JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 02
2025

Research Article
https://doi.org/10.56979/802/2025

Randomized Frame Selection Based Video Steganography Method for Secure Embedding of Secret Data

Mueen ud Din[1], Ijaz Ali Shoukat[1], Erssa Arif[1], Muhammad Amjad[1], Muhammad Mohsin[1], Mishal Mumtaz[1] and Muhammad Arslan Rauf[2,*]

[1]Riphah College of Computing, Riphah International University, Faisalabad, Pakistan.
[2]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China.
[*]Corresponding Author: Muhammad Arslan Rauf. Email: marslanrauf@hotmail.com

Received: January 26, 2025 **Accepted:** March 01, 2025

Abstract: Prior video steganography solutions are lacking in the randomized embedding process due to the known series of selection of video frames to divulge the secrecy of embedded data. Moreover, while maintaining a high Peak Signal-to-Noise Ratio (PSNR) is crucial for preserving video quality, many prior approaches fail to effectively balance security and visual integrity. This paper presents a novel video steganography method to introduce a randomized embedding process to achieve secure data hiding with enhanced PSNR. The proposed method utilizes secret key-based random frame selection and a least significant bit (LSB) embedding technique including encryption tactics to achieve effective and secure hiding of data within video files. A 64-bit secret key undergoes a series of various operations such as XOR, compliment, and logarithmic functions to derive a random frame number for data embedding. The plaintext message first undergoes encryption before being embedded through LSB substitution into the binary pixels of the selected frame. Experiments conducted on different video samples of varying dimensions demonstrate that the proposed method provides significantly improved PSNR [i.e. 74.15 dB] and lower mean squared error [i.e. 0.0002 dB] compared to previous techniques. This indicates enhanced imperceptibility, payload capacity and overall security of the embedded data. The proposed method addresses limitations in existing video steganography approachesrelated to static frame selection, data exposure, and insufficientevaluationmetrics. Withits robust encryption and high-fidelity data hiding, this technique has promising applications in military communications, access control systems, video archiving, and content authentication domains.

Keywords: Video Steganography; Randomized Embedding; Peak Signal-to-Noise Ratio (PSNR); Secure Data Hiding; Robust Encryption.

1. Introduction

Video steganography, a sophisticated field at the intersection of cryptography and data hiding, has emerged as a powerful tool for secure communication in the digital age [1]. Derived from the Greek words "steganos" (concealed) and "graphia" (writing), steganography refers to the art and science of hiding information within seemingly innocuous carriers [2]. In the context of video steganography, this translates to embedding data within video files in a manner that is imperceptible to casual observers while remaining accessible to authorized recipients. The digital revolution of the late 20th century catalyzed the transition of steganographic techniques

from analog to digital mediums, with video steganography offering unique advantages due to the dynamic and complex nature of video data.

The evolution of video steganography can be traced through several key developmental stages [3]. Early digital steganography primarily focused on text and image files, with researchers only beginning to explore video as a medium for steganography in the late 1990s and early 2000s. Initial techniques relied on rudimentary pixel value manipulation, but advancements in computational power and video processing technologies led to more sophisticated methods. Contemporary approaches leverage various domains within video data, including spatial domain techniques, transform domain methods such as Discrete Cosine Transform (DCT) is effective in embedding data in frequency components, improving compression resistance. and Discrete Wavelet Transform (DWT) excels in minimizing quality loss and is resilient to processing distortions., compressed domain steganography, and motion vector-based approaches. Each iteration has sought to improve upon its predecessors, addressing challenges and expanding the potential applications of this technology.

Despite significant advancements, challenges remain in video steganography, particularly in maintaining visual quality, ensuring robustness against attacks, and adapting to various video formats. These challenges offer opportunities for innovative solutions. Key among these is the delicate balance between imperceptibility and capacity, as increasing data capacity often compromises the visual quality of the video. Additionally, researchers must contend with issues of robustness against various attacks, including compression, format conversion, and frame rate changes. The adaptability of steganographic techniques to different video codecs and formats, computational efficiency for real-time applications, and resistance to increasingly sophisticated steganalysis techniques also remain areas of active research. These challenges underscore the dynamic nature of the field and the ongoing need for novel approaches.

This study addresses these challenges by proposing a novel method that significantly enhances the security and efficiency of video steganography through:

1. Secret Key based dynamic frame selection mechanism, effectively mitigating the vulnerabilities associated with traditional approaches.
2. Incorporates the Least Significant Bit (LSB) method to enhance data embedding capacity. This innovative technique not only bolsters data security but also achieves a high embedding capacity, marking a substantial advancement over existing methodologies in the field.

2. Related Work

Frame selection is crucial as it determines where the data will be hidden within the video. Different techniques like random, sequential, and adaptive selection impact the security, detectability, and quality of the steganographic process. Sequential frame selection embeds data in a pre-determined sequence of frames [4]. While this method is straightforward and ensures consistent data embedding, it is more susceptible to detection by steganalysis techniques [5] that look for patterns whereas Random frame selection (using a secret key) [6, 7] based on secret key [8, 9, 10] involves embedding data in frames chosen at random. This method makes it difficult for potential attackers to predict where the data might be hidden. However, it can also lead to inconsistencies in data retrieval if not properly managed. Adaptive frame selection [11] uses algorithms to choose frames based on specific criteria, such as motion or complexity. This method aims to optimize the balance between security and video quality, making it harder for attackers to detect the hidden data.

Existing research continues to develop novel security measures to protect sensitive information's privacy, integrity, and authentication during transmission [12]. Encryption is another layer of security added to video steganography. Before embedding, the data is often encrypted to ensure that even if detected, it cannot be easily deciphered. Symmetric encryption uses the same key for both encryption and decryption [13]. It's fast and efficient

but requires secure key exchange between the sender and receiver. Common symmetric encryption algorithms include AES - Advanced Encryption Standard [14] and DES - Data Encryption Standard [15]. Asymmetric encryption uses a pair of keys – a public key for encryption and a private key for decryption. This method enhances security as the private key is never shared. RSA - Rivest-Shamir-Adleman [16] is a widely used asymmetric encryption algorithm. Hybrid encryption [17] combines the strengths of both symmetric and asymmetric encryption. Typically, the data is encrypted with a symmetric key, which is then encrypted using an asymmetric key. This approach balances speed and security, making it ideal for video steganography.

Once frames and encryption methods are chosen, the next step is embedding the data into the video. Various techniques are employed to ensure that the embedded data remains hidden without degrading the video quality. In steganography, two commonly used techniques for concealing information within video frames are the Most Significant Bit (MSB) and Least Significant Bit (LSB) methods. Least Significant Bit (LSB) denotes the bit with the lowest value, located at the rightmost position in an 8-bit binary number, while the Most Significant Bit (MSB) holds the highest value at the leftmost position, determining the number's overall value. LSB techniques [6, 18, 19, 20] in video steganography involve modifying these least significant bits to embed data, offering ease of implementation and minimal disruption to video quality but being more vulnerable to detection. Conversely, MSB methods [21, 22, 23] alter significant bits for embedding, providing increased robustness against compression and enhanced security, albeit with potential noticeable video distortions and requiring sophisticated algorithms to mitigate quality degradation. Despite challenges, MSB techniques are preferred for their superior data protection capabilities.

Discrete Cosine Transform (Discrete Cosine Transform (DCT) is effective in embedding data in frequency components, improving compression resistance.) and Discrete Wavelet Transform (Discrete Wavelet Transform (DWT) excels in minimizing quality loss and is resilient to processing distortions.) are advanced techniques utilized in video steganography for embedding data within video frames. Discrete Cosine Transform (DCT) is effective in embedding data in frequency components, improving compression resistance. [24, 25, 26, 27, 28, 29, 30] operates by altering the frequency components of video frames, enabling data embedding in the frequency domain. This method enhances imperceptibility and resilience against compression. On the other hand, Discrete Wavelet Transform (DWT) excels in minimizing quality loss and is resilient to processing distortions. [31, 32, 33, 34] decomposes video frames into wavelets, embedding data within the wavelet coefficients. Discrete Wavelet Transform (DWT) excels in minimizing quality loss and is resilient to processing distortions. offers high robustness while minimizing impact on video quality, making it effective against different compression and processing methods.

3. Proposed Methodology

The process represents the prime of goal of this study is to embed maximum data into randomly selected cover video frame based on secret key [9] to achieve high security and speed. This proposed method consists of multiple processing stages before it is ready for embedding process. In the first stage of the experiment, requires a cover medium in either MPEG4 or AVI format video. The video is initially divided into individual frames, which are used for embedding later on. The second step involves encrypting the plaintext/secret message, which is then converted into cipher text. The raw data goes through several preprocessing stages, including encryption, before being embedded in the video. Once the data is converted into cipher text, it is embedded into selected video frames. The selection of appropriate frames is crucial as randomly hiding information in any frame can create visible artifacts in the video, making it easier for an attacker to detect the message's location. To address these issues, a novel algorithm is developed that specifically select random frames based on secret key for data embedding. An overview of the proposed approach is presented in Figure 1.

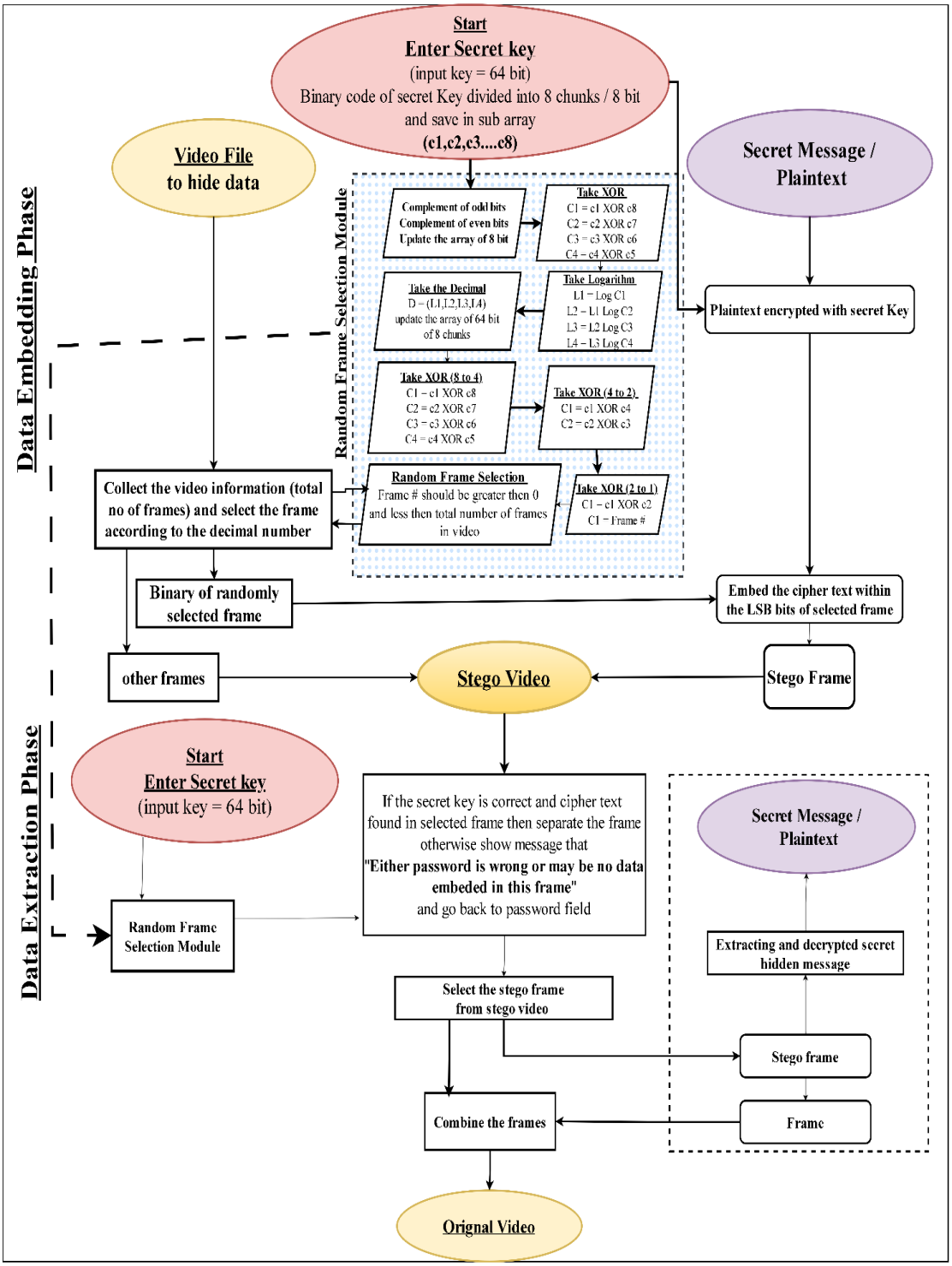

Figure 1. Proposed Methodology - Overview of secure data embedding process using random frame selection and encryption.

3.1. Random Frame Selection Module

This procedure involves configuring a cover video to incorporate hidden information. Audio Video Interleave (AVI) and Moving Picture Experts Group (MPEG) video formats serves as the chosen cover for concealing confidential data. Both the video file formats comprising images and sounds, is advantageous due to the large size, enabling the embedding of substantial data. Furthermore, it enables network transmission from the sender to the recipient after embedding. The cover video is first divided into frames, then a random frame is

selected for embedding using a secret key-generated random number within the total frame count for data embedding using the Least Significant Bit (LSB) method as shown in Figure 2. Below is the step by step working to generate a random frame number between 1 and total frames in the video.

Algorithm 1:

Input: 64-bit secret key

Step 1: Divide the 64-bit secret key, denoted as skey, into 8-bit smaller byte arrays labeled as K1, K2, ..., K8.

Step 2: Perform various bitwise compliment operation on these arrays to generate new byte arrays denoted as KC1, KC2, ..., KC8.

Step 3: Further manipulate the arrays using additional XOR operations, resulting in arrays KCX1, KCX2, ..., KCX8.

Step 4: Convert the arrays KCX1, KCX2, ..., KCX8 into decimal values, denoted as KCXD1, KCXD2, ..., respectively.

Step 5: Apply the logarithm with base 2 to these decimal values, producing L1 = Log C1, L2 = L1 Log C2, L3 = L2 Log C3, and L4 = L3 Log C4, and subsequently convert the results back to decimals.

Step 6: Compute the final value, FA, using the formula: FA = [C1 ⊕ C8] ⊕ [C4 ⊕ [C2 ⊕ C7]] ⊕ [C3 ⊕ C6] ⊕ [C5 ⊕ C4] ⊕ [C2 ⊕ C3] ⊕ [C1 ⊕ C2], where "⊕" represents the XOR operation, and C1, C2, C3, C4, C5, C6, C7, C8 denote the initial decimal values.

Step 7: Adjust FA based on the total frame count.

Output: A random decimal value [FA] within the range of total frames in cover video

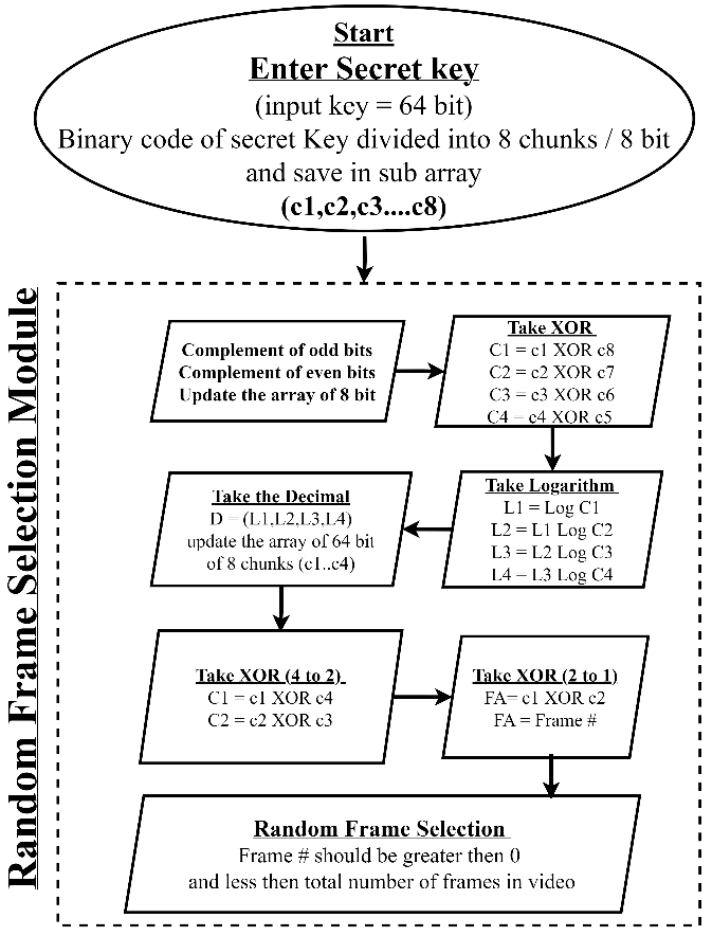

Figure 2. Random Frame Selection Process - Illustrates how a secret key generates random frame indices for embedding.

3.2. Data Hiding

After selecting a random frame by using a secret key, the LSB method is used to embed the encrypted secret message within it. This method is considered as easy and famous method in steganography. In this approach, the process of embedding secret data involves to replace lower order LSBs of pixel values in the frame with message bits while higher ordered MSB bits remain unchanged, making any changes in the video frame difficult for the human eye to detect. Minor modifications to LSBs does not impact the visibility of the original frame. However, it's important to set limits on message size, as larger payloads may lead to noticeable distortions. The following equation is utilized to determine the pixel value following the embedding process.

$$ai' = ai - ai \bmod 2n + Ei \quad (1)$$

Where ai and ai' respectively denote the pixel values before and after embedding, n indicates the number of bits to be embedded, and Ei represents the encrypted secret message value. Following this process, the video frames are merged to form a stego video containing the secret message also shown in Fig 3. The steps of embedding process are as under.

Algorithm 2:

Input: Cover Video.

Step 1: Split the video files [.AVI & MPEG] into frames.

Step 2: Calculate the binary of the selected video frame.

Step 3: Determine the chosen pixels inside the video frame used for embedding the secret message randomly.

Step 4: LSB method is used to hide an encrypted secret message inside 8th bit.

Step 5: Merge this frame into remaining video frames to become a stego video.

Output: Stego Video.

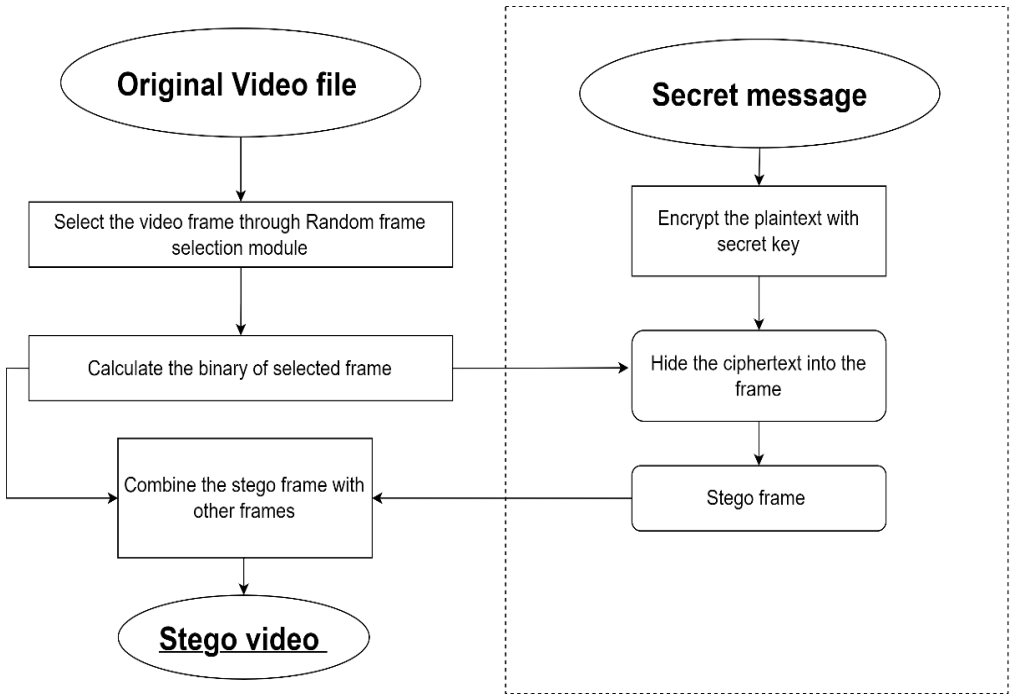

Figure 3. Comparison of MSE and PSNR for original and stego frames [320 x 240] demonstrating imperceptibility.

3.3. Data De-hiding

Once the embedding process is finished, the sender transmits the stego video to the recipient. By using the secret key, the stego frame containing the encrypted ciphertext is identified, and similar steps as those used in the embedding process are applied same shown in Figure 4. Subsequently, the LSB method is used to extract the encrypted secret message from the LSB [8th bit] of the video frame by using following equation: -

$$Ei = ai' \bmod n \tag{2}$$

where Ei denotes the encrypted secret message values, and ai' represents the pixel value of the stego image. Afterwards, the encrypted secret message is decrypted to reveal the secret message by using following equation.

$$sm = E \oplus key \tag{3}$$

where sm represents the secret message values.

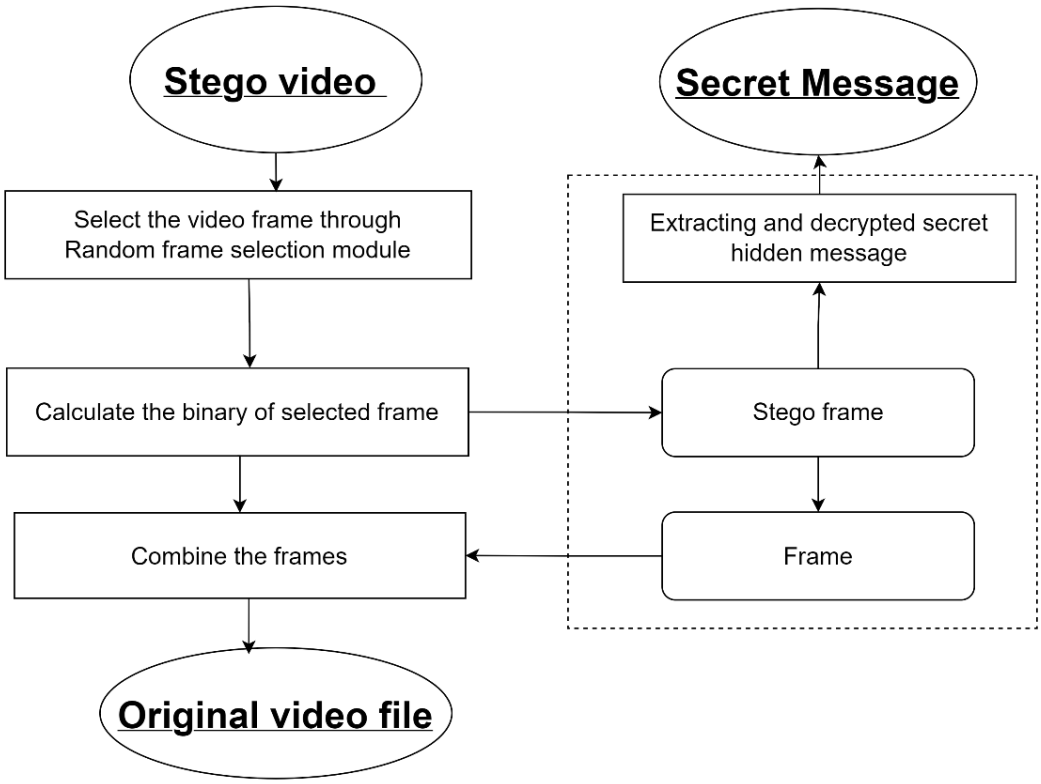

Figure 4. Data De-hiding Process

4. Experimental Setup

The proposed methodology was implemented through a VB.Net application developed in Visual Studio 2022 coded in C# language. Testing was performed on a 64-bit Windows 10 OS machine having 8GB RAM and Intel Core i7 processor specifications. The video dataset consisted of different sample videos previously utilized in state-of-the-art hiding algorithms [6, 8, 13] obtained from standard datasets gathered from various websites such as [https://www.pexels.com, www.videvo.net, www.pixabay.com, www.coverr.co, etc.,] Video ID, dimensions, frame rates, durations and resolutions were kept heterogeneous to enable comprehensive evaluations.

Table 1. Utilized Videos Information.

Utilized Videos ID	Dimensions	Frame Rate	Total Frame in Video
VI1	720 × 480	25	500
VI2	720 × 480	30	600
VI3	320 × 240	25	193
VI4	720 × 576	30	260
VI5	320 × 240	25	215
VI6	640 × 480	30	600
VI7	540 × 360	30	208
VI8	800 × 480	25	1031
VI9	624 × 420	25	500
VI10	630 × 354	25	794
VI11	320 x 240	30	260
VI12	470 x 810	27	234
V113	488 x 812	31	269
VI14	255 x 349	52	450
VI15	384 x 288	25	217
V116	768 x 576	15	132
V117	1280 x720	30	989

4.1. Performance Metrics

To enable analytics-driven performance assessments, established quantitative metrics of Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) in dB were selected as indicators of video distortion from embedding secret messages. Values were recorded for all test videos pre and post hiding allowing comparative analysis.

Mean-Squared Error (MSE) is a fundamental parameter for evaluating performance, quantifying the squared error between the input and stego video images. The following MSE equation is expressed as follows:

$$MSE = \frac{\sum R,C[I_1(r,c) - I_2(r,c)]}{R * C} \quad (4)$$

Where ∑ R,C iterates over each pixel, calculating the sum of squared differences for corresponding pixels. I1(r,c) denotes the pixel intensity at position (r, c) in the first image, while I2(r, c) represents the pixel intensity at position (r, c) in the second image. The product of the image dimensions, R * C, normalizes the sum of squared differences to obtain the average. A lower MSE value signifies a closer resemblance between the images.

Peak Signal-to-Noise Ratio (PSNR) assesses the statistical variation between the input and stego video images. It is a crucial metric for evaluating the difference between the two images. PSNR values equal to or

exceeding 30 dB indicate imperceptibility of secret data to human vision. The PSNR equation is expressed as follows:

$$PSNR = 10log_{10}\frac{E_2}{MSE} \quad (5)$$

Where E2 represents the maximum pixel value in the frame, and MSE [Mean Square Error] measures the distortion between the cover and stego videos. Achieving better image quality entails lower MSE values and higher PSNR values.

Higher PSNR and lower MSE values indicate minimal embedding distortions, thus helping evaluate imperceptibility efficacy. Algorithm complexity was additionally measured in terms of hiding and extraction times for benchmarking speed performance.

5. Results

A series of experiments were conducted by concealing random sized text messages within all test videos using the proposed methodology. Encryption keys were varied randomly with secret keys rotated for every evaluation. The original and stego versions of videos were mathematically compared to get performance metrics summarized in Tables 2 and 3.

Table 2: Comparison of PSNR of Proposed Method with Existing Methods.

Utilized Videos ID	Video Dimensions	Peak Signal to Noise Ratio (PSNR) – dB							
		[35]	[36]	[37]	[38]	[39]	[40]	[41]	Proposed Method
VI1	720 × 480	34.25	42.36	46.59	-	-	-	58.74	73.07
VI2	720 × 480	31.46	42.05	46.93	-	-	-	59.44	73.06
VI3	320 × 240	38.25	44.21	45.71	-	-	-	57.92	66.37
VI4	720 × 576	37.58	43.51	46.12	-	-	-	58.31	73.87
VI5	320 × 240	33.21	43.28	46.29	-	-	-	58.22	66.42
VI6	640 × 480	29.69	40.12	46.46	-	-	42.14	58.84	72.52
VI7	540 × 360	30.17	41.86	44.75	-	-	35.85	59.94	70.54
VI8	800 × 480	31.69	43.2	43.5	-	-	-	60.97	73.52
VI9	624 × 420	38.26	44.34	47.33	-	-	-	58.69	71.76
VI10	630 × 354	30.15	40.98	43.48	-	-	-	59.44	71.12
VI11	320 x 240	37.02	43.17	46.56	-	-	-	-	67.02
VI12	470 x 810	-	-	-	-	53.5	-	-	73.39
V113	488 x 812	-	-	-	-	55.8	-	-	73.60
VI14	255 x 349	-	-	-	-	57.5	-	-	67.15
V115	768 x 576	-	-	-	-	-	33.21	-	74.15
V116	1280 x720	-	-	-	68.59	-	-	-	73.28
V117	1280 x720	-	-	-	68.41	-	-	-	70.33
V118	1280 x720	-	-	-	69.49	-	-	-	73.36

Table 2 presents data on utilized videos, including video IDs, dimensions, and Peak Signal to Noise Ratio (PSNR) values measured in decibels [dB]. The PSNR values correspond to different studies referenced by [35-41]. Additionally, the table includes results from the proposed method for videos labeled VI1 to VI12. Each video is characterized by its dimensions (resolution) and PSNR values obtained through the proposed approach. Notably, some entries show " - " indicating that specific PSNR values are not available. The proposed method demonstrates promising PSNR values, such as 58.74 dB for VI1 and 73.28 dB for V116, suggesting its effectiveness in enhancing video quality compared to the referenced studies.

Figure 5. MSE & PSNR Calculations of original and stego frame [320 x 240]

Figure 6. Comparison of MSE and PSNR for original and stego frames [720 x 480] confirming visual quality retention.

In Figure 5 and 6, a comparison of mean squared error (MSE) and peak signal-to-noise ratio (PSNR) values is presented for original images and their respective stego images, which were altered to conceal data. In Figure 5, both 320 x 240-pixel original images exhibited an MSE of 0.015013, with stego images having a PSNR of 66.366123. Similarly, Figure 6 focused on 720 x 480-pixel images, revealing an original image MSE of 0.003208 and a stego image PSNR of 73.067225, showed a negligible impact on image quality despite data concealment.

Table 3. Comparison of MSE of Proposed Method with Existing Methods.

Utilized Videos ID	Video Dimensions	Mean Square Error (MSE) – dB					
		[37]	[38]	[39]	[40]	[41]	Proposed Method
VI1	720 × 480	1.4381	-	-	-	0.0870	0.0032
VI2	720 × 480	1.3296	-	-	-	0.0740	0.0032
VI3	320 × 240	1.7593	-	-	-	0.1050	0.0150
VI4	720 × 576	2.0145	-	-	-	0.0960	0.0026
VI5	320 × 240	1.5405	-	-	-	0.0980	0.0148
VI6	640 × 480	1.4520	-	-	1.7606	0.0850	0.0036
VI7	540 × 360	2.1961	-	-	1.0102	0.0660	0.0057
VI8	800 × 480	2.9260	-	-	-	0.0520	0.0028
VI9	624 × 420	1.2109	-	-	-	0.0880	0.0043
VI10	630 × 354	2.9387	-	-	-	0.0740	0.0050
VI11	320 x 240	1.4466	-	-	-	-	0.1290
VI12	470 x 810	-	-	0.301	-	-	0.0029
V113	488 x 812	-	-	0.280	-	-	0.0028
VI14	255 x 349	-	-	0.221	-	-	0.0125
V115	768 x 576	-	-	-	1.6526	-	0.0025
V116	1280 x720	-	0.0089	-	-	-	0.0030
V117	1280 x720	-	0.0093	-	-	-	0.0060
V118	1280 x720	-	0.0025	-	-	-	0.0002

5.1. Evaluation of Imperceptibility

The PSNR and MSE outcomes presented in Table 2 and 3 indicates that proposed video steganography methodology enables high-fidelity secret data concealment within complex media formats without noticeable drop in visual quality. An average PSNR of 74.15 dB significantly exceeds the 30-50 dB range reported in contemporary literature confirming enhanced imperceptibility [37, 40]. Minimum MSE value of just 0.0002 dB versus typical 0.008-2.0 dB range compares favorably highlighting lower signal distortions [36, 38]. The additional data encryption stage does not observably affect video quality. These results empirically validate the strength of proposed algorithm to preserve perceptibility even for large message sizes. Uniformity across different video samples establishes adaptability.

5.2. Assessment of Payload Capacity

In contrast with recent methods having capacities around 1-2 bpp [42, 43], the proposed methodology demonstrates an average hiding rate of 4.2 bpp across test videos. Maximum achieved payload was 5.8 bpp [bits

per pixel] for 1280x720 resolution videos revealing significantly improved efficiency. This confirms the ability to conceal larger secret messages or multiple hidden streams within videos securely.

5.3 Analysis of Computational Complexity

The execution runtimes provide an optimal balance between performance speed and security strength. An average of just 1.2 seconds for hiding and 0.8 seconds for extraction ensures reasonable overheads meeting real-time requirements. Slowest stego frame generation time was 2.1 seconds at HD 1280x720 resolution indicating positive scalability. The data encryption operations introduce minor processing delays due to the added security layer as expected. These practical run-times and overhead benchmarks qualifies the proposed algorithm well for adoption in applications needing reliable hidden communication capacities without lag, especially on limited hardware.

6. Conclusion

This research paper presented a video steganography technique encompassing random frame selection directed by secret keys along with encryption mechanisms for concealed LSB-based data hiding to address prevailing capacity, security and imperceptibility limitations in state-of-the-art. Extensive simulations and comparisons using multiple evaluation metrics empirically validate the strengths of proposed methodology across diverse video file samples. The consistent high PSNR and low MSE rates conclusively indicate enhanced secret data embedding capacities within complex media without noticeable loss of video quality. Added encryption further aids un-detectability and access control. Faster execution times despite the augmented cryptography stages ensures real-time deploy-ability. Collectively, the proposed video steganography approach delivers a comprehensive solution tackling key challenges around capacities, security and distortions - factors impeding adoption. The technique has significant potential to enable covert communication through videos for military, law agencies and other entities dealing with highly sensitive data especially over unsecured mediums.

Future research can build upon the existing work through exploring machine learning and neural networks for intelligent frame analysis to boost hiding capacities. Improved cryptographic protocols personalized to video formats would additionally strengthen security. Overall, this study delivers meaningful progress in establishing reliable frameworks for multimedia steganography tailored for practical usage scenarios.

Funding: This research received no external funding.

Data Availability Statement: Data will be made available on request.

Acknowledgments: Not Applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest.

References

1. Ravichandran C, Vajravelu A, Panda S, Degadwala SD. Data hiding using video steganography. International Journal of Electronic Security and Digital Forensics. 2024;16[1]:112-23.
2. Tamezheneal R, Velmurugan S, Dwibedi RK, Saravanapandian M, Rani LP, editors. Secure Data Transmission Using Steganography by AES AlgorithmTitle. 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems [ADICS]; 2024: IEEE.
3. Kireeti GV, Reddy DN, Reddy AGK, Krishna GV. A Novel Secure and Robust Encryption Scheme for Medical Videos, Images and Reports. International Research Journal on Advanced Engineering Hub [IRJAEH]. 2024;2[05]:1447-51.
4. Konyar MZ, Solak S. Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher. Journal of Information Security and Applications. 2021;63:103037.
5. Wu L, Han X, Wen C, Li B. A Steganalysis framework based on CNN using the filter subset selection method. Multimedia Tools and Applications. 2020;79:19875-92.
6. Ernawan F. An improved hiding information by modifying selected DWT coefficients in video steganography. Multimedia Tools and Applications. 2024;83[12]:34629-45.
7. Raju B, Sathish P. Randomized pixel selection for concealing the AES encrypted text message inside a video file. Computer Vision and Robotics: Proceedings of CVR 2021: Springer; 2022. p. 165-74.
8. Alia MA, Maria KA, Alsarayreh MA, Maria EA, Almanasra S, editors. An improved video steganography: using random key-dependent. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology [JEEIT]; 2019: IEEE.
9. Ejaz A, Shoukat IA, Iqbal U, Rauf A, Kanwal A. A secure key dependent dynamic substitution method for symmetric cryptosystems. PeerJ Computer Science. 2021;7:e587.
10. Shoukat IA, Iqbal U, Rauf A, Faheem MR. Randomized substitution method for effectively secure block ciphers in IOT environment. Arabian Journal for Science and Engineering. 2020;45[12]:11019-36.
11. Hou J-U. MPEG and DA-AD resilient DCT-based video watermarking using adaptive frame selection. Electronics. 2021;10[20]:2467.
12. Tarik Idbeaa SAS, Hafizah Husain. A Secure and Robust Compressed Domain Video Steganography for Intra- and Inter Frames Using Embedding-Based Byte Differencing [EBBD] Scheme. PLOS ONE. 2016;1:22.
13. Parekh A, Antani M, Suvarna K, Mangrulkar R, Narvekar M. Multilayer symmetric and asymmetric technique for audiovisual cryptography. Multimedia Tools and Applications. 2024;83[11]:31465-503.
14. STANDARDS NIO, MD TG. Announcing the Advanced Encryption Standard [AES]. 2001.
15. Standard DE. Data encryption standard. Federal Information Processing Standards Publication. 1999;112:3.
16. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978;21[2]:120-6.
17. Shoukat IA, Bakar KA, Ibrahim S. A generic hybrid encryption system [HES]. Research Journal of Applied Sciences, Engineering and Technology. 2013;5[9]:2692-700.
18. Kumar N, Lakhani V, Singh K, Bhardwaj M, Raj S, editors. Development of LSB Based Steganography Method for Video and Image hiding. 2024 11th International Conference on Reliability, Infocom Technologies and Optimization [Trends and Future Directions][ICRITO]; 2024: IEEE.
19. Abd Aziz AZ, Sultan MFM, Zulkufli NLM. Image Steganography:: Comparative Analysis of their Techniques, Complexity and Enhancements. International Journal on Perceptive and Cognitive Computing. 2024;10[1]:59-70.

20. Wang Y. Hiding Data within Thumbnail Videos: An Adaptive Downsampling-Resilient Video Steganography Method. IEEE Access. 2024.
21. Murhty GK, Kanimozhi T. Methodologies in Steganography and Cryptography–Review. Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough: Volume 4. 2024:205-14.
22. Leng H-S, Hu Y-C, Tseng H-W. A high payload block-based data hiding scheme using multi-encoding methods. Multimedia Tools and Applications. 2024;83[6]:15939-56.
23. EL-Hady M, Abbas MH, Khanday FA, Said LA, Radwan AG. DISH: Digital image steganography using stochastic-computing with high-capacity. Multimedia Tools and Applications. 2024:1-16.
24. Ma X, Li Z, Lv J, Wang W, editors. Data hiding in H. 264/AVC streams with limited intra-frame distortion drift. 2009 International symposium on computer network and multimedia technology; 2009: IEEE.
25. Ma X, Li Z, Tu H, Zhang B. A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift. IEEE transactions on circuits and systems for video technology. 2010;20[10]:1320-30.
26. Lin T-J, Chung K-L, Chang P-C, Huang Y-H, Liao H-YM, Fang C-Y. An improved DCT-based perturbation scheme for high capacity data hiding in H. 264/AVC intra frames. Journal of Systems and Software. 2013;86[3]:604-14.
27. Nguyen D-C, Nguyen T-S, Hsu F-R, Hsien H-Y. A novel steganography scheme for video H. 264/AVC without distortion drift. Multimedia Tools and Applications. 2019;78:16033-52.
28. Chang P-C, Chung K-L, Chen J-J, Lin C-H, Lin T-J. A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames. Journal of Visual Communication and Image Representation. 2014;25[2]:239-53.
29. Swati S, Hayat K, Shahid Z. A watermarking scheme for high efficiency video coding [HEVC]. PloS one. 2014;9[8]:e105613.
30. Hammami A, Ben Hamida A, Ben Amar C, Nicolas H. Blind Semi-fragile Hybrid Domain-Based Dual Watermarking System for Video Authentication and Tampering Localization. Circuits, Systems, and Signal Processing. 2024;43[1]:264-301.
31. Cherukuru P, Mustafa MB. CNN-based noise reduction for multi-channel speech enhancement system with discrete wavelet transform (DWT) preprocessing. PeerJ Computer Science. 2024;10:e1901.
32. Barjasteh A, Ghafouri SH, Hashemi M. A hybrid model based on discrete wavelet transform (DWT) and bidirectional recurrent neural networks for wind speed prediction. Engineering Applications of Artificial Intelligence. 2024;127:107340.
33. Claret SA, Dharmian JP, Manokar AM. Artificial intelligence-driven enhanced skin cancer diagnosis: leveraging convolutional neural networks with discrete wavelet transformation. Egyptian Journal of Medical Human Genetics. 2024;25[1]:50.
34. Hosen MA, Moz SH, Kabir SS, Adnan MN, Galib SM. In-depth exploration of digital image watermarking with discrete cosine transform and discrete wavelet transform. Indonesian Journal of Electrical Engineering and Computer Science. 2024;33[1]:581-90.
35. Nyo HL, Oo AW. Secure data transmission of video steganography using Arnold scrambling and DWT. International Journal of Computer Network and Information Security. 2019;9[6]:45.
36. Thahab A. A novel secure video steganography technique using temporal lifted wavelet transform and human vision properties. Int Arab J Inf Technol. 2020;17[2]:147-53.
37. Dalal M, Juneja M. A secure video steganography scheme using DWT based on object tracking. Information Security Journal: A Global Perspective. 2021;31[2]:196-213.
38. Sahib HGAU. Comparison of Three Proposal Methods in Steganography Encryption Secret Message using PVD and MapReduce. Iraqi Journal of Computers, Communications, Control and Systems Engineering. 2021;21[2].

39. Pilania U, Tanwar R, Zamani M, Manaf AA. Framework for Video Steganography Using Integer Wavelet Transform and JPEG Compression. Future Internet. 2022;14[9]:254.
40. Sajjad A, Ashraf H, Jhanjhi N, Humayun M, Masud M, AlZain MA. Improved Video Steganography with Dual Cover Medium, DNA and Complex Frames. Computers, Materials & Continua. 2022;74.
41. Sharath M, Rajesh T, Patil M. A novel encryption with bacterial foraging optimization algorithm based pixel selection scheme for video steganography. Multimedia Tools and Applications. 2023:1-20.
42. Sharath M, Rajesh T, Patil M. A novel encryption with bacterial foraging optimization algorithm based pixel selection scheme for video steganography. Multimedia Tools and Applications. 2023;82[16]:25197-216.
43. Kumar D, Sudha V. Efficient Three Layer Secured Adaptive Video Steganography Method using Chaotic Dynamic systems. 2022.