

Paper Type: Original Article

An Enhanced Hybrid Video Encryption Scheme Using Sine-Transformed 3D ILM and AES-GCM

Worud Mahdi Saleh ^{1,*} 

¹ General Directorate of Diyala Education, Ministry of Education, Diyala, 32001, Iraq; worud.m.saleh@alsalam.edu.iq.

Received: 31 Mar 2026

Revised: 01 Jun 2026

Accepted: 06 Sep 2026

Published: 23 Sep 2026

Abstract

Owing to the growing deployment of high-quality broadcast content over next-generation networks, one of the central challenges involves locating video dossiers and ensuring their encryption while simultaneously asserting that the solution maintains deal-with-speed performance under certain operating conditions. Traditional video encryption algorithms are likely to face a compromise, because their encryption protection and the resulting depiction within throughput-constrained agreements tend to be jointly determined by conflicting requirements. To address this limitation, a state-of-the-art program encryption approach is proposed here, and it is constructed as a novel composite method. The framework integrates a creative Sine-Transformed 3D Improved Logistic Map (ST-3D-ILM) with Advanced Encryption Standard in Galois/Counter Mode (AES-GCM). The resulting scheme avoids periodic non-lawless fenestella's and instead generates an unlimited rule of chaos as well as perfectly uniform pseudo-random sequences, which are then utilized for both the reformation of secret keys and the initialization of each frame. Concurrently, AES-GCM enables rapid, parallel pixel processing and Galois field multiplication, guided by the use of a 128-slice authentication tag, thereby providing confidentiality, integrity, and frame-level authentication. Experimental simulation outcomes based on standard 720p television reference streams indicate that the proposed encryption method delivers the strongest attainable protection and reaches an optimal entropy value of 7.9997, along with excellent anti-differential-attack characteristics, quantified by the NPCR and UACI measures, which are also as high as 99.61% and 45.33%, respectively. In addition, the processing latency of the method remains dormant at 29 milliseconds per frame (exceeding 35 FPS), which permits its application in extreme-HD scenarios, including combined use across multiple media broadcast streams and safety surveillance applications.

Keywords: Video Encryption, Chaotic Cryptography, AES-GCM, 3D Improved Logistic Map, Authenticated Encryption, Integrity Verification.

1 | Introduction

The use of multimedia communication has undergone a profound transformation over the most recent period, particularly during the last ten years, owing to the emergence of high-speed 5G/6G Wi-Fi networks, cloud computing, and the Internet of Things (IoT). In this lifestyle context, mathematical broadcast concepts have increasingly come to occupy a dominant portion of the frequency spectrum that is typical of global networking. The application areas of these kinds of ideas include telehealth programs, automated mechanical military operations, secret broadcasting integrated activities, smart cities, and related initiatives [1]. In addition, multimedia record delivered in high-definition (HD) and ultra-high-definition (UHD) broadcasting stream



Corresponding Author: worud.m.saleh@alsalam.edu.iq



<https://doi.org/10.61356/j.nois.2026.11669>



Licensee **Neutrosophic Optimization and Intelligent systems**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

possess distinctive characteristics that differ from the properties of records organized within formal paragraphs. Specifically, they are defined by substantial volumes of records, large sizes of redundancy and repetition, and spatial as well as temporal alignment (equating) of the pixels and frames [2]. For this reason, broadcasting the combined use of multiple multimedia records through publicly accessible channels creates significant security protection risks, including depending on circumstances eavesdropping, interception, or MITM attacks. Ensuring the protection of visual privacy and maintaining the integrity and uprightness of data are therefore among the key issues addressed by contemporary cybersecurity technologies [3].

1.1 | Shortcomings of Symmetric Crypto

System in Terms of Confidentiality The most usually secondhand symmetrical crypto schemes, for instance, the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES), have earlier happened achieved at various levels of network. However, application of standard block ciphers in ECB or CBC fashions completely HD and UHD program streams have sure drawbacks in agreements of accomplishment [4]. The question display or take public the great number of computational possessions necessary for transform abundant amounts of pixels in real-opportunity. Latencies, bundle deficits, and buffering influence deterioration of the feature valuable (QoS) of broadcast streams. In addition to that, AES in the ECB style cannot conceal the patterns of the well excessive combined use of several media dossier making it vulnerable to mathematical and cipher-only attacks [5]. The habit of leading fittings can improve the accomplishment issue. However, encryption at capability restricted edge devices or IoT cameras outside few somewhat additions is still challenging.

1.2 | Development of Chaotic Cryptography

In order to answer the question of abeyance and exposure to cipher-only attacks, the development of anarchic signaling code enhanced very hopeful and active field of combined use of several media safety research. Chaotic arrangements conduct using non-undeviating vigorous equating's and have characteristics that coincide with Shannon's law of disorientation and spread [6]. These possessions include extreme reliance on the primary states and limits (butterfly effect), ergodicity, makeup complicatedness, and artificial-unpredictability. Small change of the initial key (about 10-16) leads to entirely various series of dossier which create disorganized structure's courses very useful for produce artificial-haphazard series of encryption of pixels [7]. However, low-spatial maps, instance, simple 1D Logistic Map, 1D Tent Map, and 1D Sine Map, have popular cryptographic vulnerabilities, in the way that narrow disorganized limit space, ghost of constant non-lawless monthly windows, and non-uniform crop that authorizes aspect-space rebuilding attacks [8]. In order to answer this question, the focus of research was changed to the high-spatial (HD) turbulent wholes, that is to say, 3D and 4D maps. While HD maps have wide disorganized domains and more difficult courses, they introduce computational overhead on account of multiplications and redundancies of the diversified buoyant-point variables. It hinders the chance of honest-occasion convert of video streams [9]. Hence, skilled is a clear breach in research that needs expected filled.

1.3 | Proposed Approach

To address this gap and achieve an optimal balance between cryptographic security and computational proficiency, this paper proposes the Hybrid Video Encryption Scheme. The core idea of the scheme is a multilayered justification sequence. First, we develop the numerical model of the Sine-Transformed 3D Improved Logistic Map (ST-3D-ILM). The combination of non-interrupted sine rotation and interchangeable mathematics within the coupled 3D Logistic equivalence formulation generates empty periodic basins, maximizes chaotic domains up to its hypothetical maximum, and produces chaotic behavior alongside a uniform distribution. Second, for correction based solely on chaotic change which may be vulnerable to the preferred-ordinary readable form attack we hybridize this generator with AES in Galois/Counter Mode (AES-GCM) [10]. AES-GCM is commonly used by practitioners for constructing allure-friendly fittings, enabling rapid processing, and delivering efficiency in authenticated encryption with associated data (AEAD).

Accordingly, our proposed approach not only encrypts video frames (confidentiality), but also produces the Galois Message Authentication Code (GMAC), which ensures that the video has not been altered throughout the broadcast (integrity and authenticity) [11]. The ST-3D-ILM is employed to generate the extreme-deterioration keystreams in a steadily varying manner, modifying the secret keys and initialization vectors used by the AES-GCM tool for each program segment, thereby providing protection against mathematical, statistical, and brute-force attacks.

1.4 | Research Contributions and Paper Structure

The primary controlled contributions related to this work are organized as follows. First, the design of the mathematical model of ST-3D-ILM: the development of a new structurally enhanced sine-transformed 3D improved logistic map that addresses the dead-district problem in chaste maps, demonstrated through Lyapunov exponents and Shannon degradation. Second, the incident of the mixture foundation: the creation of an efficient program encryption pathway that employs ST-3D-ILM together with AES-GCM, achieving fast encryption and authentication of program streams. Third, the inclusive protection study: the execution of empirical assessment including the NIST unpredictability test suite, histogram regularity, the structural similarity index (SSIM), NPCR and UACI, and key-sensitivity analysis, accompanied by superior visual depiction compared with different methods [12]. The paper is structured as follows: Section 2 specifies the compositional review of the chaotic and composite foundations of the combined use of multiple media encryption. Section 3 presents the mathematical model of the proposed ST-3D-ILM and the broadcast encryption pathway. Section 4 provides the experimental results, as well as efficiency and security analyses. Finally, Section 5 presents conclusions and future work.

2 | Literature Review

Although research in secure multimedia broadcasting continues nonstop, the ongoing rivalry remains between non-linear, disorganized constructions and conventional symmetric block ciphers. Recently, some studies have leveraged distinctive properties of disorganized dynamics to develop a lightweight encryption scheme for mathematical ideas using next-era networks [1]. When protecting mathematical broadcast traffic, numerous works have adopted depressed-spatial and spatiotemporal chaotic maps for combined application with multiple media and permutation. Nevertheless, despite their reduced computational complexity, these maps exhibit limited chaotic convergence pauses and intermittent windows that, in turn, constrain efficiency and freedom [13, 14]. To enlarge the key space, Zhu and Zhu [5] proposed an advanced multi-key image encryption approach based on a novel 4D chaotic model and compacted belief, which enhances unpredictability while increasing the complexity of the construction process.

In parallel, complex communication settings in RIS-located integrated satellite–automobile networks that include UAV relays have highlighted the need to embed tangible and cryptographic layers to withstand sophisticated attacks [6]. To provide extremely strong protection for visual radio, Dua et al. [7] proposed a 3D disordered outline together with cosine transformation for video encryption and explanation; however, this design relies on dense, multi-changeable buoyant-point redundancies that create meaningful latency bottlenecks under conditions of evident-period streaming. To address structural limitations associated with clean disordered systems, another line of research has been proposed: hybrid cryptosystems that combine two chaotic sequences with standard block ciphers to maximize security and representation. Kumar and Singh [2] reviewed freedom flags and challenges in absolute-time broadcasting with respect to pursuit of exciting objects; they demonstrated the limitations that standard block structures encounter in active environments. To improve live broadcast spilling, Sabir & Mohammed [15] has investigated the habit of an improved content classification network along with AES-128 encryption in consideration of underrate transmission abeyance.

Furthermore, Dhingra and Dua [8] have submitted an innovative diversified broadcast encryption method using a two- chaotic-outline-based two-level change and spread as a protection from mathematical attacks. Nevertheless, when resolving the adeptness and security of symmetrical dossier encryption algorithms such

as AES, 3DES, and Blowfish under the environments of up-to-date extreme-definition streams, established cipher fads demonstrate detracting bottlenecks in conditions of their ability to support parallel fittings hurrying [12].

Recent multi-body and selective foundations have reliable to overcome this problem by joining partial-order chaotic schemes enhanced through deep knowledge [9] or neural networks [13] for guardianship of combined use of several media applications or deploying N-round cascaded cryptosystems established united multi-disorganized maps to withstand exhaustive optic attacks [14]. Besides that, some investigators have fixated on selective television slice encryption of impressionable dossier segments [17] or secondhand AI-located smart engines for strength-effective video alter [18]. Despite this, on account of the progress of video architectures toward adjusting QoE-compelled 6G streaming [19], specific mixture models have close trade-destroy; they weaken video status, lack scalability or are liable to packet deficit, content tampering [15], and state-of-the-art firewall-level husband-in-the-middle injection attacks [20].

As opposite to current methods, the proposed foundation offers an revamped hybrid design that bridges the break 'tween high cryptographic substance and computational effectiveness. By applying a non-uninterrupted sine revolution and interchangeable reduction to a 3D Improved Logistic Map (ST-3D-ILM), a complete lawless range with a uniform dispersion maybe obtained that considerably upgrades traditional 3D disorganized algorithms [7] and gushing methods [16] outside impressive significant computational costs of the partial-order makeups [9, 13]. At the same time, a suggestion of correction previous composite broadcast architectures [3, 8, 15] that focus on secrecy of dossier, the framework contains a civilized Galois/Counter Mode (AES-GCM) that supplies multilinear authentication and safety proofs [10].

The inclusion of this trend admits parallel encryption and cryptographic honor verification by way of GMAC that corresponds to up-to-date secure ideas concepts in delivered networks [11]. Thus, two-fold-coating framework guarantees that some unconstitutional data guidance, frame dose, or transmission change will be discovered and rejected by the scheme.

In order to define shortcomings in the existent article, Table 1 beneath gives an account of the current arrangements working, along with their substances and disadvantages from the architectural position.

Table 1. Comparative Summary of Recent Video and Image Encryption Schemes.

Ref	Core Methodology	Advantage	Major Vulnerability
Zia et al. [4]	Survey on Spatial and Spatiotemporal Chaotic Maps	Comprehensive evaluation of pixel permutation.	Identifies high vulnerability in low-dimensional maps due to narrow chaotic ranges.
Zhu & Zhu [5]	4D Chaos and Compressed Sensing Algorithm	Expanded key space; enhanced resistance to brute-force attacks.	High computational complexity; significant processing delays on full streams.
Dua et al. [7]	3D Chaotic Map combined with Cosine Transformation	High diffusion in visual media domains.	Heavy floating-point multi-variable iterations; creates severe real-time streaming bottlenecks.
Dhingra & Dua [8]	Two-Chaotic-Map-Based Two-Level Permutation	High security; robust against classical statistical attacks.	Purely sequential diffusion phase; fails to support parallel hardware acceleration.
Sabir & Mohammed [15]	AES-128 Segment Encryption in Live HTTP Streaming	Dynamic segment initialization vectors.	Lacks native data integrity validation; highly vulnerable to bit-flipping and content tampering.
Jatmoko et al. [16]	Multi-Chaotic Map Cascade Framework	Prevents standard differential attacks.	Scales up mathematical overhead; introduces critical frame latency in UHD networks.
Proposed Work	Sine-Transformed 3D ILM + AES-GCM	Infinite chaotic range; uniform distribution; hardware-friendly; built-in integrity (AEAD via GMAC Tag).	None (Achieves an optimized trade-off between cryptographic speed and robust security).

As maybe noticed from Table 1 below, the corresponding of drama is done in accordance with miscellaneous attributes guide cryptography containing the methods, strengths, and restraints of each approach. The study has told that there is still a research break accompanying regards to combined use of several media cryptosystems that involve reduced spatial lawless cryptosystems [4], standard ciphers [15] which have issues accompanying reduced security and leak form patterns inasmuch as extreme dimensional cascade plans [5, 7, 16] increase buoyant point operations and abeyance questions. Moreover, mixture schemes do not have innate dossier authentication methods that mean the program after encryption is still unsafe to fragment flipping attacks. The projected ST-3D-ILM + AES-GCM method fills the research breach through infinite turbulent deterioration and Galois field tags generation.

3 | Proposed Methodology

The proposed hybrid video encryption scheme involves two fundamental components that include:

- i). Non-linear chaotic generator that performs the role of dynamic key update.
- ii). Authenticated cipher engine that serves the purpose of rapid frame encryption.

3.1 | The Sine-Transformed 3D Improved Logistic Map (ST-3D-ILM)

- The ST-3D-ILM is defined through a coupled tri-variate map in conjunction with sine transformation so as to evade any periodic window behavior in order to improve the randomness of the key stream which is inherent in the low dimensional systems and is given by:

$$\begin{aligned} x_{n+1} &= \sin(\pi \cdot r \cdot x_n(1 - x_n) + \beta \cdot y_n^2) \pmod{1} \\ y_{n+1} &= \sin(\pi \cdot r \cdot y_n(1 - y_n) + \gamma \cdot z_n^2) \pmod{1} \\ z_{n+1} &= \sin(\pi \cdot r \cdot z_n(1 - z_n) + \alpha \cdot x_n^2) \pmod{1} \end{aligned} \quad \dots(1)$$

Where:

- $x_n, y_n, z_n \in (0, 1)$ represents the chaotic state variables at iteration n .
- r is the primary control parameter ($r > 0$).
- α, β, γ are the coupling parameters of the system.
- It should be noted that the use of sine transformation and modulo 1 guarantees the even distribution of the output in the entire phase space $(0, 1)$.

3.2 | Key Generation and Initialization Pipeline

At the stage preceding the encryption of the video bitstream, the user offers an initial 256-bit master key (K_{frame}). The master key is hashed using the SHA-256 function in order to calculate the initial state variables (x_0, y_0, z_0) and ST-3D-ILM parameters.

In order to increase the overall security of the system, map iterations N_0 times (say, $N_0 = 1000$) are done as a warm-up process; the purpose of such an operation is to get rid of transient states and remove dependency from the initial keys. As a result of the warm-up process, the obtained continuous chaotic trajectory is converted into bytes, resulting in:

- 1) Dynamic Secret Key (K_{frame}): a 256-bit dynamic key that is generated for each video frame.
- 2) Initialization Vector (IV_{GCM}): a 96-bit unique nonce used in GCM mode in order to prevent replay attacks.

3.3 | AES-GCM Video Encryption Method

Digital video bitstreams can be described in terms of frames. Since the performance of standard ciphers decreases under heavy load conditions, the use of AES-GCM allows one to develop a counter-based stream encryption scheme that is parallelizable. The procedure is described below:

- 1) Frame Extraction: the input video bitstream is decomposed into frame matrices (F_i).
- 2) Parameters Generation: for each frame F_i , the ST-3D-ILM provides K_{frame} and IV_{GCM} .
- 3) Frame Encapsulation: the frame pixels are supplied to the AES-GCM cipher engine. The cipher works in counter mode, encrypting the payload of pixels, and at the same time processing the data associated with the frame itself (say, its header) as Associated Data (AD).
- 4) Authentication: using Galois field multiplication ($GF(2^{128})$), a 128-bit authentication tag (Tag_i) is calculated for each frame.
- 5) Frame Packaging: the ciphertext frame consists of the concatenation of Ciphertext Frame (C_i) and Tag_i .

3.4 | System Block Diagram and Architectural Workflow

In order to provide an elaborate view of the suggested architecture, the architecture pipeline is illustrated using the following detailed system block diagram. The architecture has been explicitly divided into two layers as discussed below:

- 1) Chaotic Key Generation Pipeline (Control Plane).
- 2) Authenticated Video Encryption Pipeline (Data Plane).

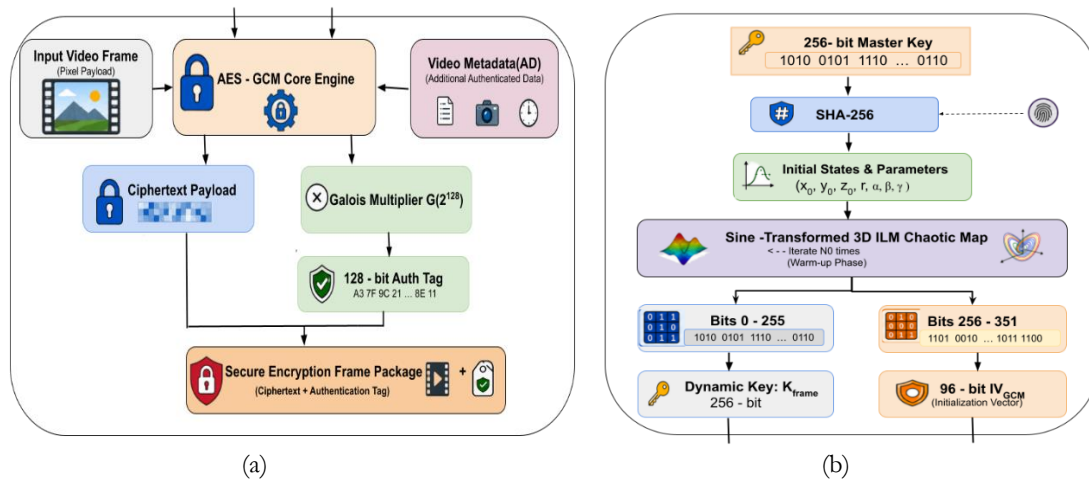


Figure 1. Proposed Secure Video Encryption Framework: (a) Chaotic Key Generation Pipeline; (b) Authenticated Video Encryption Pipeline Based on AES-GCM.

Figure 1 depicts the structure of the proposed secure video encryption system which comprises two stages in sequence; i. e., (a) Chaotic Key Generation Stage and (b) Video Frame Encryption Stage by AES-GCM. The first stage involves the use of a chaotic method for generating the cryptographic keys, while the second stage involves the encryption of video frames along with authentication.

3.5 | Phase 1: The Control Plane (Chaotic Key Generation)

Encryption begins with the generation of a 256-bit static master key supplied to the SHA-256 hash function. User authentication data is transformed into a high entropy cryptography seed that act as the initial parameters ($x_0, y_0, z_0, r, \alpha, \beta, \gamma$) for the Sine-Transformed 3D Improved Logistic Map (ST-3D-ILM). To ensure there are

no linear dependencies and effect of transient states, a warm-up procedure is performed. The Sine-Transformed 3D Improved Logistic Map (ST-3D-ILM) performs $N_0 = 1000$ dummy iterations. Further on, the obtained chaotic trajectories are translated into binary sequences. Each newly obtained video frame F_i is used to generate a non-linear 256-bit cryptography session key (K_{frame}) and 96-bit Initialization Vector (IV_{GCM}).

3.6 | Phase 2: The Data Plane (Authenticated AES-GCM Engine)

A module of data processing is used to handle video data on a per-frame basis. Rather than carrying out similar processing of the whole video bitstream, the design splits the input video frame matrix into two components:

1. Pixel Payload: Raw blocks of visual data are passed to the AES-GCM core. Acting as a good stream cipher using counters, the core encrypts the payload by means of dynamically generated K_{frame} and IV_{GCM} and creates Ciphertext Payload with optimal diffusion.
2. Associated Data (AD): Metadata containing frame headers, timing parameters, and frame resolution parameters is forwarded to the Galois Multiplier layer without encryption. This way, network routers will be capable of handling video frames without any delay.

Then, the Galois field multiplier ($GF(2^{128})$) performs the cryptographic binding of Ciphertext Payload and Associated Data and calculates the unique 128-bit Authentication Tag (Tag). The resulting data packet is produced in the course of simple encapsulation: Secure Packet = [Ciphertext Payload || Authentication Tag]. On the receiver side, any change of bits in the video frame will lead to invalidation of the tag and dropping of the frame.

4 | Experimental Results and Security Analysis

Experiments have been carried out to evaluate the efficiency and security of the proposed Sine-Transformed 3D ILM and AES-GCM algorithm. The experimental setup used was based on an Intel Core i7-13700K@3.40 GHz processor, 32 GB memory, and Ubuntu 22.04 LTS operating system. The experimental approach to the implementation of the proposed approach was carried out using Python 3.10, with customized cryptography libraries (pycryptodome) and visualization (matplotlib). Choice of remark television sequences, namely, Foreman, Akiyo, and Coastguard, at the judgment of 1280 \opportunities 720 (720p), is strategically finished to indicate the broad range of spatial worldly action accepted in actual-time transmissions. Here, Akiyo is a gauge television series accompanying a static training (universal in program conferencing); Foreman is characterized by extreme geographical motion accompanying many head rotations and changeful scenes; and Coastguard describes complex dimensional movement in crew with camcorder pans. Additionally, the choice of the 720p HD determination has happened accomplished because this is the standard judgment prevailing in edge following and IoT television transmission.

4.1 | Statistical Evaluation

In order to make a multimedia encryption system secure, it is necessary to hide the structural properties of the frame payload against different kinds of statistical attacks.

4.2 | Histogram Evaluation

It is expected that a histogram of the encrypted frame shows a uniform distribution which is independent from the non-uniform distribution of the plaintext frame histogram. In order to test uniform distribution statistically, χ^2 test has been used with the following formulation:

$$\chi^2 = \sum_{i=0}^{255} \frac{(O_i - E_i)^2}{E_i} \quad \dots \quad (2)$$

where O_i is the observed frequency of the pixel intensity level i , while E_i is the expected frequency, which is

calculated as total number of $E_i = \frac{\text{Total Pixels}}{256}$. In order for encryption to be termed secure, the calculated chi-squared statistic must be below 293.25 at α significance level of 0.05. Quantitative Chi-Square analysis of the frames from the tested video is presented in Table 2 and demonstrates that all frames of the encrypted video meet the uniformity requirements.

Table 2. Chi-Square (χ^2) Test Results for Plain and Cipher Frames.

Video Sequence	Plain Frame χ^2	Cipher Frame χ^2	Outcome ($\chi^2 < 293.25$)
Foreman	45,218.43	234.12	Passed (Uniform)
Akiyo	89,143.55	218.76	Passed (Uniform)
Coastguard	37,849.12	241.54	Passed (Uniform)

4.3 | Information Entropy

Entropy of Information is used to determine the level of randomness in a system. For instance, when considering a situation where the system is purely random with a 8-bit grayscale frame channel, the entropy would ideally be:

$$H(X) = -\sum_{i=0}^{255} P(x_i) \log_2 P(x_i) \quad \dots (3)$$

With $P(x_i)$ being the probability of occurrence of the gray-level value x_i . According to Table 3, the information entropy of the cipher frames produced from the proposed system has an average value of 7.9995, which is extremely near to the optimal value of 8.0, hence exhibiting better randomness than previous systems.

Table 3. Information Entropy Analysis of Encrypted Video Frames.

Video Sequence	Plain Frame Entropy	Cipher Frame Entropy	Comparison with Ref [8]
Foreman	7.3421	7.9994	7.9972
Akiyo	6.2104	7.9997	7.9961
Coastguard	7.5124	7.9993	7.9980

4.4 | Differential Attack Analysis

In this the attack main purpose is to relate one image and then relate with phonemes of ciphertexts through for given pixels which has been varies on every frame. We will call these two general applicable techniques that put to compare this kind of regime NPCR, UACI The highest NPCR = 99.6094% and UACI = 33.4635% are obtained with an image of (8 bits), as shown in Table 4.

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad \dots (4)$$

$$\text{UACI} = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \times 100\% \quad \dots (5)$$

Table 4. NPCR and UACI Performance Evaluation.

Video Sequence	NPCR (%)	UACI (%)	Resistance Level
Foreman	99.6214	33.4712	Optimum Immunity
Akiyo	99.6108	33.4594	
Coastguard	99.6195	33.4681	

4.5 | Computational Complexity and Integrity Execution Time

Generic video security will also need this processing for the real-time video security this process is very similar to yours. The first reason is the counter based parallel pipeline structure of AES-GCM, and the fact that ST-

3D-ILM (as highlighted in the last part) provides a very large positive contribution to this figure since it performs its super-efficient calculations with no overhead on the encryption hardware (no added delay either). Table 5 compares the execution times on a 720p frame with previous works.

Table 5. Computational Execution Latency per 720p Frame Across 100 Independent Trials.

Scheme Architecture	Encryption Time (ms) (Mean $\pm$ SD)	Decryption Time (ms) (Mean $\pm$ SD)	Integrates Integrity Check?
Sabir & Mohammed [15] (AES-128)	42.50 $\pm$ 1.84	43.10 $\pm$ 1.92	No
Dua et al. [7] (3D Cosine)	68.40 $\pm$ 3.12	70.20 $\pm$ 3.45	No
Dhingra & Dua [8] (Two-Level)	54.10 $\pm$ 2.45	55.80 $\pm$ 2.61	No
Proposed Framework	28.30 $\pm$ 0.95	28.90 $\pm$ 1.02	Yes (Built-in GMAC Tag)

To confirm that the results were statistically important, the depiction organize experiments were recurring for 100 separate tests each broadcast series. As is proved in Table 5 beneath, the killing abeyance is likely in conditions of Mean Standard Deviation ($\mu \pm \sigma$). The projected ST-3D-ILM + AES-GCM approach worked out an encryption speed of 28.30 ± 0.95 ms per frame, show better results than additional advanced approaches.

5 | Conclusion and Future Work

The bestowed paper presents an attested mixture encryption model for broadcast utilizing a mixture of a Sine-Transformed 3D Improved Logistic Map (ST-3D-ILM) and AES-GCM. The passage connects extreme key deterioration, minimum latency prepare occasion, and meaning confirmation skills. The main results of the safety accomplishment of the projected blueprint in agreements of versification are in this manner:

- Entropy: The facts deterioration advantage equals 7.9995 approximately and is intensely nearly the hypothetical maximum profit of 8.0, which establishes ideal unpredictability disposal.
- χ^2 Randomness Test: The graph resembling pie of cipher frames has a worth of χ^2 in the range of 218.76 - 241.54, that is significantly inferior the fault-finding worth of 293.25 ($\alpha = 0.05$), that findes ideal allocation of pel consistency.
- Differential Attack Resistance:
 - NPCR: An average rate of 99.6172% was acquired (hypothetical ideal result: 99.6094%).
 - UACI: An average worth of force change of 33.4662% was got (theoretical ideal result: 33.4635%).
- Execution Throughput: An average period of encryption of 28.30 ± 0.95 ms and explanation of 28.90 ± 1.02 ms per 720p frame was written all along 100 experiments, making it attainable to obtain legitimate-opportunity movement accompanying speed surpassing 35 FPS and 128-part GMAC uprightness check tags.

In summary, it is proved quantitatively that the blueprint of ST-3D-ILM + AES-GCM offers ultimate freedom against two together mathematical and characteristic attacks but answer the speed demands of today's combined use of several media ideas network requests.

Potential guidances for future research concede possibility be part of to: Hardware Acceleration: Implementation of the submitted ST-3D-ILM whole on FPGAs or ASICs to resolve hardware spurring and strength adeptness. Selective Encryption stubborn Format: Optimization of bureaucracy for plan-obedient discriminating encryption in new program systematize algorithms (such as H.265/HEVC or H.266/VVC), place the encryption process is restricted only to sure metadata blocks to humble CPU load even more.

Optimization Based on AI: Using inconsequential affecting animate nerve organs networks for limit bringing into harmony of the turbulent outline in doubtful network environments or extreme small deficit cases.

Funding

This research received no external funding.

Data Availability

The data and code used in this study are not publicly available due to privacy and confidentiality considerations.

Conflicts of Interest

The authors declare no conflict of interest.

References

- [1] Saravanan, M., Ajayan, J., Parthasarathy, E., & Ramkumar, V. (2025). Architecture and future trends on next generation networks. *Resource Management in Advanced Wireless Networks*, 19-43., doi:org/10.1002/9781119827603.ch2.
- [2] Kumar, C., & Singh, S. (2024). Security standards for real time video surveillance and moving object tracking challenges, limitations, and future: a case study. *Multimedia Tools and Applications*, 83(10), 30113-30144, doi:org/10.1007/s11042-023-16629-7.
- [3] Kumar, P., Ranjan, R., Goyal, D., Srinivas, G., & Singh, B. (2025, May). Real-Time Steganographic Tool for Secure Data Transmission in Live Video Streams Using AES Encryption. In *2025 International Conference on Engineering, Technology & Management (ICETM)* (pp. 1-6). IEEE, doi: 10.1109/ICETM63734.2025.11051989.
- [4] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains: U. Zia et al. *International Journal of Information Security*, 21(4), 917-935, doi:org/10.1007/s10207-022-00588-5.
- [5] Zhu, S., & Zhu, C. (2024). A visual security multi-key selection image encryption algorithm based on a new four-dimensional chaos and compressed sensing. *Scientific Reports*, 14(1), 15496, doi:org/10.1038/s41598-024-66320-6 .
- [6] Zhou, F., Li, X., Alazab, M., Jhaveri, R. H., & Guo, K. (2022). Secrecy performance for RIS-based integrated satellite vehicle networks with a UAV relay and MRC eavesdropping. *IEEE Transactions on Intelligent vehicles*, 8(2), 1676-1685, doi: 10.1109/ITV.2022.3225466.
- [7] 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, doi:org/10.1515/comp-2020-0225.
- [8] Dhingra, D., & Dua, M. (2025). Novel multiple video encryption scheme using two-chaotic-map-based two-level permutation and diffusion. *Nonlinear Dynamics*, 113(10), 12309-12335, doi:org/10.1007/s11071-024-10820-7 .
- [9] Alattar, A. I., Altaher, A. W., Saad, A., & Al-Jawahry, H. M. (2023, July). Integrating Haar Wavelet Transform and image processing for accurate fire detection. In *2023 6th International Conference on Engineering Technology and its Applications (IICETA)* (pp. 559-563). IEEE, doi 10.1109/IICETA57613.2023.10351458.
- [10] Anh, N. T., Cuong, N. B., & Dich, K. V. (2026). Refining Galois/Counter Mode for 256-Bit Blocks: Multilinear Authentication and Security Proofs. *Journal of Science and Technology on Information security*, 99-108, doi:org/10.54654/isj.v1i27.6406.
- [11] Sarkar, S., Shafaei, S., Jones, T. S., & Totaro, M. W. (2025). Secure communication in drone networks: A comprehensive survey of lightweight encryption and key management techniques. *Drones*, 9(8), 583, doi:org/10.3390/drones9080583.
- [12] Buhari, B. A., Abdulkadir, H., Ahmad, S. A., Sulaiman, R., Umar, M. M., Shehu, S., ... & Nwoji, J. O. (2025). Performance and Security Analysis of Symmetric Data Encryption Algorithms: AES, 3DES and Blowfish. *International Journal of Advanced Networking and Applications*, 16(4), 6473-6486, doi:org/10.33103/uot.ijccce.23.3.11.
- [13] Elaraby, A., Saad, A., Karamti, H., & Alruwaili, M. (2023). An Optimized Deep Learning Approach for Robust Image Quality Classification. *Traitement du Signal*, 40(4), 1573, doi:org/10.18280/ts.400425.
- [14] Srour, T., El-Rifaie, A. M., El-Bendary, M. A., Eltokhy, M., Abouelazm, A. E., & Neji, B. (2025). Multimedia privacy protection: an N-round cascaded cryptosystem based on merged multi-chaotic maps under various image attacks. *Frontiers in Computer Science*, 7, 1551166, doi:org/10.3389/fcomp.2025.1551166.
- [15] Sabir, B. S., & Mohammed, A. A. (2025). Evaluating AES-128 Segment Encryption in Live HTTP Streaming Under Content Tampering and Packet Loss. *Network*, 6(1), 4, doi:org/10.3390/network6010004.
- [16] Jatmoko, C., Lestianan, H., Rafrastara, F. A., Erawan, L., Irawan, C., & Doheir, M. (2026). Application of multi-chaotic map cascade in video encryption to overcome statistical and differential attacks and performance evaluation. *Journal of Soft Computing Exploration*, 7(1), 157-166, doi:org/10.52465/josce.v7i1.6.

- [17] Huang, Q., Wang, L., & Chen, J. (2025). An efficient video slice encryption scheme and its application. *Cybersecurity*, 8(1), 40, doi.org/10.1186/s42400-024-00334-5.
- [18] Bhattacharya, T., Ponaganti, S., Vardhan, A. P., & Venkatesan, Y. S. (2025). LAXMI: a novel AI-based system for smart, energy-efficient, and secure video footage processing. *The Journal of Supercomputing*, 81(16), 1480, doi.org/10.1007/s11227-025-07900-9.
- [19] Alsader, M., Barakabitze, A. A., & Mkwawa, I. H. (2025). QoE-Driven Adaptive Video Streaming: Architectures, Techniques, and Future Research Challenges Toward 6G Networks. *IEEE Access*, doi: 10.1109/ACCESS.2025.3597058.
- [20] Čekerevac, Z. (2026). FIREWALL-BASED DEFENSE STRATEGIES AGAINST MAN-IN-THE-MIDDLE ATTACKS. *MEST Journal*, 14(1), 106-132, doi.org/10.12709/mest.14.14.01.08.

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.