International Journal of Safety and Security Engineering
Vol. 15, No. 3, March, 2025, pp. 521-532
Journal homepage: http://iieta.org/journals/ijsse

A Hybrid Security System for Text Encryption and Steganography in Video Using Multi-Level Chaotic Maps

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

Department of Computer Engineering, University of Technology, Baghdad 10066, Iraq

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

https://doi.org/10.18280/ijsse.150311

Received: 13 February 2025
Revised: 21 March 2025
Accepted: 25 March 2025
Available online: 31 March 2025

Keywords:
Advanced Encryption Standard (AES), chaotic key generation, cryptography, data hiding, Least Significant Bit (LSB), multi-level chaotic maps, secure data transmission, statistical attacks, steganography, text encryption

ABSTRACT

The swift advancement of information and communication technology has made it increasingly difficult to guarantee the security of transmitted data. Traditional encryption techniques, particularly in multimedia applications, frequently fail to defend against sophisticated attackers. By combining multi-level chaotic maps with Least Significant Bit (LSB) steganography and Advanced Encryption Standard (AES) encryption, this study proposes an improved security approach for text transmission. Multiple well-known chaotic maps integrate into the chaotic system to guarantee randomness as well as key unpredictability through the Arnold Cat Map, Ikeda Map, Tent Map, Henon Map, Gingerbread Man Map, Standard Map, and Zaslavsky Map. A hybrid chaotic system dynamically creates the encryption keys, guaranteeing high unpredictability and resistance to brute-force attacks. Next, it incorporates the encrypted text into video frames, making it challenging to find the secret data. The suggested method executes three fundamental steps, which start with chaotic system-based dynamic key genesis, followed by AES encryption enabled by the generated key, and culminating in LSB steganographic text embedding insertion. The suggested method demonstrates its resilience to statistical attacks by passing 13 out of 16 NIST randomness tests and achieving high entropy values above 7.98, along with strong Chi-Square statistics confirming uniformity of encrypted text distribution. Our hybrid approach improves data secrecy and resistance to various cryptographic attacks. The proposed system provides superior encryption capabilities together with better randomness, and withstands statistical attacks while maintaining while preserving the imperceptibility of the video content .Experimental results confirm the efficiency of the suggested technique in safely sending sensitive textual information while preserving the video content's imperceptibility.

1. INTRODUCTION

Video content security has emerged as a critical component of data transmission due to the explosive rise of multimedia applications. Conventional encryption methods are susceptible to unwanted access since they frequently fail to defend against statistical and brute-force attacks. Users have employed many methods to protect data that they consider critical.

One common method is steganography [1], which is a process of hiding data in the bits of cover objects, like a graphic or an audio file. It provides a safe way to communicate privately because the presence of information in the cover item is challenging to detect [2]. Various companies use digital networks for the safe and quick distribution of their patented digital objects to authentic purchasers [3]. Applications using steganography include not only digital activities in everyday life but also text transmission in military, medical, and industrial fields. It is crucial to protect these texts from possible threats. Text encryption is the most effective way to provide text security [4].

An encryption algorithm is an effective tool for maintaining information security. It changes the information into an incomprehensible form [5]. For instance, text encryption applies confusion and diffusion principles, where good ciphering is achieved when the result is similar to that of TV jamming. One public cryptography that is widely used in various applications, such as smart cards, cell phones, automated teller machines, and web servers, is the Advanced Encryption Standard (AES) [6]. Several Assessment Standards, such as information entropy and Chi-Square, must be taken into account while encrypting a text. The method can resist statistical and differential attacks if the values of these criteria match the intended expectancy [7]. Furthermore, to withstand brute-force attacks, a text encryption method needs to have a large key space and a highly sensitive to the beginning conditions. Furthermore, the method needs to be quick for real-time applications [8].

This paper proposes a text encryption algorithm by combining the chaos system and the AES algorithm. First, we build the encryption key chaotic system, and then encrypt the text using the suggested algorithm [9], which incorporates multi-level chaos, AES, and steganography. We include the encryption mechanism in this research and divide the text to be encoded into blocks. Each block is treated separately,

whether for encryption or to include it in video frames, which provides quality and efficiency. With AES encryption algorithms, the information becomes encrypted and unreadable without the correct key, as the characters within each block are encrypted. After dividing the video into frames, we treat these frames as separate containers [10], and the frames are selected using methods such as the Least Significant Bit (LSB) algorithm and the perfect pocket curve [11]. Then, the frames containing the encoded information are collected to extract the encoded text [12].

Multiple encryptions and steganographic tools currently face different shortcomings because they produce weak random keys, allow minimal data capacity and remain susceptible to assault methods, experience different levels of random key weakness as well as restricted data capacity and sensitive attack vulnerability. This research develops a new hybrid system that combines multi-level chaotic maps for key production with Advanced Encryption Standard encryption and optimized LSB-based steganography implemented within video frames to address current limitations. Through a comprehensive method, this system strives to improve data encryption security levels with additional features for enhanced visual stealth and powerful resistance against multiple attacks.

The paper is organized as follows: The second Section reviews the literature. The third Section explains methods and materials. The fourth Section system framework includes key generation system, text encryption-decryption, video segmentation, and steganography. The fifth Section presents the results and testing, and a comparison between the suggested method and other applied ones. Finally, the sixth Section discusses steganographic capacity analysis, and the seventh Section provides the conclusions.

2. RELATED WORK

The rapid advancements in communication technologies and mobile applications have significantly increased the need for protecting transmitted and stored data. Consequently, numerous studies have explored various encryption and steganographic techniques to enhance information security. Much research presents various contributions in this field. Al-Kateeb and Jader [13] proposed a secure encryption technique integrating DNA coding with a hyperchaotic system to encrypt and conceal text. Their method employs the four DNA nucleotides (A, T, G, C) to encode data, allowing multiple representations for the same character or word, thereby enhancing complexity. The experimental results demonstrated that this approach effectively secures textual information, making it highly resistant to brute-force and known-plaintext attacks. The suggested system faces challenges from algorithmic complexity, vulnerability, susceptibility to attacks, weakness in steganography, and potential data loss. It has also been observed that limited data hiding capacity.

Elkamchouchi et al. [14] introduced novel video encryption schemes utilizing chaotic maps. Their approach involves pixel shuffling and substitution, introducing a high degree of randomness and confusion within video frames. The evaluation results indicate that these encryption schemes achieve a strong balance between security and computational efficiency, making them suitable for secure video transmission while ensuring rapid encryption and decryption processes. The developed video encryption exhibits arithmetic overhead due to complex chaotic maps and Feistel structures, and potential vulnerability for information leakage. Performance is limited with large blocks because of the sensitivity to a change in mass, which affects the value of PSNR and correlation. Wu et al. [15] proposed a plaintext-dependent dynamic key chaotic encryption system for images. Their method generates a unique key based on the plaintext image itself, ensuring that each encrypted image possesses a distinct cryptographic key. By leveraging chaotic maps, the system enhances security, making it highly resistant to differential and cryptographic attacks. The experimental findings confirm that this technique provides a robust framework for securing image data The suggested chaotic image encryption method demonstrates limitations in processing efficiency due to the complexity of Lorenz systems, and vulnerability to attacks, Sensitivity to minor changes that affect the generated key This, in turn, affects the scalability of high-resolution images. Albahrani et al. [16] conducted a comprehensive review of audio encryption techniques utilizing chaotic maps. The study analyzed multiple encryption algorithms employing chaotic systems to secure audio transmissions. Their findings indicate that chaotic map-based encryption offers superior security due to large key spaces and high sensitivity to initial conditions. A comparative analysis of various encryption methods further established the effectiveness of chaotic systems in preventing unauthorized access to audio data The complication of chaotic maps, susceptibility to initial parameters affecting key security, limited scalability when handling large audio files, incomplete resilience against hybrid attacks, and difficulties in striking a balance between security and real-time performance make the reviewed chaotic audio encryption methods Computationally burdensome. Majeed et al. [1] presented an extensive review of text steganography methods, classifying them into three main categories: statistical and random generation, format-based approaches, and linguistic techniques. Their study highlighted the challenges of text steganography due to low data redundancy, yet demonstrated that the reviewed methods successfully concealed information while remaining imperceptible. The paper also identified key areas for future research, emphasizing improvements in imperceptibility and robustness lack of redundancy in textual files, susceptibility to format changes, vulnerability to advanced linguistic steganalysis, and performance inefficiency when applied to big datasets or various languages restrict text steganography embedding process capacity. Fadhil et al. [2] added a hybrid text encryption and steganography method leveraging Harris Corner Detection and Salsa20 encryption. Their method includes detecting distinguished key points in video frames for embedding encrypted text, ensuring minimal perceptibility. The Salsa20 encryption algorithm is implemented to ensure the safety of embedded text. Experimental effects found out that the proposed method preserves excessive video quality whilst demonstrating strong safety performance based on metrics which include Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). These findings verify that this approach correctly conceals and protects textual content inside video frames, making it a highly stable approach for statistics transmission Due to a confined number of detectable corners, dangers to video quality, vulnerability to attacks and detection, reliance on key control, and feasible lack of robustness all through video compaction or facts alterations, the advised text encryption approach inside video frames is restrained by using information embedding

potential.

Meng et al. [17] proposed research presents a video steganographic system that stores secret data inside pre-defined public content while preserving the original material. Video sequences are sorted according to inter-frame similarities, while the secret segments get mapped to specific videos using a shared table. The experimental results demonstrate better storage capacity, together with more powerful protection and better security features, by removing the dependency on additional transmitted data.

Kale et al. [18] found that video steganography receives an enhancement through a method that embeds text data into video frames and audio communications. The system achieves higher security through two measures, including random frame selection procedures together with MD5 hashed text processing before hiding. The dual-layer method boosts data confidentiality and enlarges hiding capacity because it uses visual and auditory components within the video framework.

Dai and Liu [19] presented an AES encryption strengthening through the employment of Logistic and Tent chaotic maps for generating round keys. The method obtains enhanced security by using chaos-based sequences instead of conventional key expansion thus both disrupting key relationships and generating separate keys for each encryption session. Experimental findings show that the keys have successful statistical randomness test results while significantly growing the key space, which strengthens AES security against cryptographic threats and results in "one secret per session.

Badhan and Malhi [20] developed a dual-system cryptographic mechanism that unites AES and ECC cryptographic operations with inverted LSB steganography and WebP compression to achieve more powerful data security alongside better efficiency levels. AES performs encryption for the data, but ECC utilizes short key sizes to protect AES encryption keys, respecting efficiency requirements. The encryption procedure inserts the data into images using an inverted LSB method before WebP compression preserves data integrity without increasing storage needs. Experimental tests demonstrate exceptional system performance by achieving results with 68.90 PSNR and 0.0083 MSE, which demonstrates excellent visual quality after embedding and demonstrates the system's ability to provide secure and efficient image-based communication.

Hariharan et al. [21] developed a two-stage encryption model that combines optimized bivariate mathematical functions with genetic algorithms, together with random key generation methods. The transmitted data is symmetrically encrypted with RSA, securing key transmissions to maintain confidentiality at all stages. The mixed security approach provides improved encryption power and defense against forced brute-force encryption break and cryptanalysis as well as interception attacks, while handling problems characteristic of standard cryptographic systems (see Table 1) [21].

Zhu et al. [22] introduced SAEF as an encryption and anonymization framework that protects rPPG datasets through high-quality privacy removal of sensitive face regions. The system adopts a fast cascade key encryption method (CKEM), which encrypts individual frames in 5.54×10^5 seconds, resulting in negligible data correlation below 0.005 APC. The secure anonymization process of SAEF maintains signal accuracy through experimental evaluations, which show R-value and MAE deviations below 0.06 and 0.05, thus demonstrating its effectiveness for rPPG dataset sharing with privacy protection.

Table 1. Comparative analysis of recent cryptography and steganography techniques

No.	Year	Ref.	Journal	Technique Used	Advantages	Disadvantages	Type of Data
1	2020	[13]	TELKOMNIKA	DNA coding + hyperchaotic	High resistance to attacks, high data capacity	Algorithmic complexity, low stego robustness, limited hiding capacity	Text
2	2020	[14]	IET Image Processing	Chaotic maps + Feistel + MPEG-2	High randomness, fast encryption	Sensitive to frame size, PSNR drop, info leakage risk	Video
3	2021	[15]	Entropy	Plaintext-dependent chaotic AES	Dynamic key per image, high resistance	Low scalability, complex Lorenz system	Image
4	2021	[16]	Journal of Cyber Security and Mobility	Chaotic audio encryption	Large key space, high sensitivity	Low scalability, heavy computation	Audio
5	2023	[1]	MDPI	Text steganography (review)	Various methods analyzed	Low redundancy in text, format sensitivity	Text
6	2024	[2]	Baghdad Science Journal	Salsa20 + Harris Corner	High PSNR, robust metrics	Limited keypoints, quality tradeoff	Video
7	2024	[17]	IEEE TMM	Coverless video stego (mapping)	High security, avoids aux data	Fixed database, mapping dependency	Video
8	2024	[18]	IEEE ESCI	Video+audio stego + MD5	Double hiding layers, high security	Audio quality degradation, hash collision risk	Video + Audio
9	2024	[19]	IEEE EIECC	AES + chaotic keys	One secret/session, random keys	Added complexity, no image focus	Image
10	2025	[20]	IEEE IDCIOT	AES + ECC + LSB + WebP	High PSNR, compression supported	WebP artifacts, ECC complexity	Image
11	2025	[21]	IEEE ICSADL	Genetic + RSA + Bivariate	Hybrid encryption, RSA-secured keys	Heavy algorithm design, GA tuning	Text

Previous studies introduced multimedia data protection methods based on chaos-based security and hybrid cryptographic structures with steganographic insertion, but these solutions experience various drawbacks, including insecure key generation methods and detection weaknesses and restricted hiding capacity limitations, and expensive computational demands. The methods struggle between maintaining security and hiding information, or struggle with real-time processing, or produce low efficiency when handling large multimedia files.

The proposed research implements a unified system that produces complex encryption keys through multiple chaotic maps while using AES encryption for data protection and LSB steganographic processes to hide the secured text inside video frame bytes. The amalgamation of encryption algorithms creates a system that combines visual security with statistical defense and brute-force prevention and operational efficiency needed for video communication security.

Proposed Solution: A Suggestion for Resolving Current Issues with Secure Video Data Encryption and Embedding This studies attempts to create a sturdy and powerful system to remedy the bounds and shortcomings determined in earlier studies, which includes limited records embedding capacity, deteriorated video high-quality, and susceptibility to evaluate assaults by generating a high-security key, maintain video fidelity, and assure scalability, the counseled technique combines cutting-edge encryption strategies with ideal facts concealing techniques. Through the use of a hybrid device including multi-level chaotic maps and encryption algorithms (AES) and improved steganographic strategies, this work targets to provide a complete answer for secure multimedia transmission in several packages.

The section details the methods alongside algorithms implemented in the proposed system following the background research and detection of insecure text embedding shortcomings.

3. METHOD AND MATERIAL

This part outlines the methodologies, techniques, and algorithms utilized in creating the suggested system.

3.1 Steganography

Steganography, derived from the Greek phrase steganos, which means "hidden" or "covered," is the practice of concealing statistics within a medium in one of these manners that most effective the meant sender and recipient are privy to its presence. This approach has been in use for thousands of years, relationship lower back to historic Greece. One historic instance concerned shaving the heads of slaves, inscribing secret messages on their scalps, and permitting their hair to develop returned earlier before delivering them to the intended recipient. The message remained hidden until the hair was shaved again.

Modern steganography does not necessarily require complex implementations. A simple example is altering text color in a document to make it invisible against the background. Another example involves writing with invisible ink that can only be revealed under ultraviolet light. In the digital age, steganography can be applied to various media formats, including images, audio, and video files. One of the most common steganographic techniques is the LSB method, which embeds hidden data into the least significant bits of pixel values.

The LSB technique first converts the secret message into a binary format, making each bit accessible for embedding. For instance, in a 32-bit ARGB (Alpha, Red, Green, Blue) pixel representation, one bit of the message is embedded in the least significant bit of the blue channel. The alteration in pixel values is so minor that it is virtually undetectable to the human eye. Despite its effectiveness, LSB steganography has limitations, primarily in terms of data capacity. The amount of information that can be embedded depends on the size of the cover image or video. Larger media files allow for greater data insertion, following a linear correlation. However, optimized LSB implementations can enhance capacity by embedding multiple bits per byte, effectively doubling the amount of hidden data [23].

3.1.1 Video steganography

Video steganography involves embedding secret information within video sequences, utilizing their high capacity and complex structure, making them ideal as cover media compared to images, text, or audio. Video segmentation, which divides a video into distinct parts (such as frames or segments based on time or events), is crucial for efficient and secure data embedding. By converting the video into multiple frames, secret data can be embedded either in the spatial domain—directly into pixel values—or the frequency domain, using techniques like Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT). Segmentation ensures that concealed data remains secure and imperceptible during transmission or compression, safeguarding it from potential attacks or frame drops [12].

3.2 Cryptography

Cryptography secures messages, while cryptanalysis breaks the ciphertext to reveal its content. A cryptosystem encrypts and decrypts data using an algorithm with cipher keys. Cryptology covers both cryptography and cryptanalysis. Cryptosystems are divided into public key methods, which use two keys, and secret key methods, which use the same key for both encryption and decryption [24].

3.2.1 Standard AES technique

The Advanced Encryption Standard (AES) is a symmetric-key encryption algorithm that securely encrypts plaintext and decrypts ciphertext. It was developed by Joan Daemen and Vincent Rijmen of Katholieke University in Leuven and was officially adopted by the National Institute of Standards and Technology (NIST) in October 2000. It is noted for its security, efficiency, performance, implementation flexibility, and robustness. Joan Daemen of Proton World International and Vincent Rijmen of Katholieke University at Leuven developed the Rijndael algorithm. AES is an iterative algorithm, with each iteration referred to as a "round." The number of rounds is determined by the key length: 10 rounds for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys. The data block size is 128 bits, organized into 16 bytes that form a 4x4 array called the "state," which is used to perform all AES operations. In the first round, the round key is added by XORing the cipher key with the input plaintext. There are 9, 11, or 13 main rounds, each comprising four stages, while the final round includes three stages. AES decryption follows the same sequence but in reverse order, employing inverse transformations such as InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey. This process ensures secure encryption and decryption while maintaining resistance against common cryptographic attacks [25].

3.3 Chaos system

Chaos theory is a branch of mathematics that explores highly complex and dynamic systems. In these systems, seemingly insignificant changes to the input can lead to

substantial variations in the output. The key characteristics of chaotic systems include:

- Sensitivity to Initial Conditions: Small variations in initial values lead to entirely different sequences when repeatedly computed within a chaotic map.
- Sensitivity to Parameters: Minor adjustments to input parameters result in drastically different output sequences, making chaotic systems highly unpredictable.
- Randomness: Chaos sequences generated using chaotic maps exhibit pseudo-random properties, making them difficult to predict or analyze due to their complex structures. Without knowledge of the correct control parameters and initial values, an unauthorized entity cannot reconstruct the chaotic sequence.

Consequently, chaotic systems enhance the security of encryption mechanisms, particularly in image encryption applications (see Figure 1) [26].

In this study, several chaotic maps are utilized, including the Arnold Cat Map, Ikeda Map, Gingerbread Man Map, Standard Map, Henon Map, Zaslavsky Map, and Tent Map.

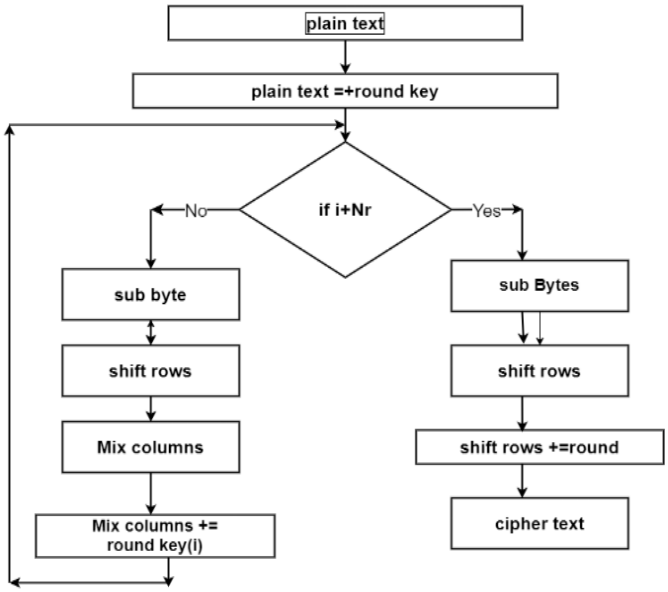


Figure 1. Block diagram of AES [26]

3.4 NIST statistical test suite

Random and pseudo-random number generation plays a critical role in cryptographic applications, particularly in generating secure cryptographic keys. Many cryptographic protocols require random or pseudo-random inputs at different stages to ensure security and unpredictability.

The National Institute of Standards and Technology (NIST) Statistical Test Suite is designed to evaluate the randomness of binary sequences used in cryptographic systems. These procedures are instrumental in detecting deviations from true randomness, which may arise due to deficiencies in generator design or inherent anomalies in the tested binary sequences. However, it is vital to word that a few deviations from randomness are predicted in sequences generated by using particular algorithms, and its miles the duty of the tester to appropriately interpret the test results. There are one kinds of generators used to supply random sequences: random number mills (RNGs) and pseudorandom number generators (PRNGs) [27].

3.5 Text encryption

Text encryption is an essential factor of current cryptography, in which readable plaintext is converted into unreadable ciphertext using algorithms such as symmetric-key cryptography. This system includes sharing a mystery key between the sender and receiver to encrypt and decrypt the message. The plaintext is encoded, for instance, by using ASCII values, and then converted via operations like transferring and XORing with the name of the key to generate the ciphertext. This ensures that handiest legal users with an appropriate key can opposite the process to access the authentic text, making it essential for securing information transmission and storage [28].

The following section describes the proposed hybrid system architecture, which combines key generation with AES encryption plus video steganography techniques.

4. THE FRAMEWORK SYSTEM

This section offers the overall framework of the proposed machine, a hybrid integration of several algorithms, along with steganography, AES, and chaotic systems. These strategies paintings together to enhance protection and ensure resilience in opposition to potential attacks by leveraging proven cryptographic concepts and robust methodologies.

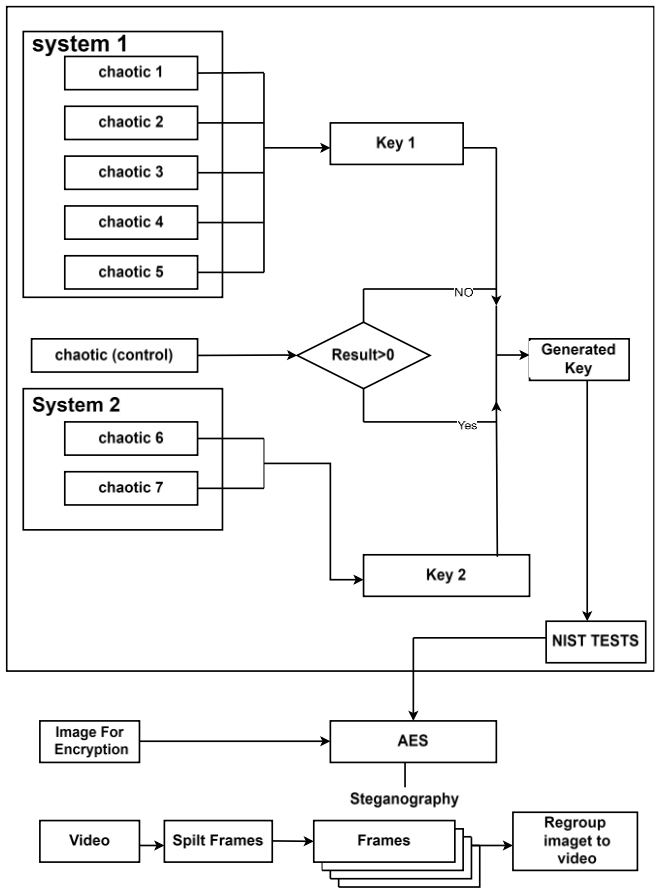


Figure 2. Hybrid framework for the proposed system

The typical structure of the hybrid system is illustrated in Figure 2 and consists of four primary components:

- Key Generation Mechanism: Responsible for producing secure cryptographic keys.

- Text Encoding and Decoding: Converts plaintext into a format suitable for encryption and decryption.
- Video Segmentation: Divides the video into frames for efficient data embedding.
- Steganography: Conceals encrypted text within video frames to enhance security.
- Text Extraction from Video: Recovers the hidden text from the video for decryption and retrieval.

Each of these components comprises multiple subprocesses that collectively contribute to the robustness and security of the proposed system.

4.1 Key creation mechanism

In this section, the chaotic system is employed to generate encryption keys, which are subsequently used to secure text using the AES encryption algorithm. The chaotic system is structured into three primary subsystems, each contributing to the key generation process.

4.1.1 Subsystem 1

As illustrated in Figure 3, this subsystem comprises five distinct chaotic equations, which play a crucial role in ensuring the unpredictability and security of the generated encryption keys.

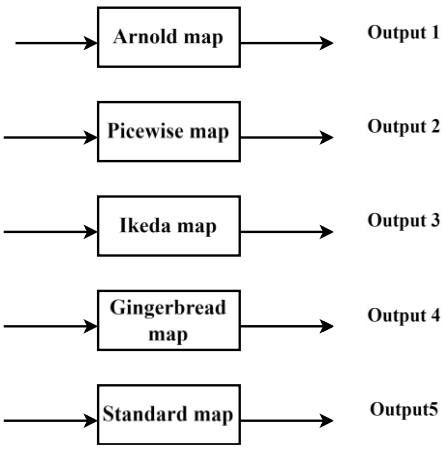


Figure 3. Subsystem 1

The outputs generated by Subsystem 1 consist of fractional values within the following defined ranges:

- Output 1: A fractional value constrained within the range $0 < x, y < 1$.
- Output 2: A fractional value ranging between $0 \leq x \leq 1$.
- Output 3: Fractional values within the range $-1 < x, y < 1$.
- Output 4: Fractional values bounded by $-10 < x, y < 10$.
- Output 5: A fractional value within the range $0 < p < 7$ and $1 < \theta < 6$.

When converting the output of System 1 into a binary format, the following condition is applied:

check_value (value, comparison):
global ones, zeros, bit_key
if value >= comparison:
bit_key+="1"
ones+=l
else:
bit_key+="o"
zeros+=l

where:

- Value: The input value obtained from the fuzzy equation.
- Comparison: A reference value used to determine whether the given value is greater or smaller.

Each conversion step yields 5 bytes.

4.1.2 Subsystem 2

Figure 4 illustrates the two chaotic equations that make up this section. As depicted in Figure 4, Subsystem 2 comprises two chaotic equations that generate the following outputs:

- Output 6: Fractional values constrained within $-1 < x, y < 1$.
- Output 7: Fractional values within the range $0 < x < 1$ and $-21 < y < 22$.

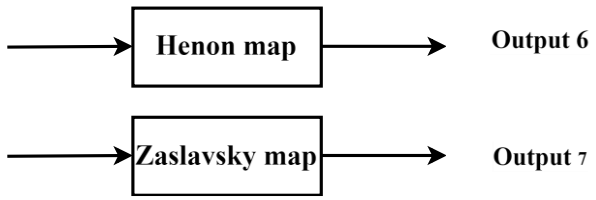


Figure 4. Subsystem 2

When converting System 1's output into binary format, the following conditions are applied:

check_value (value, comparison):
global ones, zeros, bit_key
if value >= comparison:
bit_key+="1"
ones+=l
else:
bit_key+="0"
zeros+=l

where,

- Value: The input value derived from the chaotic equation.
- Comparison: A reference value used to evaluate the relative magnitude of the given value.

Each conversion step in this subsystem produces 2 bytes.

4.1.3 Subsystem 3

This subsystem consists of a single chaotic equation, as illustrated in Figure 5.

Figure 5. Subsystem 3

This component serves as a control mechanism between Subsystem 1 and Subsystem 2. If the generated output is greater than or equal to 0.5, the encryption key is obtained from Subsystem 1. Conversely, if the output is less than 0.5, the key is selected from Subsystem 2. By manipulating this control mechanism, a vast set of binary keys is generated, ensuring a balanced distribution of zeros and ones. Once the keys are generated and balanced, they undergo a selection process using the NIST statistical test suite, where 13 out of 16 tests are successfully passed. This ensures randomness and enhances the robustness of the generated keys. The final encryption keys are then segmented into 256-bit subkeys, preparing them for use in AES encryption.

4.2 Text encoding and decoding

After generating the 256-bit (32-byte) key and using it within the AES encryption method, the ciphertext is transformed from base sixty-four to binary. The information is then cut up into two segments: the primary section carries the initialization vector (IV) with a hard and fast length of 16 bytes, and the second section incorporates the encrypted information. The preliminary vector from the encrypted facts is used to create an AES cipher object, that is then decoded the use of AES decryption. The decrypted text is then lower back after the padding has been removed.

4.3 Video dividing

At this stage, the entire video is processed and divided into frames, which can be subsequently stored in a chosen listing known as output folder.

If this folder does not already exist, it's miles created, and any formerly saved documents are removed to prevent conflicts. The video is processed to decide the entire range of frames, and every frame is extracted and stored as a PNG picture in a sequentially named layout, including "frame-00001.png." Once all frames had been stored, the video file was closed.

4.4 Steganography

The statistics-byte length header, that is 4 bytes long, specifies the period of the concealed records and is study in conjunction with the hidden textual content. Prior to embedding, the specified video frames are taken care of and prepared inside the frames-folder before being copied to the output-folder.

To disguise the data, the LSB technique is applied to modify the red channel of every pixel in the selected frames. The hidden records are shipped across more than one frame and divided into bytes to ensure secure embedding. Once the information has been successfully embedded, the changed frames containing the masked facts are stored.

The length of the first frame is determined by adding the first 4 bytes of the concealed data.

This step is critical for two motives: first to perceive the particular portion of information to be embedded and second, ensures accurate retrieval by figuring out while to forestall analyzing frames for the duration of the extraction process.

4.5 Extracting hidden text from video

In this section, the concealed text is retrieved following the procedure outlined

(Section No.). The video containing the hidden data is selected, opened, and processed frame by frame to extract the embedded information using the following steps:

- The red channel of each pixel is analyzed, and the LSB is extracted and accumulated.
- The extracted bits are used to determine the length of the hidden data (4 bytes), which specifies the number of bytes to be recovered. This process continues across all video frames.
- To ensure the successful extraction of all hidden data, the total number of extracted bits is compared with the length obtained from the first frame.
- The extracted data is then reconstructed into an image file and saved in the extracted_file folder with the filename extracted_image.png.

The following section, performance evaluation of the proposed system, incorporates three experimental tests that measure key randomness alongside encryption quality and embedding efficiency.

5. RESULTS AND TESTING

This section displays results from the proposed MCC/AES/Stego system through three main outcome sections for key generation randomness and video frame encryption assessment and steganographic capacity.

5.1 Key generation result

The key generation system uses chaotic equations to create fractional results that go through binary conversion by a control-based system. The NIST Statistical Test Suite was used to examine the random nature and strength capability of the produced secret key. Evidence from Figures 6-8 demonstrates the key's resistance to brute-force attacks and statistical attacks since it passed 13 out of 16 statistical tests.

Figures 6-8 present the result of the NIST Statistical Test Suite testing applied to the encryption key output. The key’s suitability for secure encryption becomes evident through its successful completion of 13 out of 16 NIST Statistical Test Suite tests.

The cryptographic key proved its strength against attacks through the successful completion of 13 out of 16 statistical checks.

5.2 Examination of original and encrypted text in video frames

Table 2 analyzes entropy and Chi-Square values of encrypted text within video frames. It additionally affords entropy values to assess the level of randomness within the original textual content before and after encryption, supporting to assessment of the effect of encryption on facts distribution. Additionally, the discern includes the effects of the Chi-Square statistic and Chi-Square p-value tests for the encrypted textual content, which analyze the distribution of opportunity values.

These results suggest how properly the encrypted textual content aligns with the anticipated distribution, supplying insights into the performance and protection of the encryption method.

The encrypted text entropy reaches 7.98 in various tests which reflects high-level randomness. Multiple statistical tests using Chi-square p-values above 0.95 show the uniform distribution of ciphertext which reduces the possibility of detection.

All studied test cases reveal that the proposed the method delivers higher entropy than the referenced method for both randomness and security measures.

The encrypted text demonstrates high randomness when the calculated entropy exceeds 7.98. The Chi-Square analysis verifies that the encrypted information displays uniform distribution, thus minimizing potential statistical detect.

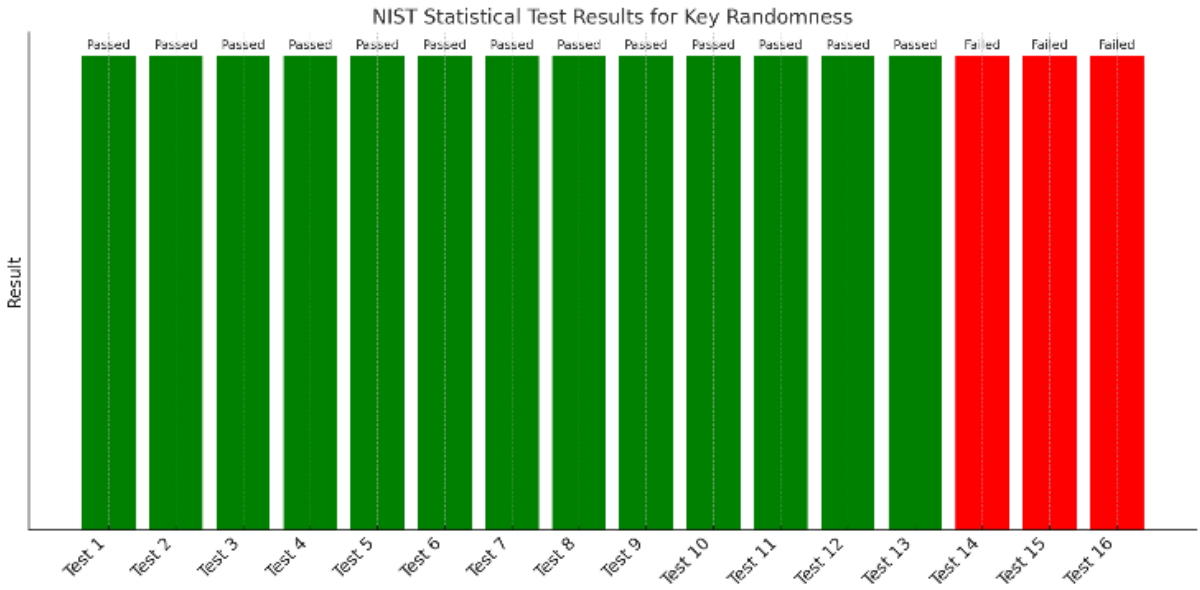
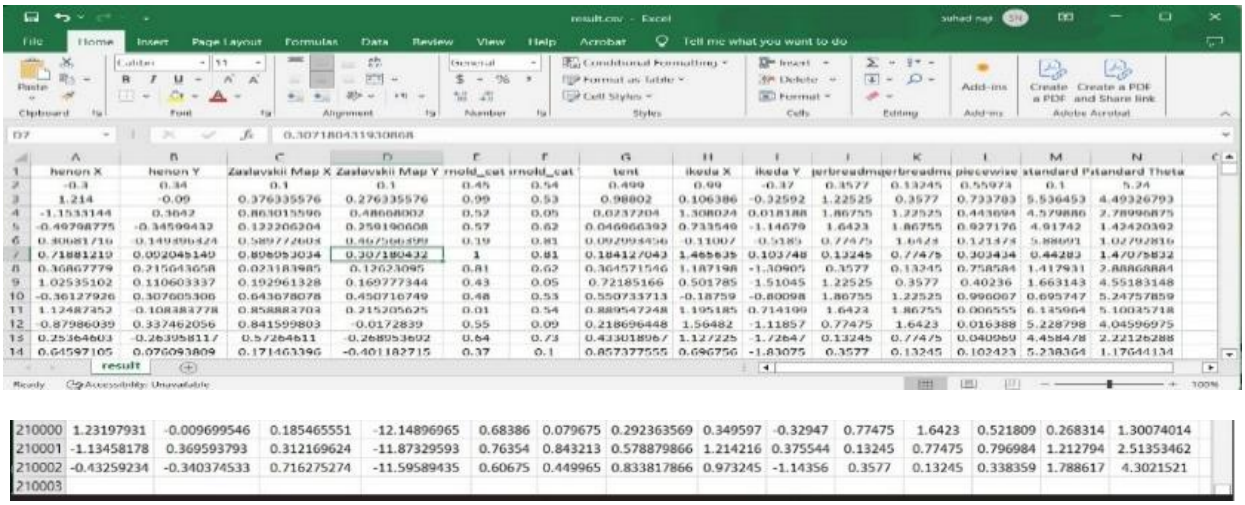


Figure 6. NIST statistical test results for the proposed chaotic key generation system



210000	1.23197931	-0.009699546	0.185465551	-12.14896965	0.68386	0.079675	0.292363569	0.349597	-0.32947	0.77475	1.6423	0.521809	0.268314	1.30074014
210001	-1.13458178	0.369593793	0.312169624	-11.87329593	0.76354	0.843213	0.578879866	1.214216	0.375544	0.13245	0.77475	0.796984	1.212794	2.51353462
210002	-0.43259234	-0.340374533	0.716275274	-11.59589435	0.60675	0.449965	0.833817866	0.973245	-1.14356	0.3577	0.13245	0.338359	1.788617	4.3021521
210003														

Figure 7. Sample fractional outputs from chaotic equations used for key generation

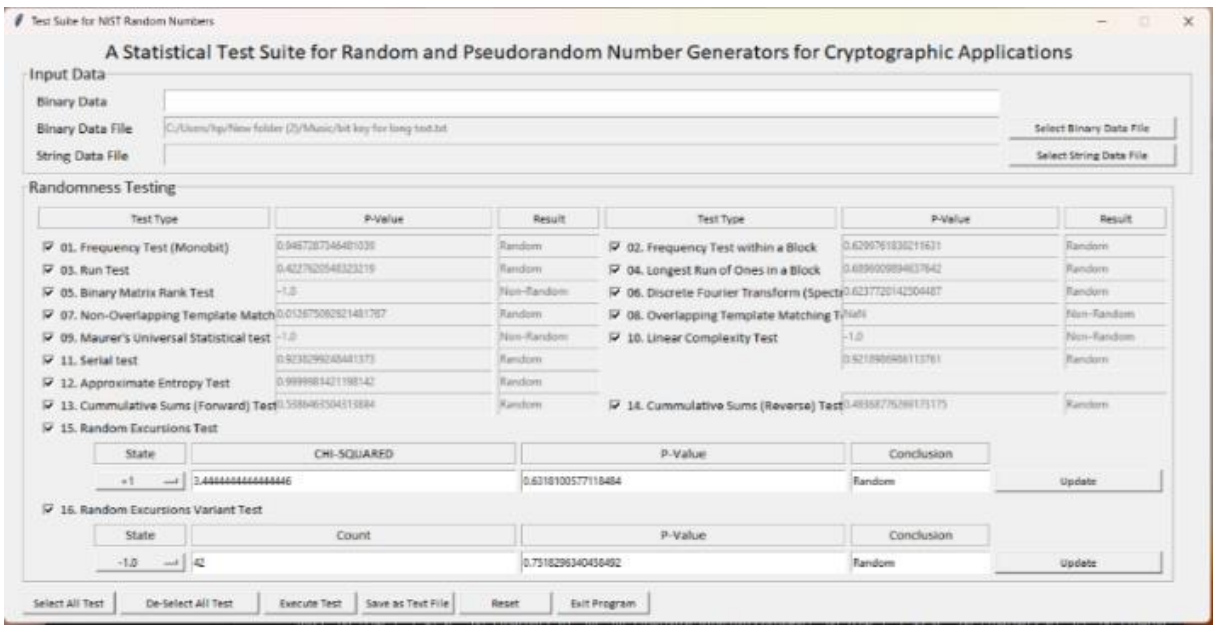
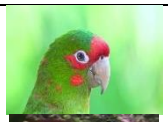
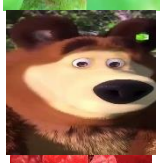
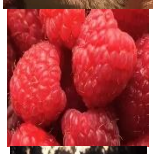
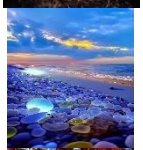


Figure 8. NIST test results confirm the quality of the generated keys

Table 2. Entropy and Chi-Square values for original and encrypted text within video frames

No.	Frames of videos	No. of Frames	Entropy for Ciphertext	Chi-Square Statistic	Chi-Squared p-Value
1		22078	7.9108	211.2000	0.978985
2		240	7.7467	265.6000	0.311200
3		35037	6.8281	230.4000	0.863609
4		610	7.9749	216.7273	0.960619
5		390	7.7656	246.4000	0.638919
6		1798	6.8996	234.1818	0.820813

Tables 3 and 4 demonstrate that the proposed system maintains outstanding video quality with both PSNR scores exceeding 76 dB and SSIM values maintaining 1.0000, indicating impossible distortion for human perception.

The proposed system reaches better PSNR values along with lower MSE measurements, which reveal stronger data hiding efficiency and improved imperceptibility (see Table 5).

Table 3. Comparison of entropy with existing methods

Text	Proposed Method	[2]
1	7.9108	7.2571
2	7.7467	7.3523
3	6.8281	6.8072

Table 4. Video quality measurement result

No. of Video	Number of Characters Inserted	MSE	PSNR	NPCR	UACI	SSIM	Correlation
1	117	0.0012	77.2020	0.1238	0.0015	1.0000	1.0000
2	109	0.0013	77.0742	0.1275	0.0015	1.0000	1.0000
3	113	0.0012	77.3283	0.1203	0.0014	1.0000	1.0000
4	109	0.0014	76.6887	0.1394	0.0016	1.0000	1.0000
5	106	0.0013	76.9894	0.1363	0.0015	1.0000	1.0000
6	112	0.0014	76.7866	0.1363	0.0016	1.0000	1.0000

Table 5. Comparison of PSNR, MSE, and SSIM between the proposed system and the previous studies

Title	Proposed System	[29]	[30]	[31]
Name	Video 1	-	-	Road.avi
No. frames	117	25	464	623
PSNR	77.2020	75.8898	59.9919	55.1217
MSE	0.0012	0.001675	-	0.1999
SSIM	1.0000	0.999997	-	-

6. STEGANOGRAPHIC CAPACITY ANALYSIS

This section examines the relationship between the size of encrypted text and video file size. The steganographic capacity comparison results appear in Table 1 through the analysis of encrypted text dimensions against video file dimensions. The embedded information occupies only tiny portions of the full video file which produces capacity rates between 0.00033% and 0.00436%. The embedded text shows minimal impact on video quality because it cannot be detected by the human eye.

Table 6 shows the steganographic capacity for different videos used in the experiment. The values demonstrate the efficiency of data concealment, as all videos exhibit a low-capacity percentage, indicating that the encrypted text size is

small relative to the video size. As a result, the impact on video quality is minimal. A lower capacity percentage corresponds to higher hiding efficiency, preserving video quality and making the hidden data less detectable.

Figure 9 depicts the steganographic capacity percentage rates from the data cases given in Table 7. Results demonstrate consistently low embedding ratios, which proves both high video confidentiality and efficient usage of video frames during secure data concealment.

The next section evaluates the research outcome about existing scholarly work while suggesting improvements for forthcoming studies.

Table 6. Steganographic capacity for encryption text

Plain Text	Encrypted Text Size (Bytes)	Video Size (Bytes)	Capacity (%)
Hide text inside a video with AES technology	48	1101727	0.00436
The project utilizes the AES algorithm to securely and efficiently hide data within video frames	96	24229803	0.0004
The research methodology integrates chaotic encryption to ensure the confidentiality and security of hidden data	112	10992073	0.00102
The video is divided into frames, and the encrypted text is embedded using the LSB technique	96	29067153	0.00033
The project aims to enhance the security of hidden data without compromising video quality	96	6099430	0.00157

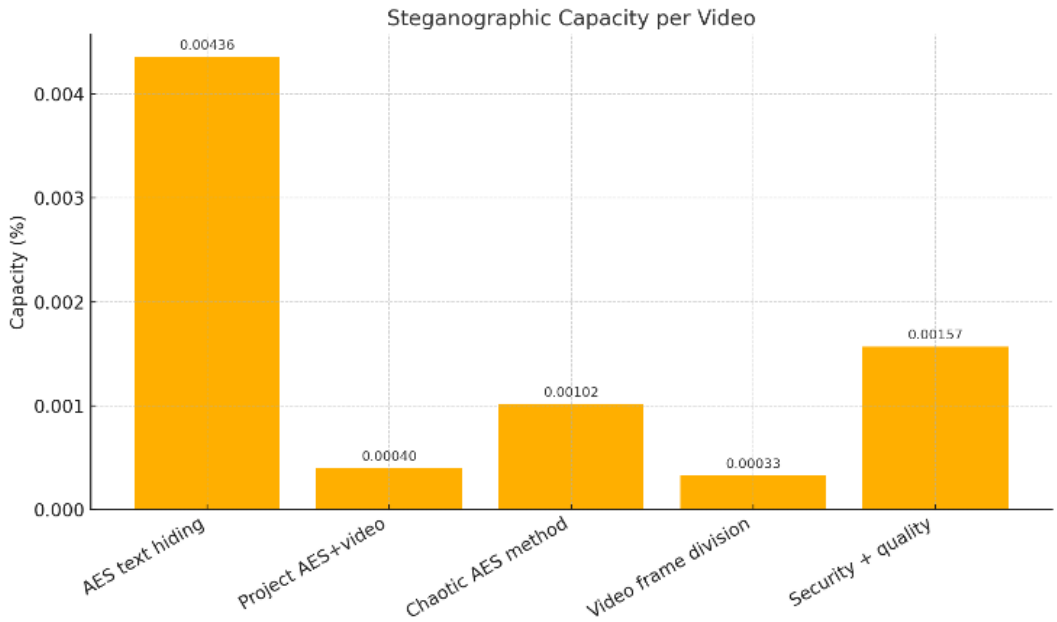
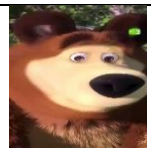


Figure 9. Bar chart showing steganographic capacity across different video cases

Table 7. Extracted text from stego-frames

1	 The confidential document was encrypted using a multi-level chaotic system and securely transmitted through a steganographic video channel. M/DieNVzRPQS778wb96lYue8vZo+H6sYY0AgruIqQB4ut261achnCKgyjMXmy1YksK5JjKWJIirUhqWPybfoKNb9h+Dm2LztfLt9gJsTnUzjMlzyYC1GVBrdpEsAprAgC4z4p3rRo3c9UzuTHfb3f15OhYIrVAOxFQ7pw/SY6Hgz5yAqEdlqp/17eV7wLb7ifi8GrWmKF3Ape6mW7Z760A==
2	 To protect sensitive information from unauthorized access, a combination of AES and multi-level chaotic maps was implemented during encryption. 6ogB181k3shE8JEuL0THLn+qGWHMSh9J7OF+xdZe/NahxFVCe2U0/ChUzGjQoWWdl9+gY9iowK+TptOY5qAk0GaiqkRZ3VR7ZVvqRDu3Edc6UMMtyFz33wGjM1M5oYXYRVXPyiWy9Ms7ZIdtlZo16BfVi7nskZ8nuQj+c2dUyTmA8iu5rga3/gG3TyYsoI5BwMJwEzwf1q30EhthCKyGtQ==

7. DISCUSSION AND FUTURE WORK

The developed system achieved major advancements in encryption security and steganographic functionality. Both statistical NIST testing results show 13 tests passed, while entropy measurements exceeding 7.98 confirm the unpredictability of the chaotic key creation system. The encryption process generates data with such high randomness that attackers fail to detect or recover meaningful information embedded within.

The newly proposed model implements a better modular structure and robustness than previous low-dimensional chaotic models, which closely connect encryption to embedding procedures. The system maintains highly imperceptible video quality through low embedding capacity ratios that keep original content intact.

The system requires expansion to accommodate real-time video encryption functions alongside the support for multimedia elements, including audio and image content. The scalability and transmission efficiency across limited networks can be boosted through adaptation methods that integrate compression standards like H.264 or WebP.

The research has shown that the combined security system presented an effective and practical solution for protection needs.

8. CONCLUSION

The presented research established a dual-layer security system which blends multi-level chaotic maps with AES encryption, together with LSB-based steganography approaches to embed texts securely in video frame data. The proposed system implements a chaotic key generator that strengthens both randomness and security based on NIST test suite and statistical entropy evaluation findings.

Experimental investigation verified that the security system maintains high video quality standards alongside successful hiding of confidential details. The method delivers an effective security system for multimedia communication through its ability to strike a perfect balance between visual integrity and security reliability and processing speed.

REFERENCES

[1] Majeed, M.A., Sulaiman, R., Shukur, Z., Hasan, M.K. (2021). A review on text steganography techniques. Mathematics, 9(21): 2829. https://doi.org/10.3390/math9212829

[2] 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

[3] Mangi, H.T., Ali, S.A., Jawad, M.J. (2023). Encrypting of text based on chaotic map. Journal of University of Babylon for Pure and Applied Sciences, 25-39.

[4] Kaur, M., Kaur, A. (2014). Improved security mechanism of text in video using steganographic technique. International Journal of Advance Research in Computer Science and Management Studies, 2(10): 44-51.

[5] Shakhovska, N. (2017). Advances in Intelligent Systems and Computing. Springer International Pu.

[6] Wadi, S.M., Zainal, N. (2013). Rapid encryption method based on AES algorithm for grey scale HD image encryption. Procedia Technology, 11: 51-56. https://doi.org/10.1016/j.protcy.2013.12.161

[7] Almajmaie, L.K.A., Raheem, A.R., Mahmood, W.A., Albawi, S. (2022). MRI image segmentation using machine learning networks and level set approaches. International Journal of Electrical and Computer Engineering, 12(1): 793-801. https://doi.org/10.11591/ijece.v12i1.pp793-801

[8] Waleed, J., Almajmaie, L.K., Mazher, A.N., Albawi, S. (2023). A fast and accurate optimized iris recognition scheme based on a modified GSO algorithm. In 2023 3rd International Scientific Conference of Engineering Sciences (ISCES), Diyala, Iraq, pp. 1-6. https://doi.org/10.1109/ISCES58193.2023.10311496

[9] Arab, A., Rostami, M.J., Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75: 6663-6682. https://doi.org/10.1007/s11227-019-02878-7

[10] Dua, M., Makhija, D., Manasa, P.Y.L., Mishra, P. (2022). 3D chaotic map-cosine transformation based approach to video encryption and decryption. Open Computer Science, 12(1): 37-56. https://doi.org/10.1515/comp-2020-0225

[11] Abbood, Z.T., Al-Turfi, M.N., Almajmaie, L.K.A. (2023). An abbreviated review of deep learning-based image classification models. Indonesian Journal of Electrical Engineering and Computer Science, 30(1): 491-500. https://doi.org/10.11591/ijeecs.v30.i1.pp491-500

[12] 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

[13] Al-Khateeb, Z.N., Jader, M.F. (2020). Encryption and hiding text using DNA coding and hyperchaotic system. Indonesian Journal of Electrical Engineering and Computer Science, 19(2): 766-774. https://doi.org/10.11591/ijeecs.v19.i2.pp766-77

[14] Elkamchouchi, H., Salama, W.M., Abouelseoud, Y. (2020). New video encryption schemes based on chaotic maps. IET Image Processing, 14(2): 397-406. https://doi.org/10.1049/iet-ipr.2018.5250

[15] Wu, Z., Pan, P., Sun, C., Zhao, B. (2021). Plaintext-related dynamic key chaotic image encryption algorithm. Entropy, 23(9): 1159. https://doi.org/10.3390/e23091159

[16] 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, 53-82. https://doi.org/10.13052/jcsm2245-1439.1113

[17] 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

[18] 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
[19] 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
[20] 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
[21] Hariharan, N.R., Ritheshwar, R.S., Suseendran, R., Meena, R., Kalaiselvi, T. (2025). Genetic algorithm powered bivariate function encryption for robust data security. In 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, pp. 209-214. https://doi.org/10.1109/ICSADL65848.2025.10933102
[22] Zhu, F., Su, H., Ding, J., Niu, Q., Zhao, Q., Shuai, J. (2025). SAEF: Secure anonymization and encryption framework for open-access remote photoplethysmography datasets. IEEE Journal of Biomedical and Health Informatics. https://doi.org/10.1109/JBHI.2025.3552455
[23] Wijaya, K., Lansky, B., Dewi, C.A., Nabiilah, G.Z. (2023). Time-based steganography image with dynamic encryption key generation. Procedia Computer Science, 227: 233-242. https://doi.org/10.1016/j.procs.2023.10.521
[24] Alhassan, S. (2019). Design of perceptual video encryption algorithms for content providers. Doctoral dissertation, Department of Mathematics, Faculty of Mathematical Sciences, University for Development Studies.
[25] Alsaffar, Q.S., Mohaisen, H.N., Almashhdini, F.N. (2021). An encryption based on DNA and AES algorithms for hiding a compressed text in colored image. IOP Conference Series: Materials Science and Engineering, 1058(1): 012048. https://doi.org/10.1088/1757-899x/1058/1/012048
[26] Arab, A., Rostami, M.J., Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75: 6663-6682. https://doi.org/10.1007/s11227-019-02878-7
[27] Elkhateeb, A. (2021). AES encryption and 3D image steganography. Bachelor Thesis. Information Engineering and Technology Faculty, The German University in Cairo. https://doi.org/10.13140/RG.2.2.23931.64800
[28] Sattar, K.A., Haider, T., Hayat, U., Bustamante, M.D. (2023). An efficient and secure cryptographic algorithm using elliptic curves and max-plus algebra-based wavelet transform. Applied Sciences, 13(14): 8385. https://doi.org/10.3390/app13148385
[29] Al-Kateeb, Z.N., Jader, M. (2024). Multi level of encryption and steganography depending on Rabinovich Hyperchaotic System & DNA. Multimedia Tools and Applications, 84: 1211-1237. https://doi.org/10.1007/s11042-024-19057-3
[30] 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
[31] Deshmukh, P.R., Rahangdale, B. (2014). Data hiding using video steganography. International Journal of Engineering Research & Technology, 3(4): 856-860. https://doi.org/10.1504/ijesdf.2024.10052934