International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Video Steganography with DNA and Complex Frames

Dr. Manjula G R[1], Raksha P K[2], Shraddha C S Atreya[3], Swathi H R[4], Vaishnavi N[5]

[1]Professor, Dept. of CS&E, JNN College of Engineering, Shivamogga, India.

[2,3,4,5] UG Student, Dept. of CS&E, JNN College of Engineering, Shivamogga, India.

Abstract **- A modern approach to video steganography combines DNA embedding of encrypted data with intelligent frame selection, enhancing data security during transmission. By creating fake DNA for frame selection and embedding it into strategically chosen frames, termed complex frames this method ensures robust encryption and imperceptibility, offering a promising solution for secure internet data transmission.**

KeyWords**:** Complex frames, DNA, embedding, encryption, stego video.

1. INTRODUCTION

Data security during transmission is a paramount concern in today's interconnected world, were sensitive information traverse networks vulnerable to interception and manipulation. As cyber threats evolve in complexity and scale, the quest for robust data protection mechanisms intensifies. Among the arsenal of tools in cybersecurity, cryptography and steganography stand out as pillars of defence against unauthorized access and data breaches.

Cryptography transforms plaintext messages into ciphertext using algorithms and cryptographic keys, ensuring that only authorized parties can decipher the information. Symmetric cryptography employs a single key for both encryption and decryption, while asymmetric cryptography uses a pair of keys, public and private, for these operations. Notable encryption algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), International Data Encryption Algorithm (IDEA), and Rivest-Shamir-Adleman (RSA) play vital roles in securing data at rest and in transit**.**

In contrast, steganography focuses on concealing the existence of data within innocuous carriers or cover media. This technique obscures sensitive information from prying eyes by embedding it seamlessly into images, audio files, text, or videos. Steganographic methods exploit the Human Visual System's (HVS) limited perceptual abilities, leveraging imperceptible alterations in media to hide data effectively. For instance, plain text steganography employs whitespace or special characters to hide messages within seemingly innocuous text passages, making detection challenging without prior knowledge of the steganographic method used.

The realm of video steganography expands these concealment techniques to multimedia content, where data can be concealed within the frames of video files. This approach capitalizes on the HVS's reduced sensitivity to minor changes in video scenes, ensuring that the hidden data remains undetectable to casual observation. Recent advancements in steganographic research have explored novel cover media, with DNA steganography emerging as a frontier due to its vast information storage capacity. By encoding data within the structure of DNA molecules using nucleotide bases (A, T, C, G), this cutting-edge technique offers a promising avenue for ultra-secure data concealment and transmission, heralding a new era in covert communication technologies.

The objectives of this study encompass a comprehensive exploration of steganographic techniques, with a focus on enhancing data transmission security. This includes delving into the intricacies of hyperchaotic mapping for precise pixel selection within frames, a critical aspect of robust data concealment. Additionally, the implementation of a dual cover medium approach will be pursued to further fortify data hiding capabilities, aiming to achieve a sophisticated and resilient system for secure information exchange.

2. LITERATURE SURVEY

A concept of dual cover medium using DNA and complex frames for embedding secret messages in videos was proposed. Frame selection is based on DNA binary values., codon count, and a user-supplied key, with a linear congruential generator generating a random number XORed with DNA for frame selection. Pixel selection utilizes the Burger chaotic map and linear congruential generator, employing LSB replacement for data concealment. However, random frame embedding may lead to perceptible artifacts, prompting the modified LSB strategy to create both encrypted and non-encrypted AVI files, compromising encryption and requiring two files for transmission [1].

A method assigns unique two-digit binary values to DNA bases (A, C, G, T) using a DNA dictionary. Messages are converted to 8-bit binary sequences based on ASCII, then to corresponding DNA sequences. A random DNA sequence serves as cover media, forming a balanced tree with node characters. Tree height, based on message size, affects the random DNA sequence size. Internal nodes ensure unpredictability, limiting even-level nodes to two children and odd-level nodes to three. Encoding involves converting characters to binary and then DNA, replacing leaf nodes in the tree for an encrypted DNA sequence. Decoding reverses this process to retrieve the original message [3].

Techniques integrating DNA coding, hyperchaotic Liu systems, and chaos theory are employed for enhanced data security. The coding algorithm converts secure text to binary, segments it, and substitutes parts with letters based on a table, creating coded text. Chaos theory's complexity and sensitivity to initial conditions aid data encryption and hiding. The Message

Coding & Embedding Technology encompasses message coding, non-sequential data hiding, pixel diffusion, extraction, and decoding, ensuring secure message handling. Steps include calculating message size, DNA role selection, binary conversion, dynamic DNA coding, Liu system-generated sequences, data hiding in pixels, extraction, decoding, and ASCII conversion, enhancing security and data concealment capabilities [2].

A video steganography concept based on DCT psychovisual and object motion was introduced, leveraging motion vectors in P and B frames to identify low-distortion areas for message hiding. The technique embeds data in DCT coefficients, focusing on coefficients between 4 and 5 in frequency order, to minimize image quality impact. By optimizing embedding locations based on psychovisual effects, the approach ensures resilience to compression and minimal visual distortion. Experimentation with thresholds f and s strategically scales selected coefficient pairs, enhancing data hiding effectiveness while maintaining visual fidelity [4].

The recommended method involves binary conversion of DNA bases using the DNA dictionary, with each base uniquely assigned a two-digit binary value (A: 00, C: 01, G: 10, T: 11). The secret message undergoes ASCII to binary conversion, split into eight-bit segments. Two key values, K1 (0 to 255) for XORing the message and K2 for segmenting the binary converted DNA, are utilized. Encoding involves XORing K1 with the message's first 8 bits iteratively, segmenting the binary DNA with K2, and inserting the cipher's binary bits into each segment. Decoding reverses this process, recovering the message iteratively using fake DNA, cipher, and random array sequences, followed by XOR-ing and conversion to ASCII for the final message. This approach enhances security through repeated XOR-ing, complicating decoding for potential intruders [5].

An advanced chaos-based video steganography method using DNA alphabets was introduced, featuring frame selection, data embedding, and extraction stages. The frame selection process involves converting a DNA strand into binary, determining its length, and deriving corresponding decimal values crucial for subsequent operations. Data embedding strategically occurs at selected pixel points governed by the Burger chaotic map, with added randomization for heightened security. Integration of random numbers from a linear congruential generator further augments the randomness of pixel selection. During extraction, the original message retrieval entails isolating frames, generating chaotic maps, pinpointing pixel locations, extracting bits in a specific order, and reconstructing the hidden information based on secret parameters and keys. Quality assessment metrics such as Mean Squared Error and Peak Signal to Noise Ratio are employed for evaluating the perceptual quality of the cover and stego video frames, ensuring the fidelity of the steganographic process [6].

A secured data hiding technique combining the DES algorithm with LSB coding was proposed for robust data security. DES, a symmetric key algorithm, ensures confidentiality through 16 iterative rounds involving bit shuffling, S-box substitutions, and exclusive-OR operations. This method initiates with receiving a cover file and secret data from users, encrypting the latter using DES and a user-provided secret key. The encrypted data is then seamlessly embedded into video frames using LSB, ensuring hidden data concealment within the video structure. At the recipient's end, the stego video undergoes processing to extract and decrypt the hidden data, leveraging the message length indication in the first frame for efficient extraction. This sophisticated approach guarantees secure and reliable data hiding and retrieval within video files, maintaining the integrity and confidentiality of sensitive information throughout the transmission and storage processes [7].

To boost system efficiency and minimize data redundancy, the proposed method begins with a series of innovative steps. Initially, a frame skipping algorithm selectively extracts frames from a sequence, reducing system complexity significantly. These chosen frames are then converted to grayscale and undergo motion filtering to exclude those with minimal movement. This preprocessing, involving frame skipping and motion filtering, employs temporal differencing for quick motion assessment. Following frame extraction and grayscale conversion, frames with notable motion are identified. Moreover, the system incorporates an advanced feature extraction approach based on MoBSIFT, integrating MoBSIFT and MBH techniques. This method utilizes interest point detection and local feature description to focus on crucial points, ensuring superior scale and rotation invariance while maintaining precision and efficiency [9].

A method for enhancing the processing efficiency of traffic surveillance videos has been proposed, with a focus on addressing challenges posed by the presence of redundant static frames captured at a rate of 25 frames per second. The approach involves the identification and removal of redundant frames through the analysis of changes in motion detection boxes. By implementing this technique, the processing load is reduced, thereby improving speed, particularly during feature extraction and matching. The method includes video segmentation to isolate relevant portions and extract the Region of Interest (ROI) for event retrieval. Furthermore, video super frame segmentation is employed to partition the video sequence into specific subsets based on predefined rules. Additionally, an image quality assessment method is utilized to efficiently distinguish between high-quality professional images and low-quality snapshots, ultimately leading to enhanced processing and analysis efficiency in traffic surveillance scenarios [8].

A method integrates Fractional Grey Wolf Optimization and a multi-objective cost function for efficient data hiding. Key frames are selected using the Structural Similarity Index measurement (SSIM) to ensure optimal concealment. These frames undergo region division through grid lines, with the optimization algorithm determining the best regions based on criteria like energy, coverage, intensity, and kurtosis. Security is enhanced by encrypting secret data before embedding it into the video stream using Fractional Grey Wolf Optimization. This integration ensures efficient and secure data hiding. The systematic process involves key frame extraction, optimal region selection, encryption, embedding using lifting wavelet transform (LWT), standardization of the cover video, and data extraction. Pre-processing steps such as key generation, nonlinear diffusion, and wavelet transform enhance encryption and embedding techniques. The retrieval process involves extracting secret information from optimal regions, ensuring data remains secure and accessible only to authorized recipients [10].

An approach combines Least Significant Bit (LSB) manipulation with Huffman Coding to efficiently embed and compress data within multimedia files. By adjusting 3 bits per

RGB pixel in images with a 24-bit depth, substantial data can be hidden within the image pixels without noticeable visual alterations. This method takes advantage of the human eye's limited sensitivity to minor color changes resulting from LSB modifications, ensuring that the concealed information remains undetectable. The integration of Huffman Coding further improves data storage efficiency by assigning variable-length codes based on character frequencies, facilitating effective compression while preserving accurate data retrieval during decoding. This combined strategy, referred to as the Combination of LSB and Huffman Coding, presents a robust solution for securely embedding and compressing data in multimedia content, maintaining a balance between storage capacity, data integrity, and visual fidelity [11].

3. PROPOSED METHODOLOGY

The proposed approach merges cryptographic and steganographic methods to boost security. Initially, data goes through multiple processing stages, starting with encryption and DNA embedding before being integrated into an MPEG4 video, used as the cover medium. This process entails segmenting the video into frames for later embedding. During embedding, appropriate frames are selected to avoid visible artifacts that could aid attackers in finding hidden information. DNA serves as the cover medium for the cryptographic message in Fig. 1. Extraction of the original message from the stego video follows a detailed data extraction procedure, as shown in Fig. 2.

This involves identifying complex frames housing encrypted content, pinpointing embedded pixels within frames and decrypting the extracted data using Caesar cipher encryption, revealing the concealed text. The data extraction module replicates the encryption phase's parameters, segmenting the stego video into frames under identical conditions as during encryption. Utilizing a frame embedding algorithm, complex frames with encrypted content are singled out, and pixel bits are retrieved in a specific order from these frames. These bits, representing index values in reference DNA, undergo transformation per DNA complementary rules, leading to decryption via Caeser cipher encryption and ultimately unveiling the hidden text.

4. SYSTEM DESIGN

The proposed approach enhances security by combining cryptographic and steganographic techniques. Initially, data is encrypted using the Caeser cipher algorithm, transforming it into an unreadable format. This encrypted data is then encoded into a DNA sequence, leveraging the complexity and high storage capacity of genetic codes for an additional layer of obscurity as in Fig 1.

Next, the DNA-encoded data is embedded into an MPEG4 video file. The video is segmented into individual frames, with specific frames selected for embedding to avoid visible artifacts. To extract the original message, the algorithm identifies the frames containing the embedded data used for embedding. The data is then extracted and decrypted using the Caesar cipher algorithm, revealing the concealed text. This multi-layered security approach effectively protects confidential information by combining DNA encoding, Text encryption, and strategic embedding in video frames. The extraction process mirrors encryption parameters as shown in Fig 2, separating the stego video into frames for retrieval, embedding bits from complex frames, transforming using DNA rules, and decrypting with Caesar cipher encryption to reveal the hidden text.

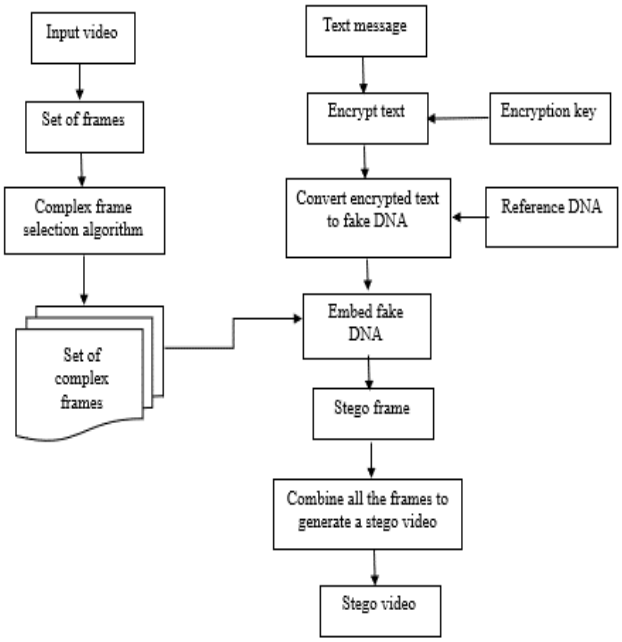

Fig 1. System architecture.

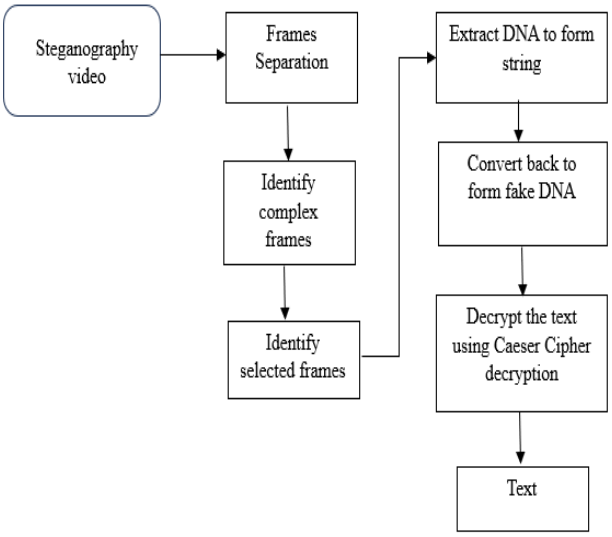

Fig 2. Extraction module.

5. IMPLEMENTATION

Implementing video steganography with DNA and complex frames follows a structured process to hide data within the video bases. discreetly. Initially, data undergoes encoding into DNA sequences, translating binary information into nucleotide bases. Complex frames, distinguished by features like rapid motion or intricate patterns, are chosen as prime locations for embedding the DNA sequences to minimize visual impact. During extraction, embedded DNA sequences are detected and extracted from the complex frames, then decoded into binary data to uncover the hidden information. Testing evaluates

imperceptibility, capacity, and robustness against attacks, refining implementation for optimal performance. Ethical considerations ensure responsible deployment, adhering to legal and ethical standards, while ongoing research enhances efficacy and resilience against detection methods.

A. Frame selection algorithm

Algorithm: Frame Selection Algorithm
Input: Video P (sequence of frames)
Output: Array of selected complex frames
Step 1: Preprocessing
- Take input video P as a sequence of frames.
- Define a complex frame as one significantly differing from its preceding frame.

Step 2: Discrete Cosine Transform (DCT)
- Perform DCT on each frame of video P.
- Convert spatial information into frequency data for analysis.

Step 3: Calculate Mean
- Calculate the mean value of DCT coefficients for each frame.
- Measure the energy distribution or content in the frequency domain.

Step 4: Identify Complex Frames
- Compare mean values of consecutive frames' DCT coefficients.
- Identify frames with significant changes in frequency content.
- Store identified complex frames in an array.

Step 5: Output
- Output the array containing selected complex frames.

B. Data Encryption Algorithm

Algorithm: Data Encryption Algorithm
Input: Cipher text M
Output: Fake DNA
Step 1: Convert Cipher Text to Binary
- Convert M into binary representation M′.

Step 2: Apply DNA Complementary Rule
- Apply DNA complementary rule to each binary pair Xi in M′ to get modified binary M′′.

Step 3: Iterate Through Modified Binary
- Iterate through modified binary M′′

Step 4: Process Iterated Pairs
- Perform a specific operation for each pair X′′i in M′′.

Step 5: Generate Fake DNA
- Use modified binary pairs X′′i to generate fake DNA.

6. RESULTS

Results are discussed for video file named input_video.mp4 file that has a duration of 5s and a file size of 1.031 Mb. In the input video file, there are 132 frames in total, provided a message *"We are Engineers"* for encryption, and chooses a key value of 12. The algorithm requires 2 security paths to encrypt the data. One is for the encryption of data using the cipher and the other is a reference DNA for building a fake DNA sequence out of the encrypted text. Reference DNA used is reference_DNA = {'00': 'A', '01': 'T', '10': 'C', '11': 'G'}. The text has been encrypted using Caesar cipher. We have analyzed the method using Mean Squared Error, Peak Signal to Noise Ratio of the steganographic video frames.

Table 1: Cover video details

File (Mpeg-4)	Durations (s)	Size (MB)	Total frames	Selected frame
Bunny	5	1.03	132	39
Lesson	10	2.87	256	61
Earth	30	1.53	901	531

A. Mean Squared Error (MSE)

Aggregating the differences between the corresponding pixel values of the original and the stego video frame mean square error is calculated. We calculate the difference between the original and the stego video frame, and divide the total by the frame' s size using formula, MSE = h n=1 h n=1 Cc ij − sc ij. Two bytes are selected of the color c at the (i, j) location from the original frame and stego frame here in called the Cij c and Sij c respectively, c is the color component, w = width of image, h = height of image.

Tab. 2 shows the MSE values derived from video using the proposed algorithm and random frame selection strategy. The Tab.2 shows that the suggested approach gives improved result for the proposed approach as it has a lower MSE value than the other two algorithms.

Table 2: Results for MSE

Name of video file	Proposed mechanism	Algorithm [3]	Algorithm [6]
Bunny	1.479e-04	1.649e-01	1.8181e-04
Lesson	1.2049e-04	1.653e01	1.7484e-05
Earth	1.7606e-05	1.139e01	2.8247e-06

B. Peak Signal to Noise Ratio (PSNR)

The quality of an image corrupted due to noise and blur can be measured using PSNR. It is used to determine the degree of similarity between the original and stego frames by calculating the difference between them. Higher the value of PSNR, indicates higher the quality rate and more similarity between the two frames. MSE is in directly proportional to the PSNR. PSNR is computed by using the following formula PSNR = 10log10 Maxl2/MSE, Where Maxl2 denotes the highest pixel value of a RGB image, (8 bits for each making one pixel is equal to 24 bits). PSNR is calculated separately for each of the three channels, resulting in a maximum value of (28–1) = 255. The suggested algorithm's results were compared to video Steganography employing random frame selection techniques. We created three videos with the same resolution and framerate as for comparison. The PSNR of the proposed approach, algorithm [14] and algorithm [6] are compared in Tab. 3.

Table 3: Results for PSNR

Name of video file	Proposed mechanism	Algorithm [3]	Algorithm [5]
Bunny	37.2126	36.8241	32.1959
Lesson	34.3982	33.8256	25.3075
Earth	3 5.8532	34.712	31.1546

7. CONCLUSION

The method titled "Video Steganography with DNA and Complex Frames" introduces a novel approach by employing an innovative frame selection algorithm. This involves the creation of fake DNA, utilizing DNA's inherent cutting properties for this purpose. These fabricated DNA sequences are then strategically embedded into specific frames of a cover video using a newly proposed frame selection algorithm that incorporates scene change detection. Following the frame selection process, the fake DNA is concealed within pixel locations.

The effectiveness of this technique is evidenced by its ability to maintain video perceptibility at a high level, minimizing the chances of immediate detection. Moreover, it demonstrates superior embedding efficiency, as indicated by reduced Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), showcasing its superiority over previously discussed techniques. This study underscores the critical role of intelligent frame selection in preserving video quality, as many embedding schemes without such intelligence can inadvertently introduce perceptible anomalies into the video, potentially revealing the presence of hidden data. Consequently, the fusion of an advanced frame selection methodology with enhanced embedding techniques presents a robust solution for securely transmitting steganographic videos across various communication channels.

REFERENCES

[1] Asma Sajjad, Humaira Ashraf, NZ Jhanjhi, Mamoona Humayun, Mehedi Masud and Mohammed A. AlZain, “Improved Video Steganography with Dual Cover Medium, DNA and Complex Frames”, Computers, Materials & Continua 2023, 74(2), 31 October 2022.

[2] Shaohua Wan, Xiaolong Xu, Member, Tian Wang, Zonghua Gu, “An Intelligent Video Analysis Method for Abnormal Event Detection in Intelligent Transportation Systems”, IEEE Transactions on Intelligent Transportation Systems, July 2021.

[3] N. Kar, K. Mandal and B. Bhattacharya, “Improved chaos-based video steganography using DNA alphabets,” ICT Express, vol. 4, pp. 6–13, 2018.

[4] Partha Saha, Lubna Yasmin Pinky, Mohammad Ashraful Islam, Papia Akter, “Higher Payload Capacity in DNA Steganography using Balanced Tree Data Structure”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019.

[5] Z.L.Yi and Z.W.Dong, “A novel steganography algorithm based on motion vector and matrix encoding,” in Proc. IEEE 3rd Int. Conf. on Communication Software and Networks, Xian, China, pp. 406–409, 2011.

[6]S.Mumthas and A.Lijiya, “Transform domain video steganography using RSA, random DNA encryption and huffman encoding”, in Proc. Computer Science, Cochin, India, vol. 115, pp. 660–666, 2017.

[7] Marghny H. Mohammed and Alaa Abdel-Razeq, “DNA-based steganography using genetic algorithm”, Information Science Letters, 1 Sept. 2020.

[8] Malathi Pa, Manoaj Ma, Manoj Ra, Vaikunth Raghavana, Vinodhini R Ea, “Highly Improved DNA Based Steganography”, 7th International Conference on Advances in Computing & Communications, ICACC-2017, 22- 24 August 2017, Cochin, India.

[9] Nirmalya Kar, Kaushik Mandal, Baby Bhattacharya, “Improved chaos-based video steganography using DNA” alphabets, ICTE 126, ICT Express, Jan 2018.

[10] Gat Pooja Rajkumar, Virendra S Malemath, “Video Steganography: Secure Data Hiding Technique”, I. J. Computer Network and Information Security, Sept 2017.

[11] Qabeela Q. Thabita, Alaa A. Al-saffarb and Issa Ahmed Abedb, “A new DNA strand-based encryption algorithm using symmetric key generation table”, Al-Qadisiyah Journal for Engineering Sciences, February, 2022.

[12] I. P. Febin, K. Jayasree and P. T. Joy, “Violence detection in videos for an intelligent surveillance system using MoBSIFT and movement filtering algorithm,” Pattern Analysis and Applications, vol. 23, no. 2, pp. 611–623, May 2020.

[13] Meenu Suresh a, I. Shatheesh Sam B, “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,15 August 2022.

[14] Shwe Sin Myat Than, “Secure Data Transmission in Video Format Based on LSB and Huffman Coding”, I.J. Image, Graphics and Signal Processing, 2020.

[15] M.Ramalingam, “Stego machine–video steganography using modified LSB algorithm,” World Academy of Science, Engineering and Technology, vol. 74, pp. 502–505, 2011.