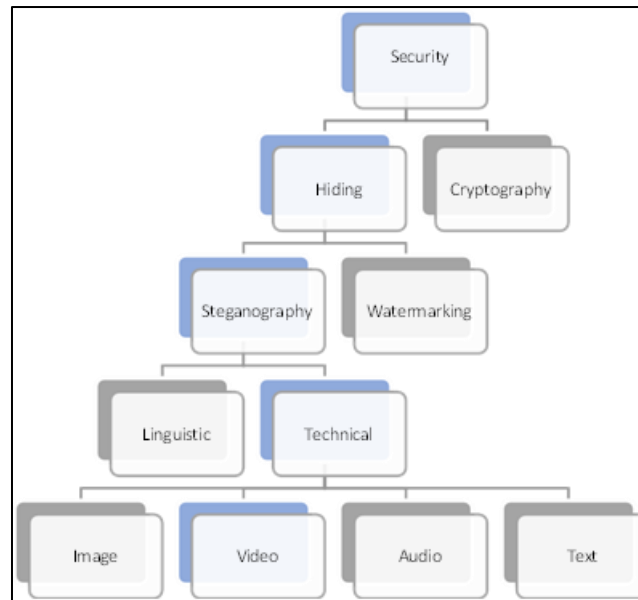
**Keywords:** Video Steganography; Knight Tour Algorithm; 7th-Bit Embedding; Information Hiding; PSNR; SSIM; Robustness.

### 1. Introduction

In the digital era, information has become one of the most valuable resources. As the volume of data exchanged through communication networks continues to grow, protecting sensitive information from unauthorized access has become increasingly important. Information security plays a vital role in ensuring confidentiality, integrity, and availability of data. Although several security mechanisms have been developed, there is still a need for improved techniques that provide stronger protection while maintaining efficiency. Information security approaches can generally be categorized into two major groups: **cryptography** and **information hiding**. Cryptography protects data by converting it into an unreadable format using encryption algorithms and secret keys. Only authorized users possessing the correct decryption key can recover the original information.

The figure indicates the classification of security systems.

\* Corresponding author: Sharath M N.



**Figure 1** Classification of Security Systems

In contrast, **steganography** focuses on concealing the existence of secret information. Instead of transforming the message into an unreadable form, steganography hides the message within a cover medium such as an image, audio file, text document, or video. The primary objective is to ensure that observers cannot detect the presence of hidden communication. This characteristic makes steganography an effective tool for secure data transmission. Among various steganographic techniques, **video steganography** has attracted significant attention because videos provide a large amount of redundant data and consist of multiple frames that can be utilized for information embedding. The extensive use of video-sharing platforms, streaming services, and multimedia communication systems has further increased the demand for secure video-based information hiding techniques. Applications of video steganography include secure communication, military data exchange, medical information protection, digital rights management, and law enforcement operations.

**Imperceptibility:** Imperceptibility refers to the ability of the steganographic system to conceal information without producing visible changes in the cover video. The embedded video should appear identical to the original video so that the hidden communication remains undetectable to human observers and statistical analysis methods.

**Robustness:** Robustness indicates the capability of the hidden information to withstand intentional attacks and common video processing operations such as compression, scaling, frame manipulation, transmission noise, and format conversion. A robust steganographic scheme ensures reliable recovery of the embedded message even under adverse conditions.

### 1.1. Embedding Capacity

Embedding capacity represents the amount of secret data that can be hidden within the cover video. Higher capacity enables larger messages to be embedded; however, excessive embedding may degrade visual quality and increase the risk of detection. Therefore, an effective steganographic technique must achieve a balance between capacity, security, and visual quality. Numerous video steganography methods have been proposed in recent years. However, many existing approaches either offer limited payload capacity, reduced robustness, or increased computational complexity. To address these limitations, this work proposes a novel video steganography technique that combines the **Knight Tour algorithm** for secure pixel selection and the **7th-bit embedding model** for data hiding. The integration of these two mechanisms enhances security, increases embedding efficiency, and preserves the visual quality of the stego video.

## 2. Related works

Video steganography has become an active research area due to the increasing demand for secure multimedia communication. Researchers have proposed numerous techniques for concealing confidential information within digital media while attempting to maintain visual quality, robustness, and payload capacity.

One of the earliest and most widely adopted methods is the **Least Significant Bit (LSB) substitution technique**. In this approach, secret data bits are embedded into the least significant bits of pixel values. Because modifications occur in the lowest-order bits, the visual distortion introduced into the cover media is minimal. However, the predictable nature of LSB embedding makes it vulnerable to statistical attacks and steganalysis techniques.

To overcome the weaknesses of conventional LSB methods, several enhanced embedding schemes have been proposed. Moderately Significant Bit (MSB)-based approaches embed information in higher-order bit positions to improve hiding efficiency. Some methods also incorporate pixel adjustment mechanisms to reduce distortion after embedding. Although these techniques improve embedding performance, they often fail to achieve an optimal balance between visual quality and payload capacity.

Histogram-based data hiding methods have also attracted attention. These techniques utilize histogram modification and histogram shifting strategies to embed secret information while preserving image quality. By manipulating histogram characteristics, researchers have achieved improved embedding capacity and reduced distortion. Nevertheless, the computational complexity of these methods increases significantly as the size of multimedia content grows.

Another important category is **transform-domain steganography**, where secret information is embedded after transforming the media into another representation. Common transformations include the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Fourier Transform, and Integer Wavelet Transform (IWT). These methods generally provide better robustness against compression and signal-processing attacks. However, transform-domain approaches often require additional computational resources and more complex embedding procedures.

Wavelet-based techniques have been extensively explored because of their ability to preserve visual quality while providing secure embedding. Researchers have proposed embedding schemes using DWT and IWT coefficients to increase hiding capacity and improve resistance to attacks. Although these methods produce satisfactory results, the computational overhead associated with transformation and inverse transformation processes remains a challenge.

In compressed video environments, several studies have focused on embedding information within motion vectors, prediction errors, and frame structures. These approaches exploit temporal redundancy in video sequences to hide data efficiently. Multiple-group-picture techniques and frame-based embedding strategies have also been investigated to improve payload capacity and security. Despite these advancements, maintaining robustness during compression and transmission continues to be a difficult task.

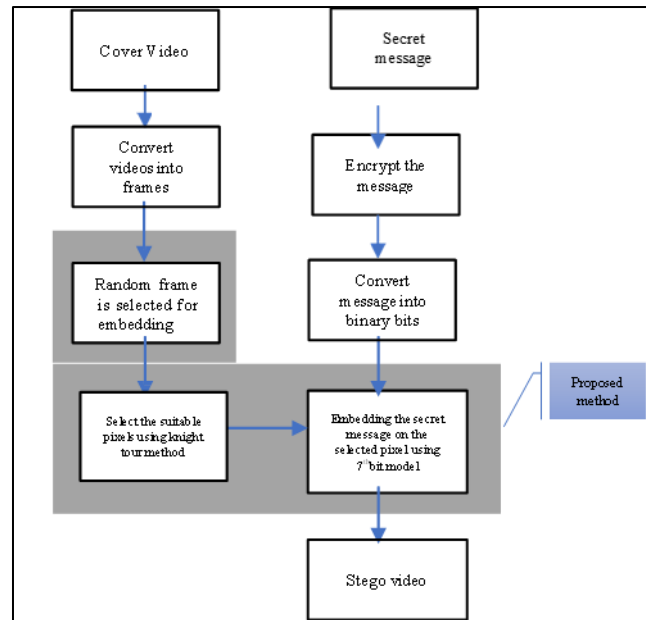
Recent studies have introduced intelligent pixel-selection mechanisms to strengthen security. Instead of embedding data sequentially, these approaches use randomized algorithms to determine embedding locations. Randomized embedding significantly increases the difficulty for attackers attempting to locate hidden information. Among such methods, the Knight Tour algorithm has shown promising results by providing a large search space and non-linear traversal patterns.

Despite the considerable progress achieved in video steganography, several challenges remain unresolved. Many existing techniques suffer from one or more limitations, including low embedding capacity, reduced robustness against attacks, increased computational complexity, or degradation of visual quality. Furthermore, some methods utilize all frames uniformly without considering intelligent frame selection, which may negatively affect the imperceptibility of the stego video.

To address these limitations, this work proposes a video steganography framework that combines random frame selection, Knight Tour-based pixel traversal, and a 7th-bit embedding mechanism. The proposed approach aims to enhance security, increase embedding capacity, improve robustness, and preserve the visual quality of the stego video.

## 2.1. Proposed method

The final aim of video steganography is to hide the data without affecting the data quality and to do it with utmost secrecy. The proposed model will ensure that the elements of invisibility, robustness, and capacity of embedding are achieved, and these are the essential aspects of steganographic technology. The first step in the process is the creation of the message that is to be hidden.



**Figure 2** Proposed Architecture of Video Steganography

## 2.2. Selection of frames:

In this method, the initial process of video steganography involves selecting frames where the hidden data can be embedded. The algorithm used in the selection of frames consists of a pseudo-random generator (PRG), where random selection of frames occurs from the range of 0th to 20th frames without any frame duplication [25].

Let us assume the range for generating the frame using the pseudo-random generator (PRG) is ' $n$ '. The seed could be provided by the equation  $x_1 + x_2 + x_3$  and the feedback equation would be  $(x_2 + x_3)dn$

## 2.3. Embedding process

Position based secret message embedding technique involves choosing the pixel position and embedding the secret information in that pixel position. The pixel position based embedding technique in which encoding the secret message is done through the knight tour algorithm, while the information hiding process is done through the seventh bit of the selected pixel and the next pixel value.

## 2.4. Knight tour algorithm.

As opposed to the conventional approach for choosing the pixel location which involves serial selection, it becomes imperative to choose the pixel randomly. This is done through the knight tour algorithm which uses the concept of randomness inspired by the knight of the chessboard [26]. The selected frame will be considered as a chessboard for this knight to play its tricks.

The algorithm involves partitioning the board into blocks. The  $n \times n$  chessboard consists of all positions being moved to by the knight only once, as shown in Figure. This method enables enhanced security than PRNG because the search space involved is larger.

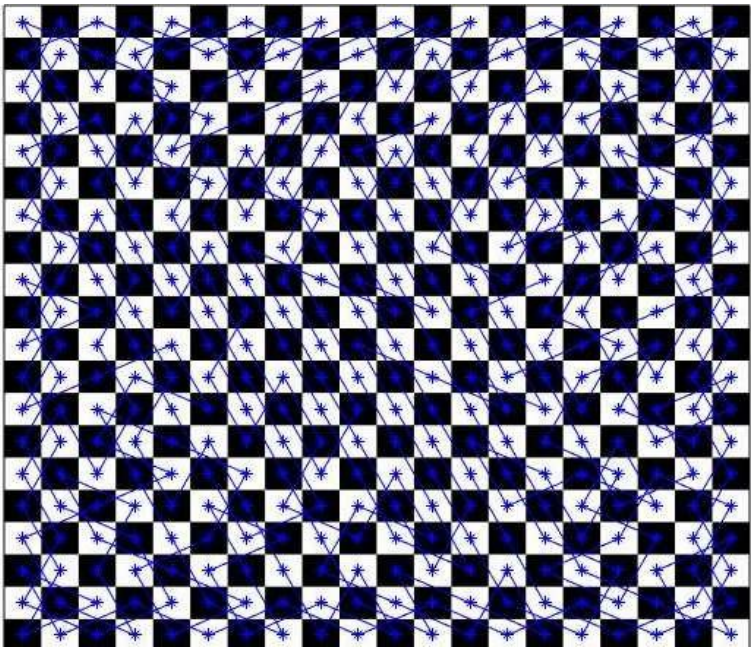


Figure 3 20 x 20 chessboard knight tour travel

According to our algorithm, the use of the chessboard of dimension 20 x 20 helps in ensuring security through an increase in the size of the search area within the video. Moreover, for the coverage of all the pixels, the size must be multiple of 4. Table below represents the pixel traversing of 20 x 20 matrix.

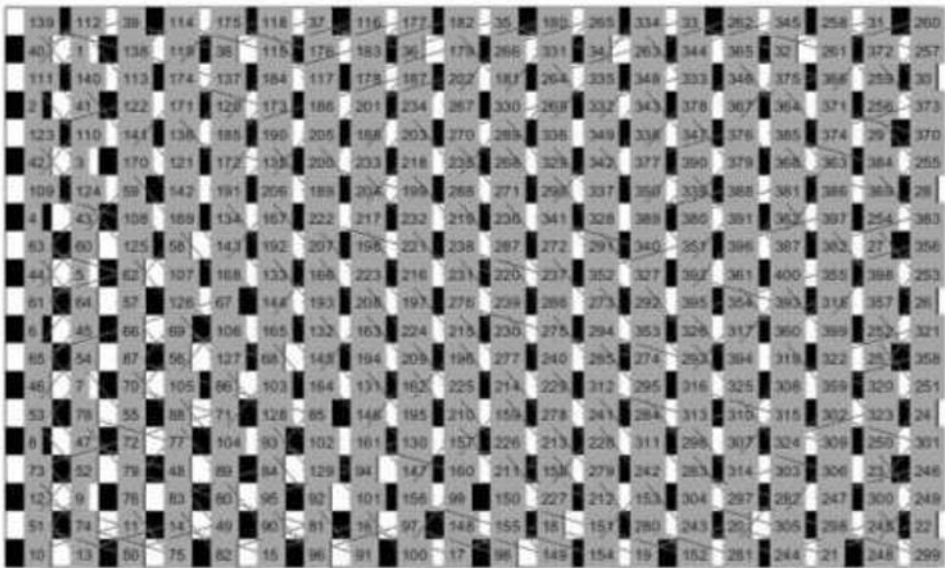
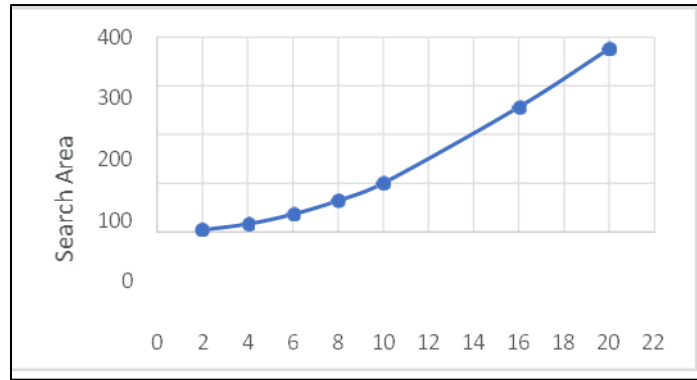


Figure 4 Pixel Traversing of a 20 x 20 chessboard matrix

The below graph shows the search area required for the intruders to access the secret message based on the chessboard size.



**Figure 5** Comparative analysis – Chessboard size vs Search Area

### 2.5. 7<sup>th</sup> bit model:

Under the 7<sup>th</sup> bit scheme for encoding of the secret message, the mathematical formula is used on the 7<sup>th</sup> bit of the recognized pixel ( $p$ ) and its adjacent pixel value ( $p+1$ ), leading to formation of the 2-bit pair value. This process enables combinations of the bits 00, 01, 10 and 11 to be formed. In this way, the 2 bit of the message can be encoded in each pixel.

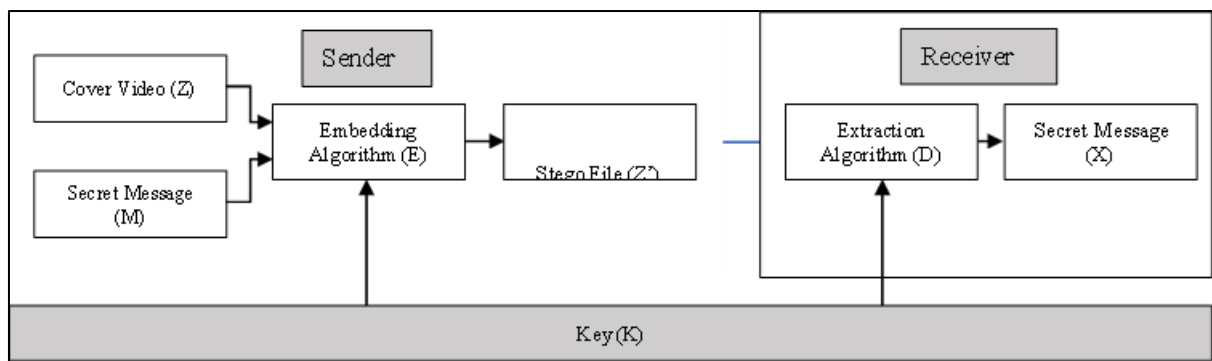
If  $C$  is the cover image with a size of  $H * W$  pixels, the  $M$  is the  $N$ -bit hidden message,  $x$  is the pixel value and the  $m$  is the secret message bit, and then image matrix can be interpreted as,

$$C = \{x_{ij} \mid 1 \leq i \leq H, 1 \leq j \leq W, x \in \{0, 1, \dots, 255\}\} \quad (1)$$

The secret message can be represented as,

$$M = \{m_N \mid 1 \leq N \leq n, m_N \in \{0, 1\}\} \quad (2)$$

Let  $M$  is the secret message,  $Z$  is the cover video,  $K$  is the key that can be utilized for embedding ( $E$ ) and extraction of the message, ( $D$ ) and  $Z'$  is the stego file.



**Figure 6** Block diagram of Video Steganography

The embedding of a secret message in the cover file is done using the following equation:

$$Z' = EK(M, Z) \quad (3)$$

$EK$  refers to the embedding algorithm that hides the secret data ( $M$ ) within the cover file ( $Z$ ). This process will be shown below with an example.

While the extraction process, whereby the message is extracted from the cover, is done as follows.

$$X = DK(Z') \quad (4)$$

In the same way, the DK algorithm is used for extracting the hidden secret message back into its original form by means of the secret key (k), which is known to both sender and receiver. The above-discussed DK extraction algorithm has been described appropriately through an illustration.

Consider the character 'd' should be sent as a secret message.

The binary equivalent of the secret message 'd' is {01 10 01 00}, and the four-pixel values selected using knight tour method are  $p = \{78, 35, 68, 98\}$ .

*At the embedding side:*

*Pixel 1:*

$P1 = 78(01001110),$

$P1 + 1 = 79(01001111).$

The 7<sup>th</sup> bits of P1 and P1+1 form the "11" pair, but the original two message bits to introduce are "01." Thus, we must apply -1 to the P1 value. Therefore,

$P1' = 77(78 - 1)$

where P1' is the stego pixel.

Similarly, the bit pairs are embedded in the cover file.

**Table 1** Embedding of secret bits using 7th bit model

|                       | Pixel value        | Binary value | 7th bit pair | Secret message bit | Additional factor | Stego pixel value |
|-----------------------|--------------------|--------------|--------------|--------------------|-------------------|-------------------|
| 1 <sup>st</sup> Pixel | 78                 | 010011 1 0   | 11           | 01                 | -1                | 77                |
|                       | 79(pixel value +1) | 010011 1 1   |              |                    |                   |                   |
| 2 <sup>nd</sup> Pixel | 35                 | 001000 1 1   | 10           | 10                 | 0                 | 35                |
|                       | 36                 | 001001 0 0   |              |                    |                   |                   |
| 3 <sup>rd</sup> Pixel | 68                 | 010001 0 0   | 00           | 01                 | +1                | 69                |
|                       | 69                 | 010001 0 1   |              |                    |                   |                   |
| 4 <sup>th</sup> Pixel | 98                 | 011000 1 0   | 11           | 00                 | +2                | 100               |
|                       | 99                 | 011000 1 1   |              |                    |                   |                   |

*At the extraction side*

The set of stego pixels to be extracted to retrieve the secret message are {77, 35, 69, 100}.

*Pixel 1:*

$P1' = 77(010011 0 1),$

$P1' + 1 = 78(010011 1 0),$

The secret message bit at this pixel is 01

*Pixel 2:*

$$P2' = 35(001000 \mathbf{1} \ 1),$$

$$P2' + 1 = 36(001001 \mathbf{0} \ 0).$$

The secret message bit at this pixel is 10

*Pixel 3:*

$$P3' = 69(010001 \mathbf{0} \ 1).$$

$$P3' + 1 = 70(010001 \mathbf{1} \ 0).$$

The secret message bit at this pixel is 01

*Pixel 4:*

$$P4' = 100(011001 \mathbf{0} \ 0).$$

$$P4' + 1 = 101(011001 \mathbf{0} \ 1).$$

The secret message bit at this pixel is 00

Consequently, the concealed message becomes 01 10 01 00.

As a result, the combination of the knight tour technique and the concealment technique using the 7th bit technique becomes very effective. This technique manages to achieve invisibility with its high searching capability as well as its unreliability of the least significant bit. The knight tour technique helps increase the capacity of embedding through increasing the board size.

---

### 3. Result and Discussion

The proposed method for video steganography technique was tested with varying data sets and analyzed based on factors like peak signal-to-noise ratio (PSNR), mean squared error (MSE), structural similarity index (SSIM), and embedding capacity.

PSNR is an image quality measurement in statistics between the real and processed/reconstructed image. The greater the PSNR, the better the image quality [28].

Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) are two important picture quality metrics used in empirical computation of stego file quality. MSE is the sum of square differences between stego file and real file.

$$PSNR = 20\log_{10}$$

$$\left( \frac{\max f}{\sqrt{MSE1}} \right) \quad (5)$$

$$\sqrt{MSE1}$$

$$MSE =$$

$$mnm-1 \ n-1$$

$$\sum_{i=0}^m \sum_{j=0}^n \| (i,j) - c'(i,j) \|^2 \quad (6)$$

$$0 \quad 0$$

where,  $c$  is the cover file,  $c'$  is the stego file of size  $m \times n$  and  $\max f$  is the maximum signal value in the cover file.

The SSIM is basically a measurement of visual similarity between two pictures. The SSIM was developed by Wang et al [29] to analyze the uniformity of human visual system (HVS).

The classification of SSIM is done according to the integration of three parameters namely correlation loss, luminance distortion, and contrast distortion unlike other error measuring techniques. SSIM is formulated as:

$$SSIM = (c, c'), (c, c'), s(c, c') \quad (7)$$

$$(c, c') = \frac{2\mu_c \mu_{c'} + K1}{\mu_c^2 + \mu_{c'}^2 + K1}$$

$$\mu_c^2 + \mu_{c'}^2 + K1$$

$$c \quad c'$$

$$\text{where, } (c, c') = \frac{2\sigma_c \sigma_{c'} + K2}{\sigma_c^2 + \sigma_{c'}^2 + K2}$$

$$\sigma_c^2 + \sigma_{c'}^2 + K2$$

$$c \quad c'$$

$$(c, c') = \frac{cc' + K3}{\sigma_c \sigma_{c'} + K3}$$

In the above mentioned formula,  $l(c, c')$  is luminance comparison between cover image  $c$  and the stego file  $c'$ . Here  $c(c, c')$  is the contrast comparison and  $s(c, c')$  is the structure comparison. The symbols  $K1$ ,  $K2$  and  $K3$  are the positive constants which help to prevent the null denominator.

The performance analysis of the proposed method is tabulated below,

**Table 2** Performance analysis – MSE, PSNR, SSIM, Time

| Cover Video | PSNR  | MSE   | SSIM (%) | Time (sec) |
|-------------|-------|-------|----------|------------|
| Video_1     | 84.86 | 0.213 | 100      | 0.133      |
| Video_2     | 83.77 | 0.274 | 100      | 0.166      |
| Video_3     | 85.53 | 0.183 | 100      | 0.136      |

Various video steganography techniques are analysed and compared with respect to PSNR in the table below,

**Table 3** Comparative analysis –PSNR

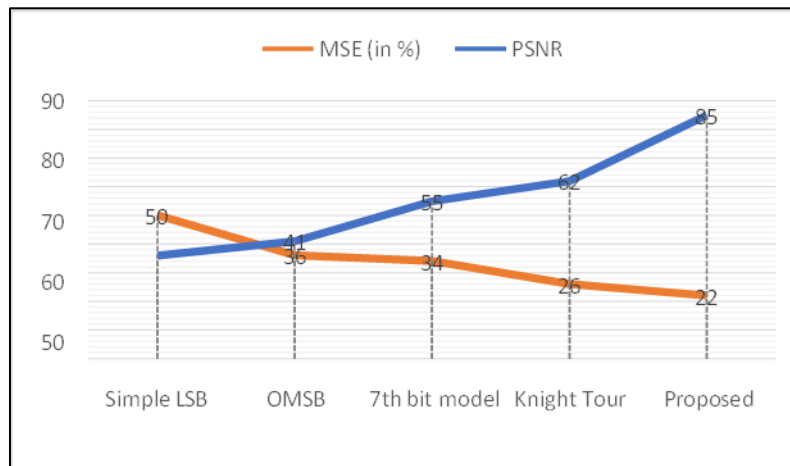
| Cover Video | Simple LSB [12] | OMSB [14] | 7th bit model [27] | Knight tour [26] | Proposed Method |
|-------------|-----------------|-----------|--------------------|------------------|-----------------|
| Video_1     | 37.8642         | 42.353    | 55.401             | 66.525           | 84.864          |
| Video_2     | 31.3307         | 41.756    | 55.418             | 62.448           | 83.773          |
| Video_3     | 38.7242         | 43.156    | 55.477             | 59.904           | 85.532          |

Similarly, the MSE values are compared in the table below,

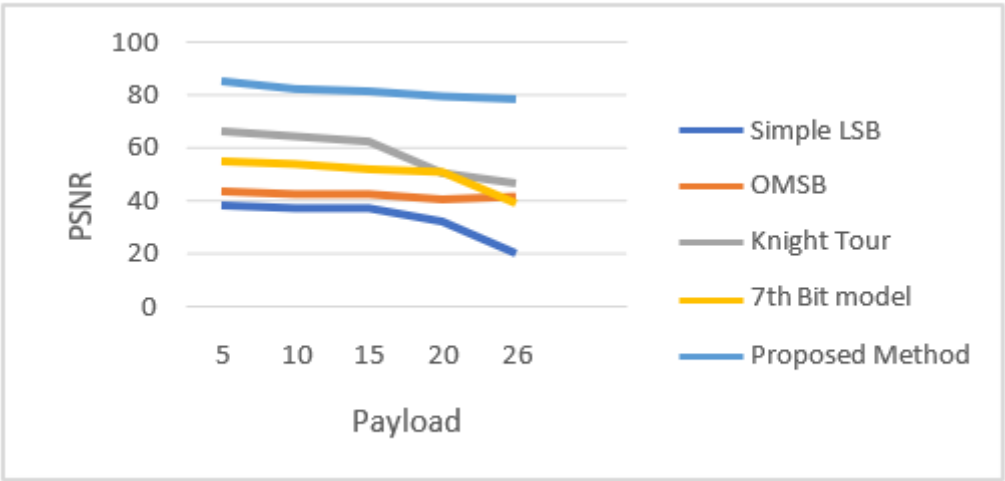
**Table 4** Comparative analysis –MSE

| Cover Video | Simple LSB [12] | OMSB [14] | 7th bit model [27] | Knight tour [26] | Proposed Method |
|-------------|-----------------|-----------|--------------------|------------------|-----------------|
| Video_1     | 0.578           | 0.318     | 0.374              | 0.277            | 0.213           |
| Video_2     | 0.489           | 0.415     | 0.365              | 0.289            | 0.274           |
| Video_3     | 0.536           | 0.378     | 0.326              | 0.227            | 0.183           |

The graph shown below, clearly compares the PSNR and MSE values of the proposed method with other methods.

**Figure 7** MSE, PSNR plot using the proposed method and other techniques

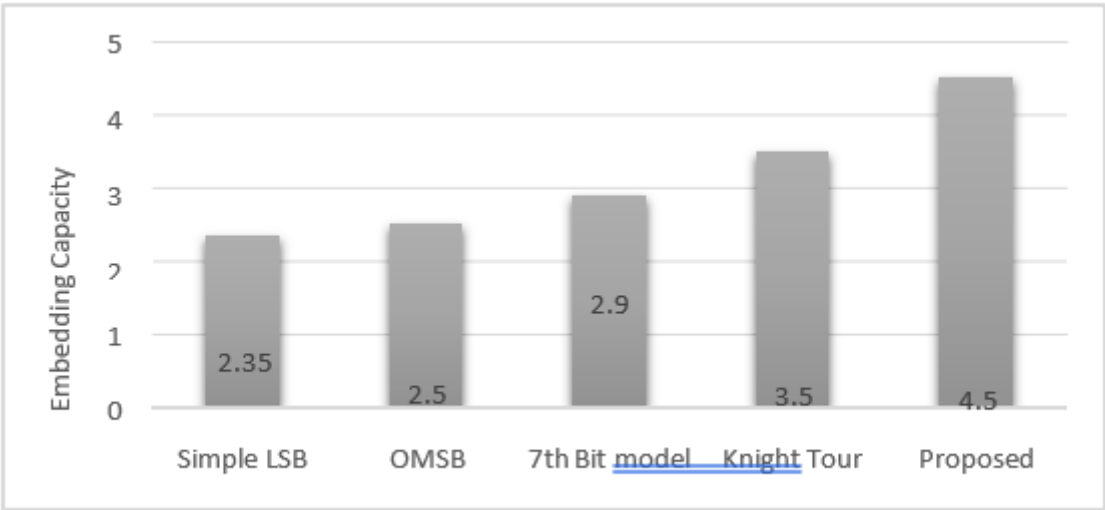
The payload is based on the size of the message contained within the cover video. Below is the graph comparing the effect of the payload in PSNR values for different video steganography methods and the proposed approach.



**Figure 8** Payload vs PSNR for proposed method and other techniques

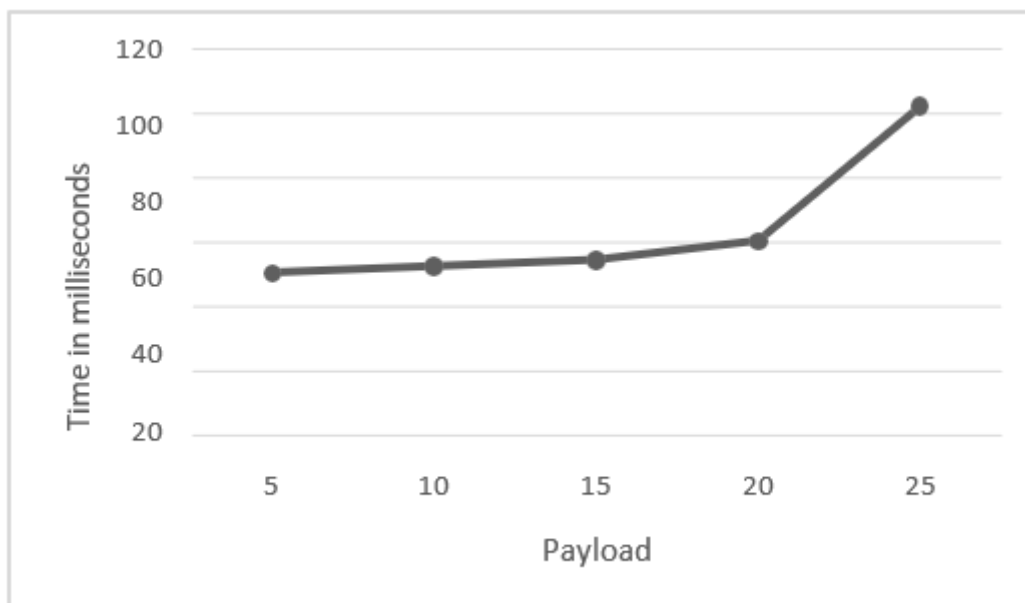
Embedded capacity is the rate of encrypted data in the cover file in bpp. It is defined as,

$$\text{Embedded capacity} = \frac{\text{Max size of embedded data}}{\text{Dimension of video cover}}$$



**Figure 9** Comparative analysis – Embedding Capacity

The graph below clearly shows that the proposed algorithm is light wait in computation irrespective of its payload.



**Figure 10** Comparative analysis – Payload vs Time

The following images show that there is no visual impact on the resultant video due to the process of embedding a secret message.



(a) Cover File (b) Stego file

**Figure 11** Visual Comparative analysis – (a) Cover file and (b) Stego file

Thus, the experimental report clearly portrays security enhancement without sacrificing the resultant accuracy of the stego video file.

#### 4. Conclusion

In this research work, an effective steganography system for video hiding is proposed through implementing the combination of the knight tour algorithm for locating the frames and 7th bit for hiding the secret message. The main idea behind the new algorithm is making the process more secure by randomizing the selection of frames where the secret message is to be incorporated. Because of the randomness, the intruders will find it hard to estimate the frames that are utilized for hiding the secret message. This adaptive algorithm can make the whole system more optimized and robust. Besides, because of the usage of 7th bit technique for data embedding, which is different from the traditional techniques that depend only on the least significant bit technique, this process can withstand any kind of attacks. The experiment has been implemented using different data sets and payloads, and the results show that this algorithm achieves better PSNR and SSIM than any other existing algorithms. As mentioned before, VIRAT Dataset has been used in order to evaluate the system. In this dataset, we selected 5000 videos, where each one of them is 10 seconds. Hence, the whole experiment lasts 12.5 hours. Our MSE value equals 0.2333 and PSNR around 85.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

- [1] Bender, W., D. Gruhl, N. Morimoto and A. Lu (1996). Techniques for data hiding, IBM Systems Journal, Vol. 35, No. 3-4, pp. 313-335.
- [2] Petitcolas, F. A. P., R. J. Anderson and M. G. Kuhn (1999). Information hiding - a survey. Proc. of the IEEE, Vol. 87, No. 7, pp. 1062-1078
- [3] P. P. Hadke and S. G. Kale, "Use of Neural Networks in cryptography: A review," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, 2016, pp. 1-4, doi: 10.1109/STARTUP.2016.7583925.
- [4] W. Hu, R. Zhou, A. El-Rafei and S. Jiang, "Quantum Image Watermarking Algorithm Based on Haar Wavelet Transform," in IEEE Access, vol. 7, pp. 121303-121320, 2019, doi: 10.1109/ACCESS.2019.2937390.
- [5] Singh, Aman. (2013). A Review on the Various Recent Steganography Techniques. International Journal of Computer Science and Network. 2. 142.
- [6] Liu, Yunxia & Liu, Shuyang & Wang, Yonghao & Zhao, Hongguo & Liu, Si. (2018). Video Steganography: A Review. Neurocomputing. 335. 10.1016/j.neucom.2018.09.091.
- [7] Suresh, Meenu & Sam, I. (2020). Optimized Interesting Region Identification for Video Steganography using Fractional Grey Wolf Optimization along with Multi-objective cost function. Journal of King Saud University - Computer and Information Sciences. 10.1016/j.jksuci.2020.08.007.
- [8] R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "Video steganography techniques: Taxonomy, challenges, and future directions," 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2017, pp. 1-6, doi: 10.1109/LISAT.2017.8001965.
- [9] Sadek, M. M., Khalifa, A. S. & Mostafa, M. G. M. Robust video steganography algorithm using adaptive skin-tone detection. Multimed Tools Appl 76, 3065–3085 (2017).
- [10] R. J. Mstafa and K. M. Elleithy, "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)," 2015 Wireless Telecommunications Symposium (WTS), New York,
- [11] NY, 2015, pp. 1-8, doi: 10.1109/WTS.2015.7117257
- [12] Pal A. K., Pramanik T. (2013) Design of an Edge Detection Based Image Steganography with High Embedding Capacity. In: Singh K., Awasthi A. K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 115. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-642-37949-9\\_69](https://doi.org/10.1007/978-3-642-37949-9_69)
- [13] Chan, Chi-Kwong & Cheng, L. M.. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition. 37. 469-474. 10.1016/j.patcog.2003.08.007.
- [14] R. J. Anderson, "Stretching the limit of steganography in information hiding," Springer Lecture Notes in Computer Science, vol. 1174, pp. 39–48, 1996.
- [15] Ran-Zan Wang, Chi-Fang Lin and Ja-Chen Lin, "Hiding data in images by optimal moderately-significant-bit replacement," in Electronics Letters, vol. 36, no. 25, pp. 2069-2070, 7 Dec. 2000, doi: 10.1049/el:20001429
- [16] M. Devi and N. Sharma, "Improved detection of least Significant bit steganography algorithms in color and gray scale images," 2014 Recent Advances in Engineering and Computational Sciences (RAECS), Chandigarh, 2014, pp. 1-5, doi: 10.1109/RAECS.2014.6799507.
- [17] Chi-Kwong Chan, L. M. Cheng, Improved hiding data in images by optimal moderately significant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018.
- [18] Wang, Z., C. C. Chang, M. Li, S. Cui (2013). Multi-dimensional and multi-level histogram-shifting-imitated reversible data hiding scheme, Smart Innovation, Systems and Technologies, Vol. 21, pp. 149-158.

- [19] Li, X., W. Zhang, X. Gui and B. Yang (2013). A novel reversible data hiding scheme based on two-dimensional difference-histogram modification, *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 7, pp. 1091-1100.
- [20] Maniriho, P., & Ahmad, T. (2019). "Information hiding scheme for digital images using difference expansion and modulus function". *Journal of King Saud University-Computer and Information Sciences*, 31(3), 335-347
- [21] Bhattacharyya, S., & Sanyal, G. (2012). "A robust image steganography using DWT difference modulation (DWTDM)". *International Journal of Computer Network and Information Security*, 4(7), 27.
- [22] Jayasudha, S. (2013). "Integer wavelet transform based steganographic method using OPA algorithm". *International Journal of Engineering and Science*, 2(4), 31-35.
- [23] Ramalingam, M., & Isa, N. A. M. (2014). "Video steganography based on integer haar wavelet transforms for secured data transfer". *Indian Journal of Science and Technology*, 7(7), 897-904.
- [24] Aly, H. A. (2011). "Data hiding in motion vectors of compressed video based on their associated prediction error". *IEEE transactions on information forensics and security*, 6(1), 14-18.
- [25] Filler, T., Judas, J., & Fridrich, J. (2011). "Minimizing additive distortion in steganography using syndrome-trellis codes". *IEEE Transactions on Information Forensics and Security*, 6(3), 920-935.
- [26] k b, Sudeepa & K, Raju & H.S., Ranjan & Aithal, Ganesh. (2016). A New Approach for Video Steganography Based on Randomization and Parallelization. *Procedia Computer Science*. 78. 483-490. 10.1016/j.procs.2016.02.092.
- [27] 490. 10.1016/j.procs.2016.02.092.
- [28] Younus, Zeyad & Talee, Ghada. (2020). Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. *Journal of Intelligent Systems*. 29. 1216–1225. 10.1515/jisys-2018-0225.
- [29] Joshi, Kamaldeep & Gill, Swati & Yadav, Rajkumar. (2018). A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. *Journal of Computer Networks and Communications*. 2018. 1-10. 10.1155/2018/9475142.
- [30] A. Horé and D. Ziou, "Image Quality Metrics: PSNR vs. SSIM," 2010 20th International Conference on Pattern Recognition, Istanbul, 2010, pp. 2366-2369, doi: 10.1109/ICPR.2010.579.
- [31] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861.