International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 5, May, 2025, pp. 1007-1018
Journal homepage: http://iieta.org/journals/ijsse

Video Steganography Using a 9-D Chaotic System and an Encryption Algorithm for Data Hiding

Suhad Naji Al-Rekaby*, Maisa'a Abid Ali Khodher, Layth Kamil Adday

Department of Computer Engineering, University of Technology, Baghdad 10001, Iraq

Corresponding Author Email: ce.23.02@grad.uotechnology.edu.iq

https://doi.org/10.18280/ijsse.150514

Received: 11 March 2025
Revised: 20 April 2025
Accepted: 18 May 2025
Available online: 31 May 2025

Keywords:
Advanced Encryption Standard (AES), chaotic logistic map, cryptographic key generation, data hiding, information security, least significant bit (LSB) embedding, secure data transmission, steganographic embedding, text encryption, video steganography

ABSTRACT

This research introduces a robust steganographic framework that combines data encryption with video encoding to conceal encrypted data effectively. A nine-dimensional logistic map is employed for key generation, resulting in significant chaos before implementing the Advanced Encryption Standard (AES) for text encryption. The generated ciphertext is integrated into video frames using the Least Significant Bit (LSB) technique, which ensures visual quality is maintained while reducing the likelihood of detection. The system's performance was assessed through various security evaluations and quality metrics. Experimental findings indicate that the proposed technique achieves a Peak Signal-to-Noise Ratio (PSNR) of 87.5 dB and a Structural Similarity Index Measure (SSIM) of 1.0000. Moreover, the method passed 14 out of 16 National Institute of Standards and Technology (NIST) randomness tests and attained an entropy value of 7.99. These results validate the method's efficacy in preserving both video quality and cryptographic strength and robustness against statistical attacks.

1. INTRODUCTION

Contemporary cyber threats, ongoing data breaches, and espionage activities have driven organizations to pursue more effective data protection strategies. The increasing inadequacy of traditional encryption and steganography methods has led to the investigation of quantum-resilient solutions. For instance, the research detailed in the study [1] introduces a two-phase chaotic confusion-diffusion framework that exhibits significant resilience against differential and occlusion attacks stemming from activities such as espionage, theft, and hacking—challenges that are paramount for organizations, companies, governments, and individuals alike the study [2]. Digital data, encompassing financial, personal, commercial, military, medical, or political information, has emerged as a prime target for professional and amateur hackers [3]. Encryption and masking techniques are essential to safeguard sensitive information during storage and transmission [4]. Encryption transforms data into an unintelligible format using various algorithms and an encryption key, aiming to thwart unauthorized access [5]. Steganography is another essential technique in which data is hidden within digital media such as videos, audios, and images without degrading their quality, making the concealed content difficult to detect [6]. This paper presents a novel hybrid approach to address these issues by integrating a 9-D chaotic system for key generation with AES encryption and steganography within video frames. The 9-D chaotic system bolsters encryption security via AES, making key prediction exceedingly challenging. It guarantees a well-distributed value set, reducing repetition and expanding the key space to render brute-force attacks impractical. Furthermore, incorporating complex mathematical characteristics complicates key extraction and bolsters resistance against analytical and mathematical attacks. This approach balances security and efficiency by effecting a seamless integration with AES while maintaining speed. Ultimately, it enhances data security when using LSB in video, significantly complicating the retrieval of hidden data without the appropriate key. This establishes it as a robust solution for data protection. Although numerous studies have explored encryption and information hiding techniques using various algorithms, most have focused either on generating encryption keys using two- or three-dimensional chaotic systems or other forms of chaotic structures. Others have addressed encryption and data hiding without clearly separating the two processes. Additionally, some prior works rely on specific image or video formats, limiting the proposed systems' overall efficiency and applicability. Moreover, many of these approaches have demonstrated limited resistance to statistical and cryptanalytic attacks. Therefore, a critical need remains for developing a more efficient, flexible, and secure data hiding system.

This study introduces a robust framework for concealing textual data within video frames through combined encryption and embedding techniques systematically and efficiently. The process begins with creating an encryption key using a 9-D chaotic logistic model. This key is then employed in the Advanced Encryption Standard (AES) algorithm to encrypt the target text. Following encryption, the text is embedded into video frames using the least significant bit (LSB) technique. The delineation and organization of these phases constitute a significant advancement in the domain.

Various metrics, such as entropy, PSNR, and the NIST randomness tests, were used to assess the proposed system's efficacy. The experimental findings show that the system attains elevated security levels while maintaining video quality, setting it apart from numerous existing approaches. This study adds to the literature by introducing several significant innovations, starting with designing a 9-D chaotic logistic system that functions as a secure key generator, offering improved sensitivity and randomness. The chaotic key is integrated into the AES encryption process before data embedding. A steganographic protocol based on LSB is then employed to embed the encrypted text within the video frames. A thorough evaluation of the system, conducted using entropy, PSNR, SSIM, and NIST statistical tests, validates the security and imperceptibility of the approach.

Extensive experimental analysis validates the proposed approach's outperformance of recent techniques in terms of cryptographic robustness and video quality preservation.

The remainder of this paper is organized as follows: Section II reviews related work. Section III describes the proposed system, including the key generation, encryption, and embedding procedures. Section IV presents the experimental results and performance evaluation. In conclusion, Section V summarizes the paper's findings and suggests avenues for future research.

2. RELATED WORKS

The swift advancement of communication technologies and mobile applications has significantly increased the demand for protecting both transmitted and stored information. Consequently, several studies have explored different encryption and steganographic techniques designed to enhance data security.

In 2023, Kunhoth et al. [1] conducted a comprehensive review of video steganography techniques suitable for compressed and uncompressed data. Their analysis included techniques such as least significant bit (LSB) substitution, discrete wavelet transforms (DWTs), and discrete cosine transforms (DCTs). They also explored video steganalysis methods and metrics for evaluating performance. The review provides a comparative assessment of contemporary steganography techniques, emphasising their imperceptibility, robustness, and capacity. It addresses various challenges, such as security vulnerabilities, trade-offs between robustness and capacity, and vulnerability to steganalysis attacks.

In 2020, Guan et al. [2] proposed a novel technique for commutative encryption and data hiding designed explicitly for high efficiency video coding (HEVC) video. The method facilitates the simultaneous encryption and concealment of data while maintaining the original bit rate. The technique emphasizes the selective encryption of quantized transform coefficients (QTCs) and motion vector differences (MVDs) while modifying QTC values to accommodate data embedding. It effectively preserves visual quality, increases embedding capacity, and maintains compatibility with the HEVC standard. This allows for the extraction of the encryption status. However, it depends on strong encryption keys for security, incurs a significant computational overhead, and is limited to HEVC video formats, making it impractical for older video files.

In 2022, Kou et al. [3] introduced a 7-D complex chaotic encryption system that uses a cubic memristor specifically engineered for secure data transmission within innovative grid applications. This approach leverages a high-dimensional chaotic framework to generate robust encryption keys exhibiting high unpredictability. It ensures substantial randomness, is strongly resistant to cryptanalysis, and has an extensive key space, making it exceptionally secure for safeguarding smart grid data. Nonetheless, the methodology demands significant computational resources, restricting its applicability in low-power devices. Moreover, chaotic encryption systems may face synchronization challenges, potentially resulting in data loss.

In 2021, Albahrani et al. [4] performed a comprehensive examination of encryption techniques that use chaotic maps to safeguard audio transmissions. Their findings indicate that these encryption methods offer improved security thanks to their extensive key spaces and sensitivity to initial conditions. A comparative study of alternative techniques confirmed the superiority of chaotic systems in foiling unauthorized access to audio information. Nevertheless, these methods lack stability regarding large audio files, sufficient resilience against hybrid attacks, and struggle to balance security with real-time performance.

In the same year, Vivek and Gadgay [5] introduced a video steganography system based on chaotic encryption, incorporating an enhanced LSB (ELSB) method to securely embed data in HEVC videos. The algorithm applies logistic and Hénon chaotic maps and ensures data integrity before compression. The system achieved a peak signal-to-noise ratio (PSNR) of 35.81 dB with an execution time of 40 seconds, outperforming the common H.264 compression technique (32.72 dB, 45 sec) in imperceptibility and security. However, it has a high computational complexity due to chaotic encryption and requires extended processing times for LSB embedding, making it less efficient for real-time use.

In 2023, Salunke et al. [6] proposed a 3D Gauss encryption compression technique using multiple chaotic keys and Lyapunov exponent validation to enhance security and resistance to brute-force attacks. Despite its enhanced encryption strength and compression, the decryption process demands significant computational resources.

In 2024, Fadhil et al. [7] introduced a method for text encryption and embedding that uses Salas20 encryption alongside Harris corner detection to improve both security and imperceptibility. Although this approach outperforms traditional LSB techniques, its dependence on texture-based embedding could limit its effectiveness in low-texture videos.

In 2024, Meng et al. [8] introduced a secure and efficient coverless video steganography technique that relies on inter-frame similarity. This system creates a secret communication video database (SCVD) using publicly available video data. The SCVD organizes videos according to the similarity of frames between their start and end points using time-based video properties. A mapping table links particular video sequences from the SCVD with segments of confidential information. This mapping serves as a standard reference for both the sender and the receiver, facilitating the embedding and extraction of data without modifying the content of the video. By removing the need for extensive auxiliary data and preventing alterations to the cover medium, the system improves security and maintains the covert nature of coverless steganography. Experimental findings indicate that the proposed method provides enhanced security, capacity, and robustness compared to existing techniques, effectively mitigating the risks of transmitting substantial additional information prevalent in other coverless video steganography methods.

In 2024, Kale et al. [9] presented an innovative video steganography system that secures information by invisibly embedding text within video frames and audio streams. The approach employs unstructured frame selection methods and audio steganography techniques to expand data storage capabilities. Security is further improved using MD5 hashing, which preprocesses the text before embedding. This comprehensive methodology improves both the steganographic process's quality and the embedded data's security, ensuring high imperceptibility. Experimental results show that the method maintains audio and video quality standards while significantly enhancing data embedding capacity and resisting unauthorized access.

In 2024, Dai and Liu [10] tackled a security flaw in the AES algorithm arising from correlations among round keys. Their research employs chaotic systems, including Logistic and Tent maps, to generate highly random sequences that improve AES security. These sequences are used to produce round keys that reduce inter-key correlation. The enhanced key expansion algorithm ensures an ample key space and generates unique encryption keys per session, adhering to the "one secret at a time" principle. Experimental analysis shows that the proposed model eliminates key dependencies, generates robust random sequences, and strengthens resistance to cryptographic attacks.

In their 2024 study, Harsha and Gopika [11] have highlighted the essential role of image protection methods in safeguarding sensitive medical information, military communications, and personal digital data. This review article presents an in-depth examination of modern image encryption techniques. It assesses both traditional symmetric and asymmetric algorithms and more advanced methods such as chaos-based, quantum-based, and hybrid systems. The paper aims to provide researchers and practitioners with a comprehensive understanding of existing encryption methodologies to facilitate the advancement of robust and effective technologies. As a review, it consolidates insights from previous research rather than offering experimental findings, and it critically assesses the advantages and limitations of various encryption strategies.

In 2025, Badhan and Malhi [12] introduced a novel data security architecture that combines various cryptographic techniques to efficiently and comprehensively secure data. Their innovative system uses AES for data encrypting due to its speed and reliability. Elliptic Curve Cryptography (ECC) is used to secure the AES keys, capitalizing on ECC's lightweight structure and robust secure key exchange mechanisms. To achieve steganographic concealment, the architecture employs an LSB technique, which allows for embedding encrypted data within image files. Furthermore, the system incorporates WebP compression to minimize storage requirements and enhance data transmission efficiency. A multi-tiered security framework is established to meet the demands of contemporary secure communication networks. Experimental evaluations reveal impressive performance, with a PSNR of 68.90 and a Mean Squared Error (MSE) of 0.0083, signifying exceptional image quality following data embedding.

In 2024, Shetty et al. [13] introduced a comprehensive data security framework integrating cryptographic and steganographic methods to achieve efficiency and total confidentiality. The system utilizes AES for the primary data encryption due to its speed and reliability. At the same time, ECC is employed for encrypting AES keys, leveraging its lightweight design and robust key exchange security features. Encryption is further enhanced by applying steganography, specifically the LSB technique, effectively hides encrypted information within image files. The framework integrates Web compression to optimize storage space and improve transmission efficiency. Experimental findings validate the success of this layered strategy, demonstrating a PSNR of 68.90 and an MSE of 0.0083. This indicates negligible distortion and superior image quality post-embedding.

In 2024, Verma and Kumar [14] developed a quantum image encryption system that produces highly unpredictable pseudorandom sequences using a 3-D Bernoulli–Nahem–Map (3D-BNM) chaotic system. This innovative method integrates SHA-256 hash functions to enhance security. The framework converts traditional images into quantum images via the novel enhanced quantum representation (NEQR) format. It subsequently applies spatial scrambling through the generalized quantum Arnold transform (GQAT), followed by qubit-level controlled diffusion facilitated by C-NOT and CC-NOT quantum gates. Experimental evaluates show that this system demonstrates strong resistance to both statistical and differential attacks, all while preserving a low level of computational complexity.

In 2024, Khan et al. [15] introduced an innovative one-dimensional cosine-modulated-polynomial chaotic map to enhance image encryption techniques within Internet of Things (IoT) frameworks. This newly proposed chaotic map demonstrates an expanded chaotic range and possesses key attributes such as aperiodicity, ergodicity, heightened sensitivity to initial conditions, and lower structural complexity. The system successfully met all 17 NIST randomness criteria, and experimental evaluations such as bifurcation diagrams, Lyapunov exponents, and Kolmogorov entropy all validated the map's robust chaotic properties. These findings underscore its potential utility as a robust pseudorandom number generator for cryptographic applications.

Table 1 provides a systematic comparative analysis of the latest video steganography and encryption developments. Each row details the methodologies utilized alongside their key advantages and limitations. This comparative assessment aids in pinpointing current research gaps and guides the development of future studies. Compared to existing work, our scheme involving a Nine-Dimensional Chaotic Logistic System with AES encryption presents a new algorithmic technique for generating highly random keys that can enormously reduce the cryptanalysis. An optimized LSB embedding on video frames leads to perfect RD, while a rare combination of large capacity and low distortion is achieved.

Table 1. Comparative analysis of recent video steganography and encryption techniques

Year	Author(s)	Title	Journal/Conference	Technique(s)	Advantages	Disadvantages
2024	Fadhil et al. [7]	A Proposed Text Encryption Inside Video Using Harris Corner Detection and Salas20 Encryption Algorithm	Engineering and Technology Journal	Salsa20 + Harris Corner Detection	Precise text localization; enhanced stealth	Performance is limited in low-texture content

2024	Kale et al. [9]	Video Steganography with Text in Frame and Audio using MD5 Hashing	Journal of King Saud University – Computer and Information Sciences	Frame and audio steganography + MD5	Increased embedding capacity via dual modality	Synchronization complexity between audio and video
2024	Dai and Liu [10]	Secure AES with Chaotic Logistic and Tent Mapping for Session-Based Encryption	IEEE Access	AES + Logistic and Tent maps	Enhanced key randomness; session-level security	High resource consumption for key generation
2025	Badhan and Malhi [12]	Multilevel Security for Data Using ECC-AES and LSB Steganography	IEEE Access	ECC-AES + Inverted LSB	Efficient key exchange; layered data protection	Less suitable for lightweight systems
2024	Shetty et al. [13]	Enhanced ECC-AES and Inverted LSB with WebP Compression for Secure Image Communication	IEEE Access	ECC-AES + LSB + WebP	High imperceptibility; efficient storage	Increased processing time due to compression
2020	Guan et al. [2]	Commutative Encryption and Data Hiding with HEVC	IEEE Transactions on Multimedia	Encrypt QTCs + embed in MVDs (HEVC)	Maintains video bitrate; dual-layer protection	HEVC-specifc; incompatible with older formats
2021	Vivek and Gadgay [5]	Chaotic LSB Video Steganography with Logistic and Henon maps	Alexandria Engineering Journal (Elsevier)	LSB + Logistic + Henon chaotic maps	High PSNR; secure over H.264	Computationally intensive
2024	Meng et al. [8]	Coverless Video Steganography Using Inter-Frame Similarity	IEEE Transactions on Multimedia	Inter-frame mapping + coverless embedding	No modification of video; high stealth	Requires a shared SCVD for decoding

3. METHODS AND MATERIALS

3.1 Dynamic encryption key generation is performed using a 9-D logistic map

This approach ensures high randomness, rendering value duplication nearly impossible.

Moreover, it enhances the complexity of the encryption process, thereby increasing the system's resilience against chaos analysis and brute force attacks.

3.2 AES encryption is further refined by employing chaotic values

Subkeys are generated dynamically, ensuring that each encryption round is unique.

This strategy maximizes the avalanche effect and mitigates the risk of statistical attacks.

3.3 Frame selection is conducted randomly using chaotic values

This method improves the concealment process and diminishes the likelihood of detection.

3.4 Text is dynamically concealed within the LSBs

The selection of appropriate bits is guided by values generated from chaotic maps, which hinders the easy extraction of hidden data.

Furthermore, ciphertexts are unpredictably allocated to the frameworks, bolstering security.

This research attains a significant level of security in the encryption and concealment of texts within a video, making detecting or extracting hidden data exceedingly challenging.

4. THE PROPOSED SYSTEM

This section outlines the framework of the proposed system, which incorporates various algorithms, such as steganography, AES, and a 9-D chaotic system. These methodologies work in tandem to bolster security and ensure resilience against potential attacks by leveraging the advantages of established cryptographic techniques. Figure 1 illustrates the framework.

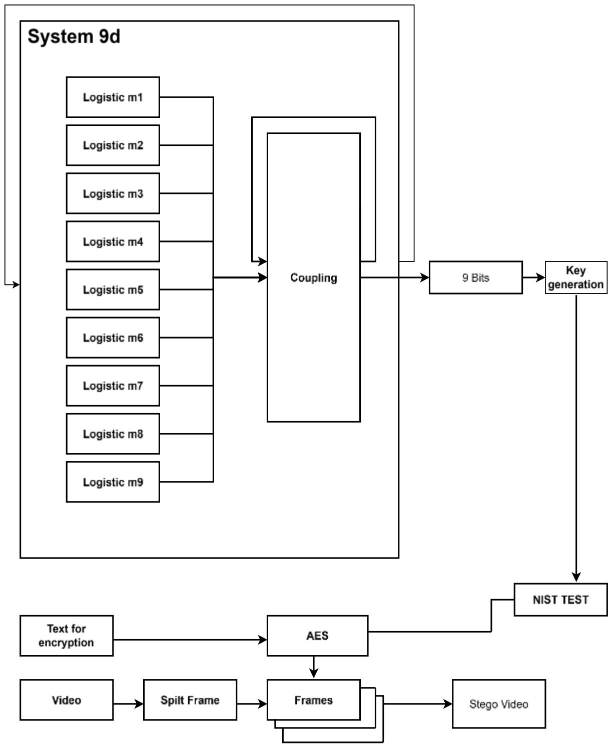

Figure 1. A hybrid framework for the proposed system

4.1 Key generation mechanism based on the 9-D chaotic logistic system

The 9-D coupled chaotic logistic system exhibits complex chaotic behavior, making it a strong candidate for cryptographic key generation. The system is defined using nine coupled logistic maps.

4.1.1 The 9-D logistic system

The following equation governs the behavior of this system:

$$x_i^{t+1} = r_i \cdot x_i^t \cdot (1 - x_i^t) + \epsilon \cdot \sum_{\substack{j=1 \\ j \neq i}}^{9} (-1)^{i+j} x_j^t \tag{1}$$

where,

x_i^t = the state of the i, the logistic map at time step t;

$r_i = 3.99$ the chaos parameter, whose value ensures the system operates in a fully chaotic regime;

$\epsilon = 0.015$ the coupling strength, which links all maps together.

The initial values are taken to be

$$X = [0.123456789, 0.234567890, 0.345678901, 0.456789012, 0.567890123, 0.678901234, 0.789012345, 0.890123456, 0.987654321].$$

These values are chosen to avoid falling into fixed points or periodic orbits. A burn-in phase of 1000 iterations is used to eliminate transient effects. For key generation, 111 112 iterations are performed after the burn-in phase. The outputs are binarized with a threshold of 0.516. The threshold of 0.015 was chosen after testing various values. It provided the best balance between detected units and false alarms. Lower values caused excessive alerts, while higher ones missed important data. Thus, 0.015 ensured better accuracy and stability.

4.1.2 Chaotic key generation process

Keys are generated according to the following procedure.

1. **System initialization:**

The nine logistic maps start from predefined initial conditions.

Burn-in iterations are performed to remove transient effects.

2. **Iterative chaotic map computation:**

At each iteration, all x_i values are updated using the logistic equation and coupled interactions.

3. **Binary key extraction:**

The output values are compared with a threshold (0.516).

If $x_i \geq 0.516$, then the corresponding bit is set to 1; otherwise, it is set to 0.

The system achieves high entropy and generates a truly random-like sequence. Since the system operates in nine dimensions, the generated keys are taken from an ample space, making brute-force attacks impractical. In addition, it is irreversible without the exact knowledge of the initial conditions.

4.2 Visual analysis of the chaotic system

Figure 2 shows a time-series representation of the 9-D logistic map over multiple iterations, demonstrating its chaotic behavior. Each panel corresponds to a dimension. The wide distribution of values from 0 to 1 confirms the unpredictable nature of the system.

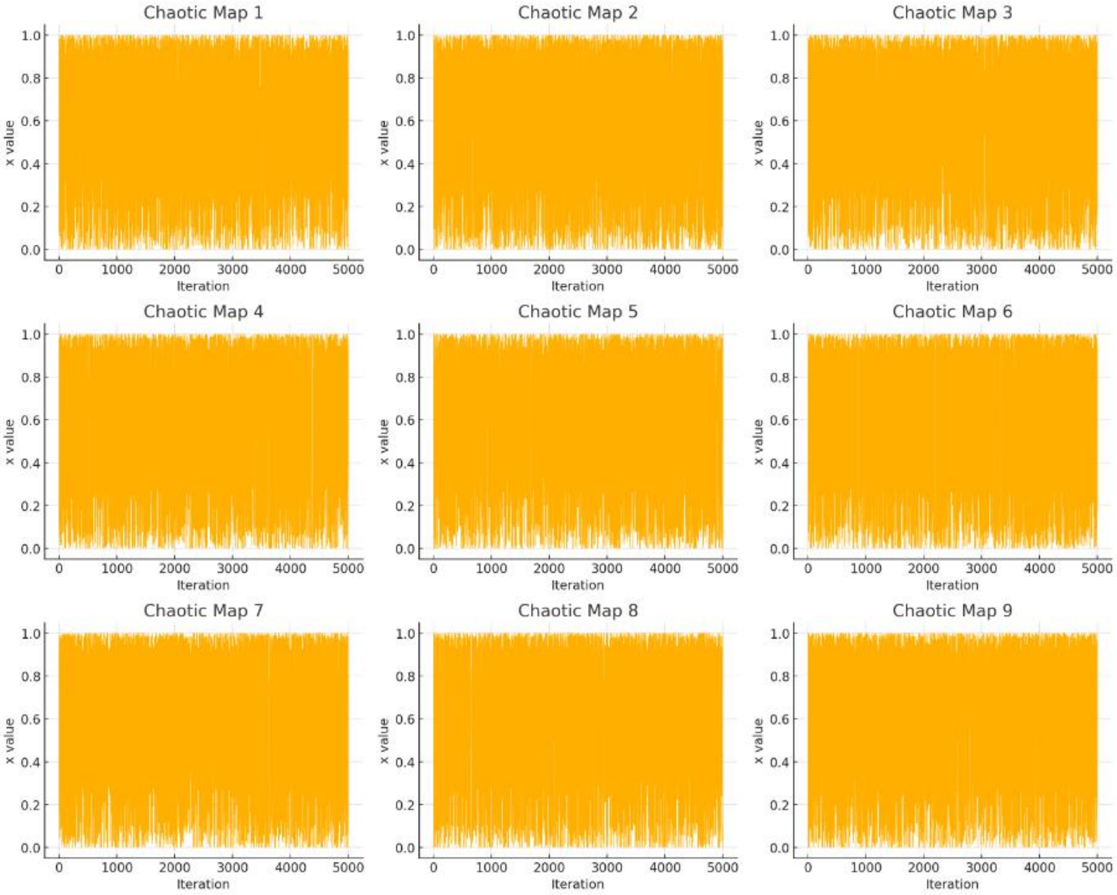

Figure 2. Chaotic behaviors of nine logistic maps

4.2.1 3-D representation of chaotic behavior

To illustrate the interaction between the variables in the chaotic map, Figure 3 shows a 3-D phase plot for the first three. The scattered distribution of points confirms the nonlinear and nonperiodic nature of the chaotic system and demonstrates its suitability for cryptographic key generation.

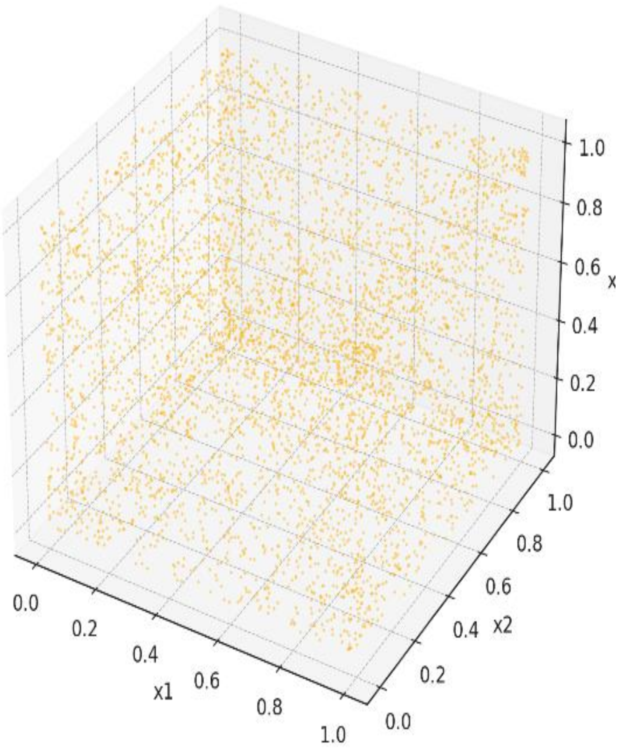

Figure 3. 3-D phase plots of the chaotic system

4.2.2 Distribution of chaotic values

The histogram in Figure 4 illustrates the distribution of values generated by the 9-D logistic map. The relatively uniform spread, with peaks at the extreme values (0 and 1), confirms the system's high entropy, ensuring strong randomness for key generation.

4.3 Applications in cryptography

The extracted binary sequence is formatted into 256-bit AES keys for AES key generation. The keys are used for secure data hiding in video frames. This ensures high-security key generation with enhanced unpredictability and robustness.

4.3.1 Secure data hiding and steganography in video using the AES and LSB algorithms

The text encoding and decoding process involves converting the ciphertext from base 64 to binary data using AES encryption. The information is divided into two segments: the initialization vector and the encrypted information. The initialization vector is used to create an AES cipher object, which is decoded using AES decryption. The video is subsequently segmented into frames and saved in a designated output directory. The steganography procedure entails a statistical examination of the byte lengths of headers, which indicates the duration of concealed records. The LSB method is employed to conceal the information, with the hidden records dispersed across various frames and segmented into bytes for secure integration. The length of the initial frame is established by summing the first four bytes of concealed data. The hidden text is retrieved from the video, analyzed frame by frame, and reassembled into an image file.

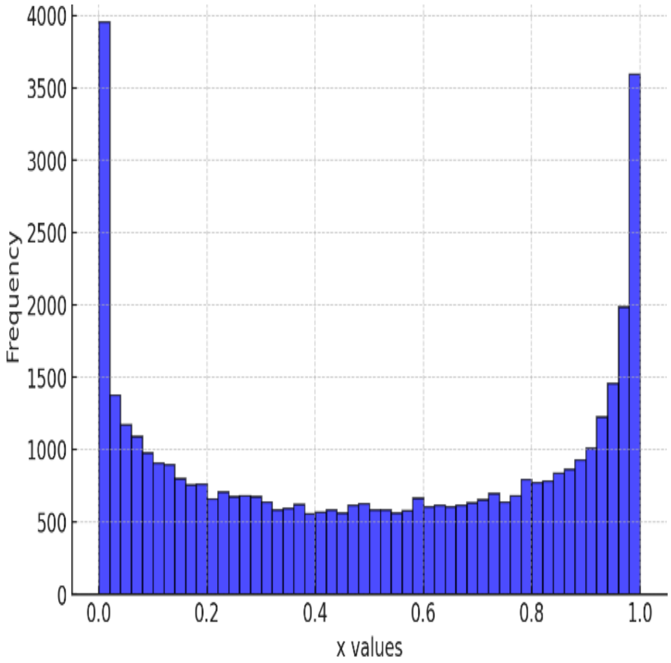

Figure 4. Histogram distribution of logistic maps

5. RESULTS AND TESTING

This section presents and analyzes the results derived from implementing the proposed system by applying statistical tests.

5.1 Key generation mechanism based on the 9-D chaotic logistic system

The key generation method utilizing the 9-D chaotic logistic system significantly improves security by producing extremely difficult-to-predict keys. This technique takes advantage of the intricacy of chaotic dynamics to provide strong encryption that can withstand brute-force attacks and key forecasting. Table 2 presents a selection of values derived from the 9-D chaotic equations, while the entire dataset comprises 111,112 iterations.

5.1.1 Importance of the NIST test suite and key strength evaluation

The NIST randomness test suite serves as a crucial benchmark for assessing the quality of cryptographic keys by evaluating their unpredictability and statistical randomness. This analysis conducted 16 distinct statistical tests on the generated keys. The keys successfully passed 14 of 16 tests (see Table 3). This outcome signifies a high level of randomness and security, affirming that the method demonstrates significant resilience against cryptanalytic attacks and rendering it appropriate for contemporary encryption systems.

Table 2. Sample result of the 9-D chaotic equations

Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6	Variable 7	Variable 8	Variable 9
0.982582592	0.036993143	0.979339986	0.134957276	0.517894404	0.793072746	0.909829637	0.992230015	0.160794339
0.077444106	0.14716712	0.061570413	0.497633508	0.958652599	0.688234468	0.292144834	0.064718791	0.516922781
0.291544651	0.49326185	0.239343041	0.982133861	0.166583302	0.851753228	0.835430538	0.234613584	0.996476471
0.819261068	0.999152023	0.728386822	0.056894824	0.579295613	0.468187698	0.584443666	0.689623641	0.02944226
0.586424411	0.005066542	0.791754939	0.221791519	0.956878804	1	0.950105021	0.871396726	0.106552964
0.978303531	0.018227896	0.647952291	0.707138756	0.135143515	0.028844083	0.161052168	0.476413526	0.362042098

Table 3. NIST tests for key generation

Test	*p*-value	Conclusion
Frequency test (monobit)	0.8665832790788309	Random
Frequency test within a block	0.997709365791613	Random
Run test	0.6599166566634166	Random
Longest run of ones in a block	0.9181901729231152	Random
Binary matrix rank test	0.4497406065863208	Random
Discrete Fourier transform (spectral) test	$4.6128486052932436 \times 10^{-5}$	Non-random
Non-overlapping template matching test	0.9344181980207866	Random
Overlapping template matching test	0.7128473873360851	Random
Maurer’s universal statistical test	0.9737619496847233	Random
Linear complexity test	0.027605021181555094	Random
Serial test	0.19491807545594395	Random
Approximate entropy test	$9.120896724038854 \times 10^{-139}$	Non-random
Cumulative sums (forward) test	0.9319452140593067	Random
Cumulative sums (reverse) test	0.898798411288936	Random
Random excursions test	0.08831465620980242	Random
Random excursions variant test	0.31744489871241155	Random

Table 4. Comparison of Lyapunov exponents and chaotic behavior for encryption suitability

Name	Lyapunov Exponent (Positive/Negative)	Chaotic Behavior	Suitability for Encryption
Proposed key generation system	Positive	Yes	Highly suitable
Salunke et al. [6]	Positive	Yes	Highly suitable
Nguyen et al. [16]	Positive	Yes	Highly suitable

Table 5. Randomness evaluation of encrypted text using the NIST test

Type of Test	*p*-Value	Conclusion
Frequency test (monobit)	0.31190931669831956	Random
Frequency test within a block	0.7188482626480919	Random
Run test	0.6925701750400248	Random
Longest run of ones in a block	0.8366734611882453	Random
Binary matrix rank test	0.12461606517623863	Random
Discrete Fourier transform (spectral) test	0.23094996037851234	Random
Non-overlapping template matching test	0.6352831237330236	Random
Overlapping template matching test	0.42484354133791924	Random
Maurer’s universal statistical test	−1.0	Non-random
Linear complexity test	0.30628890749596566	Random
Serial test	0.7914951442558571	Random
Approximate entropy test	0.6174723911380802	Random
Cumulative sums (forward) test	0.5174865811608715	Random
Cumulative sums (reverse) test	0.45636036550987175	Random
Random excursions test	0.022640504760700966	Random
Random excursions variant test	0.10247043485974941	Random

5.1.2 Evaluation of key strength using the Lyapunov exponent

The keys produced through the 9-D chaotic logistic map were evaluated using the Lyapunov exponent to determine their randomness. A positive value of 0.004547735804617423 was achieved, signifying robust chaotic behavior. This result confirms unpredictability, a high sensitivity to initial conditions, and resilience against attacks, rendering the method appropriate for encryption and secure communication.

Table 4 compares the proposed 9-D logistic map key generation system with current methodologies. The analysis reveals robust chaotic characteristics, evidenced by a positive Lyapunov exponent, which affirms its significant unpredictability. Consequently, this system is exceptionally well-suited for encryption, providing improved security and resistance to potential attacks.

5.2 Text encryption results

This subsection illustrates the efficacy of the proposed encryption technique, which integrates the AES algorithm with keys generated through the 9-D logistic map. A range of security metrics is employed to assess the robustness and randomness of the encrypted data.

5.2.1 NIST statistical analysis for text encryption randomness

The encrypted text underwent assessment using the NIST Statistical Test Suite, which comprises a series of statistical tests to determine the randomness of encrypted information. The method successfully passed 15 tests, affirming a high level of randomness; however, it failed two tests, suggesting the presence of identifiable patterns within the encrypted text. A comprehensive analysis is presented in Table 5.

5.2.2 Statistical analysis of encrypted text strength

This subsection provides a statistical assessment of the encrypted text to evaluate its security and randomness. The analysis encompasses the Hamming distance, the bit change rate (BCR), entropy, and a chi-square test. The findings are presented in Table 6.

The elevated Hamming distance and BCR values suggest substantial alterations in the bits, contributing to increased randomness and complicating the retrieval of the original text. Furthermore, the high entropy values and the chi-square test results affirm that the encrypted text demonstrates robust randomness, thereby enhancing its resistance to statistical analysis and decryption attempts. As illustrated in Table 7, the entropy values approach the optimal upper limit and exceed those reported in the study [13]. This signifies a considerable degree of randomness in the encrypted text, rendering it significantly more resistant to attacks and statistical scrutiny than the method presented in the study [13].

Table 6. Statistical analysis of encrypted text: Hamming distance, BCR, entropy, and chi-square test

Hamming Distance	BCR	Entropy	Chi-Square Statistic	Chi-Square *p*-Value
2070	49.01%	7.6175	271.0303	0.234270
990	48.34%	7.1320	270.000	0.247935
502	49.02%	6.9993	204.000	0.991786
2193	50.39%	7.9835	255.588	0.487184
398	51.82%	7.9943	234.6667	0.841809

Table 7. Comparison of entropy with an existing method

Text	Proposed Method	Ref. [7]
1	7.9835	7.2571
2	7.9943	7.3523
3	6.9993	6.8072

5.3 Segmentation video results

After the text encryption process, the video was segmented as illustrated in Figure 5 to prepare for embedding the encrypted text within selected frames for transmission. Ten frames were extracted from the video and utilized in the experiments to evaluate the effectiveness of the proposed methodology.

5.4 Steganography in video frames

Applying the LSB steganographic technique to conceal encrypted text within video frames offers a secure and efficient means of covert data transmission. This method embeds information in the least significant bits of the video frames, maintaining video quality while bolstering security against unauthorized access. Consequently, it is well-suited for confidential applications and secure communication. Table 8 outlines the videos utilized in this study.

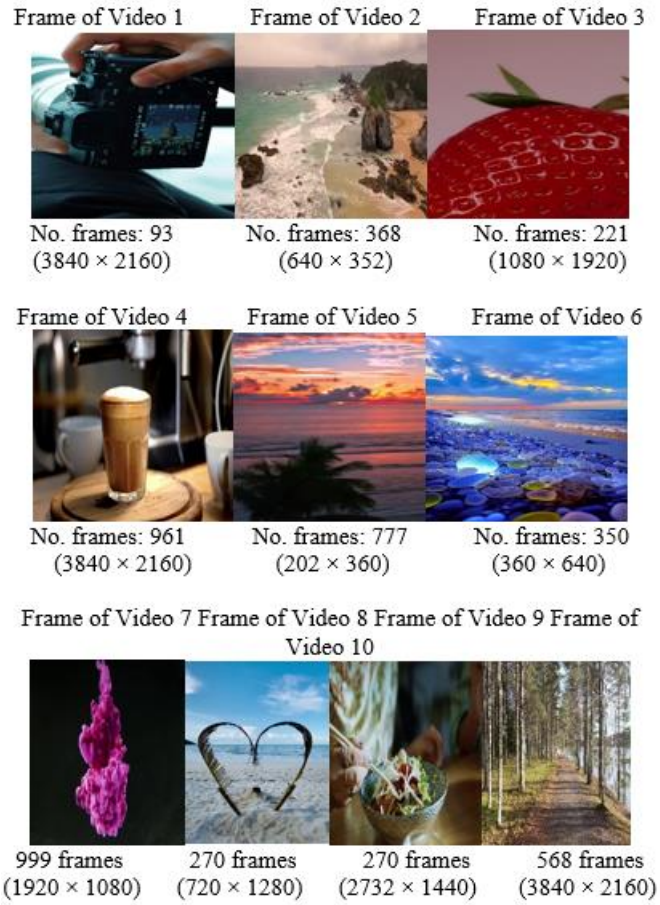

Figure 5. Experimental video dataset specifications

Table 8. Video file specification and attributes

Name	Resolution	No. Frames	Size of Video
Video 1	3840 × 2160	93 frames	6.75 MB
Video 2	640 × 352	368 frames	1.04 MB
Video 3	1080 × 1920	221 frames	5.10 MB
Video 4	3840 × 2160	961 frames	84.6 MB
Video 5	202 × 360	777 frames	863 kB
Video 6	360 × 640	211 frames	350 kB
Video 7	1920 × 1080	999 frames	19.1 MB
Video 8	720 × 1280	270 frames	686 MB
Video 9	2732 × 1440	740 frames	23.8 MB
Video 10	3840 × 2160	568 frames	494 MB

Table 8 illustrates the findings from assessing the steganographic technique applied to various video files. The evaluation incorporates several metrics, including the number of characters embedded, capacity, peak signal-to-noise ratio (PSNR), mean square error (MSE), structural similarity index measure (SSIM), entropy, number of pixels change rate (NPCR), unified average changing intensity (UACI), and correlation, to evaluate the effects of data embedding on both video quality and security. The findings demonstrate that the technique achieves a high level of imperceptibility, characterized by elevated PSNR values and minimal distortion (as indicated by low MSE), while maintaining structural similarity (SSIM = 1.0000). The SSIM value reported is 1.0000 when comparing video frames before and after embedding, not the entire video. These results validate that the optimal LSB embedding did not introduce visible distortion in the processed frames, achieving good imperceptibility and the effectiveness of the presented approach. Furthermore, the entropy and NPCR metrics indicate a robust level of randomness and security, confirming resistance to detection.

Tables 9 and 10 illustrates the proposed system's enhanced data-hiding capabilities compared to techniques employed in earlier research. The system achieves a PSNR of 87.5157 dB, which is markedly superior to the values reported in previous studies, which indicates minimal distortion in the video post-embedding. Furthermore, the significantly lower MSE value of 0.0001 corroborates that the visual effect of the concealed data is negligible. Additionally, the proposed system achieves an impeccable SSIM score of 1.0000, indicating near-perfect similarity between the original and stego-videos, in contrast to the slightly lower SSIM scores observed in prior studies. These findings underscore the efficacy of the proposed system in maintaining video quality while facilitating adequate data concealment.

Table 11 provides a comparative analysis of various video encryption and decryption durations, indicating that larger video files necessitate increased processing time. Compared with the method studied in study [7]. The proposed system demonstrates efficient encryption performance with balanced security and speed, ensuring scalability across various video sizes.

Table 9. Video quality measurement results

Video	Number of Characters Inserted	Capacity	PSNR	MSE	SSIM	Entropy	NPCR	UACI	Correlation
1	100	2.48 MB	87.5157	0.0001	1.0000	6.9122	0.0114	0.0001	1.0000
2	50	0.64 MB	75.0907	0.0020	1.0000	7.6856	0.2014	0.0024	1.0000
3	23	7.42 MB	87.6557	0.0001	1.0000	7.7856	0.0112	0.0001	1.0000
4	102	23.77 MB	87.4227	0.0001	1.0000	7.6897	0.0118	0.0001	1.0000
5	14	0.21 MB	74.3585	0.0024	1.0000	7.7195	0.2384	0.0028	1.0000
10	2174	23.77 MB	74.4940	0.0023	1.0000	7.7999	0.2310	0.0027	1.0000

Table 10. Comparison of PSNR, MSE, and SSIM between the proposed system and previous studies

Title	Proposed System	Ref. [17]	Ref. [18]
Name	Video 1	-	Road.avi
No. frames	93	464	623
PSNR	87.5157	59.9919	55.1217
MSE	0.0001	-	0.1999
SSIM	1.0000	-	-

Table 11. Compression of encryption and decryption time for the proposed method and an existing approach

Name of Video (Proposed System)	Size of Video (Proposed System)	No. Frames (Proposed System)	Encryption Time (Proposed System)	Decryption Time (Proposed System)	Name of Video [7]	No. Frames [7]	Size of Video [7]	Encryption Time [7]	Decryption Time [7]
Video 1	6.75 MB	93 frames	1.2636 s	1.8428 s	Book	132	2.09 MB	2.74 s	2.19 s
Video 2	1.04 MB	368 frames	0.0505 s	0.1017 s	Exam paper	386	5.81 MB	2.66 s	2.19 s
Video 3	5.10 MB	221 frames	0.3015 s	0.9176 s	Chat	102	704 kB	2.39 s	2.39 s
Video 4	84.6 MB	961 frames	1.2612 s	2.1610 s	Name of video [7]	No. frames [7]	Size of video [7]	Encryption time [7]	Decryption time [7]
Video 5	863 kB	777 frames	0.0275 s	0.0420 s	Book	132	2.09 MB	2.74 s	2.19 s
Video 10	494 MB	568 frames	1.3364 s	2.6990 s	Exam paper	386	5.81 MB	2.66 s	2.19 s

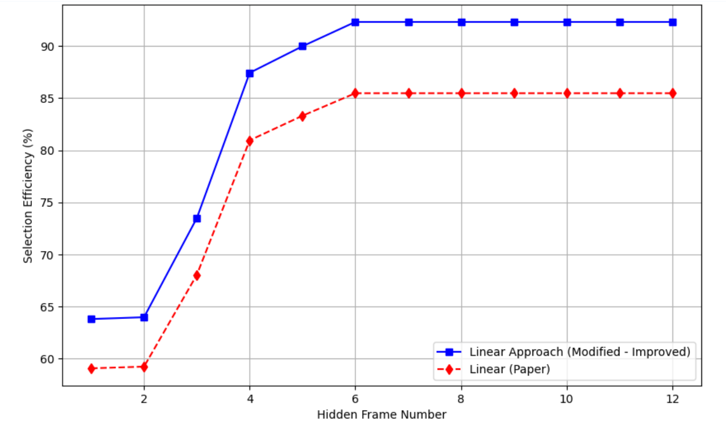

Figure 6. Comparison of linear selection efficiency in video steganography

Table 12. Compression of linear approach efficiency between the proposed system and the previous study

Frame	Proposed System	Ref. [18]
1	63.8170	59.09
2	63.9897	59.25
3	73.5045	68.06
4	87.4365	80.96
5	89.9854	83.32
6	92.3180	85.48
7	92.3180	85.48
8	92.3180	85.48
9	92.3180	85.48
10	92.3180	85.48
11	92.3180	85.48
12	92.3180	85.48

Table 12 compares the proposed method's linear selection efficiency with the approach used in the study [18]. In video steganography, linear selection efficiency is crucial in determining the efficiency of hidden data distribution across video frames. Sequentially selecting pixels ensures a uniform spread of embedded data, enhancing both imperceptibility and robustness. Figure 6 shows a plot of these results, demonstrating the improved selection efficiency of the new method.

5.5 Extracting hidden text from video results

The hidden data were extracted from within the video frames. Table 13 shows the extraction results.

Table 14 compares the capacity, embedding time, and extraction time of the proposed system with the method studied in the study [19]. The results indicate that the embedding time increases with file sizes, as seen when comparing Video 1 (6.75 MB, 40.10 sec) with Video 5 (863 KB, 9.86 sec). Compared with the study [19]. The proposed system demonstrates competitive embedding efficiency with a slight reduction in extraction time, making it suitable for secure and fast steganographic applications.

Table 13. Accuracy of extracted text from stego-frames

1	
	iGQbCbTuymhr9YgMQAV9C13/gn2eFDHJ7gQP1ljm1+yZz1fwd48uanNOsdFSuW5D36btzpRjggNaO0M/FeWullO949gR6UiZWYz+7B/kDDMRRMKcB+Iuo2p1NdCsq+c3ITgF+hr4hNZWKdIl6F1Qjhrm8/qoyEnOSI9vdARxsjAURJaCUhcTTBDWQdv/r5wbcSLdOuEdNSdT5UtrQLd2GkAFIWKirVUPg3lcdhCDJTuYbE2EFbN1+ZoljRMNQG63IvVAIdzizXSZwZUPZEJU9WrKkFO/6qlSWCL1Htm8afODv211iJuuOsymgVMssgVdYLiok5laMTxYGxusVVZob2olDIL9TX/R5bBpO40L1eB4W5uRvSuViM6IB8Mz34oug0ssTSHIVrxKoT4oezRx/KtlU9+lYRpreGHBp26BZw/h2phdDxMFkuqdnETAUHnOSHv6FNZqnlNa0Es3CPMxGzg+cJB2/uWhaCZqcEJlh7gg9C5VWBhO9FtcM1e0G5laIjrAE9gzR9H+Mjcr70BCDD0cxi/L5CMy47M+cpN6DMdOQkDzOXrvdfvs2mFoxX6MGNQn2wO8KlHbdR19XyGE/akuW9aj0Xs+L1PqMVvyY6JEzVMku5NqvAZJz0UHV024CoAZlPcMuNv5W/YjoGK/x24m7J3Vukh/c5nl6+WtC8khX1DIFv3lRHCiSsRZC6e5
	When I am in your presence, my heart is full and I feel stronger, wiser, and more confident. You inspire me to reach deep into my heart and love you with all of the passion I have. I will keep caring, adoring, and loving you forever, during the easy times and the challenges we will face. We are in this together, and you are my partner for life. How did I get so lucky to deserve someone as beautiful as you are, both inside and out? I am grateful every day that you said “Yes” when I asked you to marry me.
2	
	xOqUg4IXGnrUwF1XQJQindh/Zk2hlybza/Th1Vn8gWbHj18zntJ9nQKpOFQGEzaoTdXffiATUp42tTnNhg4faF+oMzyHAPgOvKZjbMtG4E2ZdYPRiwYmfgNH4U0avREHQi261bh0lqnBmr5bEy/jSHPhWHC8tbhrxIj7aDPGhkR7YXmzSehYXvOBP9UC9AzpiBuyV5OIsO7qKaSGcR8c4Ejfe9jQVrx9in44fnd2DmVpGO9TXInfu+R78hUfkrOarctE/TRg8lRVmGGV4AKWjECp2CYb+YzLzinH29hiazLRD7p2p1jTtceci5/0kE46Eb4gh3MEkcW62LEvlYwokQ==
	Even after all of this time together, you still give me a thrill when you kiss me. My heart still skips a beat every time you look at me in a loving way. I am head over heels in love with you, and this is how it will always be.
3	

	BrpDxcMxARWWr4SjgAr21q7+QADjYKjmwHSJRJbe3opKNCU/Y0Oe4rBNfqI6YUvs5RwzZHHHUFpt68PojQud6crt3D8ixPsRfEZd gLk2Zj6MOON/ytkSczXEp4YJB8kr4MUg+WUD4BUbb7hmMk7Ca8psvlQXnEwcBH8TdL/vSQQ=
	The more years go by, the more I learn new things to love about you. You are the most amazing woman to me

Table 14. Comparison of the hiding and extraction times of the proposed method and an existing approach

Name of the Video: Proposed System	Size of Video	Capacity Bit/Size Proposed System	Embedding the Proposed System	Extraction Time Proposed System	Name of Video [19]	Capacity Bit/Size [19]	Embedding Time [19]	Extraction Time/Second [19]
Video 1	6.75 MB	0.0371	40.10 s	0.50 s	Tiger	0.05113	-	50 s
Video 2	1.04 MB	0.9425	7.93 s	0.52 s	Elephant sleeping	0.04732	-	46 s
Video 3	5.10 MB	0.1161	31.08 s	0.51 s	Elephant walking	0.07820	-	40 s
Video 5	863 kB	2.4129	9.86 s	0.48 s	Elephant sitting	0.04723	40 s	

6. CONCLUSION

This paper proposes a novel video steganography system that emphasizes security and efficiency by incorporating AES encryption and a key generation mechanism based on a 9-D chaotic logistic map. The proposed system is characterized by high security, robustness, and imperceptibility levels, as validated by various security and quality assessments. Experimental findings indicate that the method achieves elevated PSNR values, reflecting minimal distortion in stego-frames. At the same time, the results of the entropy and chi-square tests affirm the strong randomness of the encrypted text. Furthermore, optimizing the linear selection approach for pixel embedding led to superior efficiency and security compared to existing techniques. Additionally, NIST randomness tests validated the unpredictability of the generated keys, ensuring protection against cryptanalysis. Comparative analysis with previous studies confirms that the proposed system offers a balance between embedding capacity, security, and computational efficiency. The improved encryption and decryption times demonstrate its suitability for real-world applications. Future work may focus on enhancing embedding capacity while maintaining high imperceptibility and security.

Video processing in the current system follows a batch processing approach, where the video is divided into individual frames. The system does not support real-time video processing at 1080p resolution. Real-time processing is part of the future development plan to enhance system efficiency and adaptability in live applications. Although the system demonstrates efficiency in most experiments, its performance declines when applied to highly compressed or re-encoded videos, which aligns with practical implementation requirements.

REFERENCES

[1] Kunhoth, J., Subramanian, N., Al-Maadeed, S., Bouridane, A. (2023). Video steganography: Recent advances and challenges. Multimedia Tools and Applications, 82(27): 41943-41985. https://doi.org/10.1007/s11042-023-14844-w

[2] Guan, B., Xu, D., Li, Q. (2020). An efficient commutative encryption and data hiding scheme for HEVC video. IEEE Access, 8: 60232-60245. https://doi.org/10.1109/ACCESS.2020.2983330

[3] Kou, L., Huang, Z., Jiang, C., Zhang, F., Ke, W., Wan, J., Liu, H., Li, H., Lu, J. (2022). Data encryption based on 7D complex chaotic system with cubic memristor for smart grid. Frontiers in Energy Research, 10: 980863. https://doi.org/10.3389/fenrg.2022.980863

[4] Albahrani, E.A., Alshekly, T.K., Lafta, S.H. (2022). A review on audio encryption algorithms using chaos maps-based techniques. Journal of Cyber Security and Mobility, 11(1): 53-82. https://doi.org/10.13052/jcsm2245-1439.1113

[5] Vivek, J., Gadgay, B. (2021). Video steganography using chaos encryption algorithm with high efficiency video coding for data hiding. International Journal of Intelligent Engineering and Systems, 14(5): 15-24. https://doi.org/10.22266/ijies2021.1031.02

[6] Salunke, S., Shrivastava, A.K., Hashmi, M.F., Ahuja, B., Bokde, N.D. (2023). Quad key-secured 3D Gauss encryption compression system with Lyapunov exponent validation for digital images. Applied Sciences, 13(3): 1616. https://doi.org/10.3390/app13031616

[7] Fadhil, F.A., Hussien, F.T.A., Khairi, T.W.A., Safiullin, N. (2024). A proposed text encryption inside video using harris corner detection and Salas20 encryption algorithm. Baghdad Science Journal, 21(7): 2485-2499. https://doi.org/10.21123/bsj.2023.9168

[8] Meng, L., Jiang, X., Sun, T., Zhao, Z., Xu, Q. (2023). A robust coverless video steganography based on the similarity of inter-frames. IEEE Transactions on Multimedia, 26: 5996-6011. https://doi.org/10.1109/TMM.2023.3344357

[9] Kale, G., Joshi, A., Shukla, I., Bhosale, A. (2024). A video steganography approach with randomization algorithm using image and audio steganography. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, pp. 1-5. https://doi.org/10.1109/ESCI59607.2024.10497225

[10] Dai, Q., Liu, X. (2024). Improved AES scheme based on chaotic mapping. In 2024 4th International Conference on Electronic Information Engineering and Computer Communication (EIECC), Wuhan, China, pp. 888-892. https://doi.org/10.1109/EIECC64539.2024.10929495

[11] Harsha, K., Gopika, S. (2024). A comprehensive review of image encryption algorithms: Techniques and applications. In 2024 5th International Conference on

Data Intelligence and Cognitive Informatics (ICDICI), Tirunelveli, India, pp. 920-926. https://doi.org/10.1109/ICDICI62993.2024.10810878

[12] Badhan, A., Malhi, S.S. (2025). Enhancing data security and efficiency: A hybrid cryptography approach (AES+ ECC) integrated with steganography and compression algortihm. In 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, pp. 450-456. https://doi.org/10.1109/IDCIOT64235.2025.10914830

[13] Shetty, N.P., Muniyal, B., Priyanshu, A., Kumar, D., Maben, L.M., Agrawal, Y., Natarajan, R., Gunda, S., Gupta, N. (2024). Protecting your online persona: A preferential selective encryption approach for enhanced privacy in tweets, images, memes, and metadata. IEEE Access, 12: 86403-86424. https://doi.org/10.1109/ACCESS.2024.3415663

[14] Verma, V., Kumar, S. (2025). Quantum image encryption algorithm based on 3D-BNM chaotic map. Nonlinear Dynamics, 113(4): 3829-3855. https://doi.org/10.1007/s11071-024-10403-6

[15] Khan, M.S., Ahmad, J., Al-Dubai, A., Pitropakis, N., Driss, M., Buchanan, W.J. (2024). A novel cosine-modulated-polynomial chaotic map to strengthen image encryption algorithms in IoT environments. Procedia Computer Science, 246: 4214-4223. https://doi.org/10.1016/j.procs.2024.09.261

[16] Nguyen, N., Pham-Nguyen, L., Nguyen, M.B., Kaddoum, G. (2020). A low power circuit design for chaos-key based data encryption. IEEE Access, 8: 104432-104444. https://doi.org/10.1109/ACCESS.2020.2998395

[17] Al-Agaili, A.A.H., Ali, H.H., Naser, H.A. (2024). Hide text within a video using data encryption standard (DES) technology. SAR Journal, 7(1): 24-28. https://doi.org/10.18421/sar71-04

[18] Ravichandran, C., Vajravelu, A., Panda, S., Degadwala, S.D. (2024). Data hiding using video steganography. International Journal of Electronic Security and Digital Forensics, 16(1): 112-123. https://doi.org/10.1504/ijesdf.2024.10052934

[19] Khodher, M.A.A.A., Alabaichi, A., Altameemi, A.A. (2022). Steganography encryption secret message in video raster using DNA and chaotic map. Iraqi Journal of Science, 63(12): 5534-5548. https://doi.org/10.24996/ijs.2022.63.12.38