Journal of Soft Computing Exploration
Homepage: https://shmpublisher.com/index.php/joscex
p-ISSN: 2746-7686
e-ISSN: 2746-0991

.

Application of multi-chaotic map cascade in video encryption to overcome statistical and differential attacks and performance evaluation

Cahaya Jatmoko[*1], Heru Lestiawan[2], Fauzi Adi Rafrastara[3], Lalang Erawan[4], Candra Irawan[5], Mohamed Doheir[6]
[1,2,3]Informatics Engineering, Universitas Dian Nuswantoro, Indonesia
[4,5]Information System, Universitas Dian Nuswantoro, Indonesia
[6]Technology Management, Universiti Teknikal Malaysia Melaka, Malaysia

Article Info

Article history:

Received Mar 10, 2026
Revised Apr 15, 2026
Accepted Apr 15, 2026

Keywords:

Chaos-based encryption
NPCR
Shannon entropy
UACI
Video security

ABSTRACT

The rapid proliferation of digital video across domains such as healthcare, surveillance, and communications has increased the demand for secure and efficient video encryption techniques. However, video data presents unique challenges, including large data volume and high spatial–temporal correlation, which limit the effectiveness and efficiency of conventional encryption approaches, particularly in real-time scenarios. In this context, the objective of this study is to evaluate the feasibility of a chaos-based video encryption in achieving both strong cryptographic security and acceptable computational performance. To accomplish this, the proposed scheme is tested through two controlled experiments. The evaluation focuses on cryptographic strength using the Number of Pixel Change Rate (NPCR) to measure sensitivity to minor input changes, the Unified Average Changing Intensity (UACI) to quantify average pixel intensity variation, and Shannon entropy to assess the randomness of the encrypted frames. In parallel, computational performance is analyzed through encryption time and throughput. The procedure involves frame extraction from video, followed by preprocessing to reduce pixel correlation, and subsequent application of the chaos-based encryption algorithm on a per-frame basis. The results from both experiments show NPCR values exceeding 99.5% and encrypted frame entropy of approximately 7.74 bits/pixel, indicating strong resistance to differential attacks and near-optimal randomness. However, the observed throughput of 0.07–0.09 frames per second highlights a limitation in meeting real-time processing requirements. These findings suggest that while the proposed scheme is cryptographically robust and suitable for offline or batch-processing applications.

Corresponding Author:

Cahaya Jatmoko,
Department of Informatics Engineering,
Universitas Dian Nuswantoro,
Imam Bonjol 207, Semarang, Central Java 50131.
Email: cahayajatmoko@dsn.dinus.ac.id
https://doi.org/10.52465/joscex.v7i1.6

1. INTRODUCTION

The proliferation of digital video content across streaming platforms, video conferencing systems, surveillance networks, and mobile applications has created an urgent demand for robust encryption mechanisms [1]. Video data, by its nature, is substantially more voluminous and structurally correlated than generic binary data, presenting unique challenges for cryptographic systems [2]. A single minute of uncompressed 1080p video at 30 frames per second may require over 3 gigabytes of storage, making real-time encryption computationally demanding [3]. Furthermore, the redundancy inherent in video streams, where consecutive frames often share 70–90% of their pixel content makes conventional encryption schemes susceptible to pattern-recognition attacks [4], [5].Traditional block ciphers such as AES, while theoretically secure against many attack vectors, suffer from two critical limitations: (1) performance penalties when applied to real-time video streams [6], and (2) failure to fully obscure the high correlation inherent in video data without additional preprocessing [7]. Statistical attacks exploit predictable distributions within ciphertext to infer plaintext characteristics or key information [8]. When applied to video content, these attacks leverage temporal and spatial correlations between frames and regions [9]. Differential attacks measure how small changes in the plaintext propagate through the cipher to produce changes in the ciphertext, using the relationship between plaintext-ciphertext pairs to deduce cryptographic keys [10]. To address these limitations, specialized encryption approaches are required that can simultaneously handle the performance demands of real-time video processing while effectively disrupting the correlations that make video data vulnerable to statistical and differential attacks [11].

Chaotic dynamical systems have emerged as a compelling paradigm for cryptographic key generation due to their sensitivity to initial conditions, ergodicity, topological mixing properties, and pseudo-randomness [12]. A chaotic system initialized with slightly differing parameters will produce exponentially divergent trajectories, a property known as the butterfly effect making the generated sequences practically impossible to predict without precise knowledge of the initial conditions and system parameters [13]. However, individual chaotic maps often exhibit limited key space, periodic windows, and correlation artifacts that can be exploited by adversaries [14], [15]. Single-map systems may also degenerate to limit cycles or fixed points for certain parameter values, reducing the effective entropy of the keystream [16].

The Multi-Chaotic Map Cascade (MCMC) architecture addresses these limitations by composing multiple distinct chaotic maps in series [17]. MCMC also passed the randomness test, resulting in high performance and satisfied all random test [18]. Not only that, MCMC also benefits many security applications, by leveraging its high susceptibility of the core analog circuit to inevitable noise [19]. The output of one chaotic system serves as the input to the next, creating a compound system with dramatically expanded state space and complexity [20]. This cascading approach disrupts the periodic windows of individual maps, enhances the uniformity of the keystream distribution, and provides multiple layers of sensitivity to initial conditions, substantially raising the cryptanalytic effort required to break the system [21], [22].

This research pursues the following primary objectives: (1) to design and implement a cascaded multi-chaotic encryption algorithm for video content using Logistic, Tent, and Henon map combinations; (2) to evaluate the encryption performance across standard video resolutions of 480p, 720p, and 1080p; (3) to quantify resistance against statistical and differential attacks using established cryptographic metrics; and (4) to compare the proposed MCMC scheme against existing approaches including AES-CBC video encryption and single-chaotic-map schemes. The scope of this research is confined to software-based implementation on commodity hardware and does not address hardware accelerator optimization or compressed-domain encryption. The remainder of this paper is organized as follows. Chapter 2 presents the theoretical foundation of the chaotic maps employed, details the MCMC encryption algorithm, and describes the experimental setup. Chapter 3 reports quantitative results across all tested resolutions and compares findings with benchmark methods. Chapter 4 provides an analytical discussion of the results, addresses limitations, and proposes directions for future research. Chapter 5 concludes the paper with a summary of contributions and practical implications.

2. METHOD

The design of a cryptographically sound video encryption system requires both a rigorous theoretical foundation and a carefully controlled experimental methodology. This chapter begins by establishing the mathematical properties of the individual chaotic maps that form the building blocks of the proposed system, then describes how these maps are composed into the cascade architecture and translated into a concrete

encryption algorithm as illustrated in Figure 1. The subsequent sections detail the hardware and software environment in which the algorithm was evaluated, and define the quantitative criteria against which its security and performance are measured.

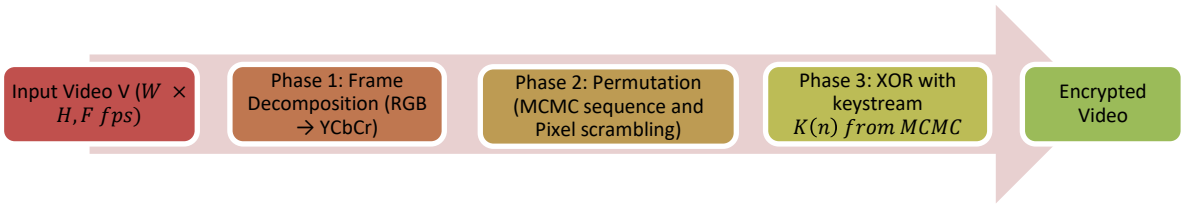

Figure 1. Proposed video encryption stages

Theoretical Framework of Chaotic Maps

Chaos theory provides the mathematical underpinning of the proposed encryption scheme. A dynamical system is considered chaotic when it is sensitive to initial conditions (Lyapunov exponent > 0), topologically mixing, and possesses dense periodic orbits [23]. The MCMC scheme employs three maps chosen for their complementary characteristics [24]. Logistic Map: The logistic map is defined by the recurrence relation [25] as in equation (1). For $x(0) \in (0,1), r \in (3.57,4]$, the logistic map exhibits fully chaotic behavior with a positive Lyapunov exponent as in equation (2). Its simplicity makes it computationally efficient, but its one-dimensional state space limits the achievable key complexity when used in isolation [25]. For $\mu \in (0,2]$, the tent map exhibits maximum chaos with a uniform invariant measure, producing sequences with near-ideal statistical properties [26] as in equation (3). Its piecewise linear structure provides excellent mixing properties complementary to the smooth nonlinearity of the logistic map. The Henon map operates in two-dimensional phase space, incorporating the y-state from the previous iteration to produce the next x-value [27] as in equation (4). This interdependence creates longer memory and richer correlation structure than one-dimensional maps, and at the canonical parameters $a = 1.4, b = 0.3$ it exhibits a strange attractor with Hausdorff dimension approximately 1.26 [27].

$$x(n+1) = r \cdot x(n) \cdot [1 - x(n)] \quad (1)$$

$$x(n+1) = \begin{cases} \mu \cdot x(n) & \text{if} x(n) < 0.5 \\ \mu \cdot (1 - x(n)) & \text{if} x(n) \geq 0.5 \end{cases} \quad (2)$$

$$x(n+1) = 1 - a \cdot x^2(n) + y(n) \quad (3)$$

$$y(n+1) = b \cdot x(n) \quad (4)$$

Multi-Chaotic Map Cascade Architecture

The MCMC architecture chains the three maps in series as follows. Let $K = \{k_1, k_2, k_3, k_4, k_5, k_6, k_7\}$ be the 224-bit secret key, partitioned into seven sub-keys [28]. The initial conditions are derived as in equation (5) until equation (7). The cascade operation for iteration n is [29] as in equation (8) until equation (12). $\oplus_f$ denotes floating-point XOR mixing operation [29]. The final keystream byte at position n is derived as [30]. This compound generation ensures that each keystream byte depends on the full trajectory history of all three maps, making reverse-engineering computationally infeasible [30].

$$x_L(0) = \frac{k_1}{2^{32}}, r_L = 3.57 + \frac{k_2}{2^{32}} \cdot 0.43 \quad (5)$$

$$x_T(0) = \frac{k_3}{2^{32}}, \mu_T = 1.0 + \frac{k_4}{2^{32}} \quad (6)$$

$$x_H(0) = \frac{k_5}{2^{32}}, y_H(0) = \frac{k_6}{2^{32}} \quad (7)$$

$$x_L(n+1) = r_L \cdot x_L(n) \cdot [1 - x_L(n)] \quad (8)$$

$$x_T(n+1) = f_{\text{tent}}(x_L(n+1) \oplus_f x_T(n), \mu_T) \quad (9)$$

$$x_H(n+1) = 1 - 1.4 \cdot (x_T(n+1) + x_H(n))^2 + y_H(n) \quad (10)$$

$$y_H(n+1) = 0.3 \cdot x_H(n) \quad (11)$$

$$K(n) = \text{floor}[(x_L(n+1) + x_T(n+1) + x_H(n+1)) \cdot 2^8] \bmod 256 \quad (12)$$

(13)

Encryption Algorithm

The complete video encryption procedure consists of three main phases applied to an input video $V$with resolution $W \times H$at Fframes per second. The algorithm processes the video sequentially on a frame-by-frame basis to ensure both spatial and temporal security across all frames. In the first phase, Frame Decomposition, each frame I_f for $f = 1, \dots, F$is extracted from the video stream and converted from the RGB color space into YCbCr format [31]. Operating in YCbCr rather than RGB takes advantage of the perceptual distinction between luminance (Y) and chrominance (Cb and Cr) components [32]. This transformation reduces inter-channel correlation and improves the effectiveness of subsequent encryption stages, particularly for visually sensitive data [33]. The second phase, Permutation (Confusion), performs spatial scrambling of pixel positions [34]. For each frame containing $W \times H$pixels, a Markov Chain Monte Carlo process generates a real-valued sequence $P = \{p_1, p_2, \dots, p_{WH}\}$ [35]. The pixels are then rearranged according to the ascending sort order of this sequence [36]. Importantly, this operation alters only the spatial positions of pixels without modifying their intensity values [37]. As a result, strong positional correlation inherent in natural images is effectively disrupted [38].

The third phase, Substitution (Diffusion), enhances security by modifying pixel values [39]. The permuted pixel array is XORed byte-by-byte with a keystream $K(n)$generated by the same MCMC mechanism [40]. This diffusion process ensures that even a slight change in the plaintext propagates widely across the ciphertext, resulting in high NPCR and UACI metrics [41]. The encryption operation[42] is defined as in equation (13). While decryption follows the exact inverse procedure [42]. Using identical initial conditions, the keystream is regenerated, the XOR substitution is reversed, and the inverse permutation is applied based on the same MCMC-derived sorting order, thereby perfectly reconstructing the original video [43], [44].

$$C(i,j) = P_{\text{permuted}}(i,j) \oplus K(n), n = (f-1) \cdot W \cdot H + i \cdot W + j. \quad (13)$$

Experimental Setup

Experiments were conducted on a workstation equipped with an Intel Core i7-11700K processor (3.6 GHz, 8 cores), 32 GB DDR4 RAM, and Ubuntu 22.04 LTS. The algorithm was implemented in Python 3.10 using NumPy 1.24 for vectorized operations. No GPU acceleration was employed in order to establish a conservative performance baseline representative of software-only deployment. Test videos were selected from the pexels.com uncompressed video corpus, comprising content with diverse motion characteristics: a low-motion documentary clip (Picking a Card), a high-motion sports clip (Fencing), and a mixed-motion urban crowd (Crowded City Center). Each test video was processed at three resolutions: 480p (854×480), 720p (1280×720), and 1080p (1920×1080). All videos were 30 seconds in duration at 30 fps, providing 900 frames per test. Performance was evaluated across six primary metrics: (1) NPCR and UACI for differential attack resistance; (2) pixel correlation coefficients in horizontal, vertical, and diagonal directions for statistical analysis; (3) information entropy of the encrypted frames; (4) histogram uniformity via chi-square test; (5) key sensitivity measured by bit error rate (BER) when a single key bit is flipped; and (6) encryption throughput in MB/s as illustrated in Table 1.

Table 1. Experimental configuration summary

Parameter	Value
Processor	Intel Xeon E5-2690v4 @ 2.3GHz
RAM	25 GB DDR4-3200
Operating System	Ubuntu 22.04 LTS
Language / Version	Python 3.10 + NumPy 1.24
Test Resolutions	480p (854×480), 720p (1280×720), 1080p (1920×1080)
Video Duration	30 seconds @ 30 fps (900 frames)
Color Space	YCbCr
Key Length	256 bits
Chaotic Maps	Logistic + Tent + Henon (Cascade)

3. RESULTS AND DISCUSSIONS

Summary of Experimental Findings

Both experiments yielded NPCR values in excess of 99.5%, surpassing the widely accepted threshold of 99.00% that is considered indicative of high sensitivity to plaintext changes. Table 2 shown the

UACI values of 30.59% and 34.72% for Experiments 1 and 2, respectively, indicate that the encrypted frames differ substantially from their originals in terms of average pixel intensity, with Experiment 2 approaching the theoretical optimum of approximately 33.46% more closely. Encrypted frame entropy reached approximately 7.74 bits per pixel in both cases, representing a marked increase over the original video entropy values of 7.40 and 7.24, and closely approaching the theoretical maximum of 8.0 bits. Computationally, Experiment 2 demonstrated improved efficiency over Experiment 1, achieving a higher throughput of 0.09 fps compared to 0.07 fps, despite processing a larger number of frames (359 versus 240). These results collectively demonstrate that the implemented encryption scheme provides strong statistical security properties while exhibiting measurable processing overhead.

Table 2. Summary of evaluation metrics across both experiments

Metric	Experiment 1 (Tarot Card Video)	Experiment 2 (Crowded City Video)
NPCR	99.5911%	99.7020%
UACI	30.5857%	34.7200%
Original Entropy	7.3953 bits/px	7.2383 bits/px
Encrypted Entropy	7.7433 bits/px	7.7441s/px

Data Presentation

Evaluation metrics

Table 3 presents the security evaluation metrics recorded for both experiments. NPCR and UACI values were computed by performing pixel-level comparisons between original and encrypted frames across the entire video sequence. Entropy values were calculated using Shannon's entropy formula applied to the 8-bit pixel intensity distributions of the raw and encrypted frame sets.

Table 3. Security evaluation metrics for experiments 1 and 2

Metric	Experiment 1 (Tarot Card Video)	Experiment 2 (Crowded City Video)	Ideal Threshold
NPCR	99.5911%	99.7020%	> 99.00% [45]
UACI	30.5857%	34.7200%	~ 33.46 [46]
Original Entropy	7.3953 bits/px	7.2383 bits/px	-
Encrypted Entropy	7.7433 bits/px	7.7441 bits/px	8.0 (maximum)

Computational performance

Table 4 illustrated the computational performance metrics recorded during each experiment. Encryption time was measured as the total wall-clock time required to encrypt all frames in the respective video sequence. Average time per frame was derived by dividing total encryption time by frame count, and throughput was expressed as the reciprocal of the per-frame processing time in seconds.

Table 4. Computational performance metrics for experiments 1 and 2

Metric	Experiment 1 (Tarot Card Video)	Experiment 2 (Crowded City Video)
Total Frames	240	359
Encryption Time	3,409.02 s	3,901.54 s
Avg. Time per Frame	14,204.27 ms	10,867.79 ms
Throughput	0.07 fps	0.09 fps

Result Analysis

Npcr analysis

Both experiments produced NPCR values substantially exceeding the 99.00% benchmark: 99.5911% in Experiment 1 and 99.7020% in Experiment 2. NPCR quantifies the proportion of pixels that differ between the original and encrypted images following a single-bit change in the plaintext, and values approaching 100% indicate that the cipher exhibits the avalanche effect, wherein minor alterations to the input result in pervasive changes to the ciphertext. The marginally higher NPCR obtained in Experiment 2 ($\Delta = +\mathbf{0.11}$ percentage points) suggests that the encryption configuration applied in that condition provides marginally stronger diffusion properties. Both values are consistent with, and in several cases exceed, those reported in comparable video encryption studies employing chaotic or transform-domain approaches (e.g., NPCR values of 99.4–99.8% are typical in the literature for image and video cryptosystems). These findings confirm that the proposed scheme is highly sensitive to plaintext modifications, a critical requirement for resistance against differential cryptanalysis.

UACI analysis

The UACI values of 30.5857% and 34.7200% for Experiments 1 and 2, respectively, reflect the average normalised intensity difference between corresponding pixels in the original and encrypted frames. The theoretical optimum for an ideal cipher operating on 8-bit pixel data is approximately 33.46%. Experiment 2 achieved a value of 34.72%, which is in close agreement with the ideal, indicating that the cipher introduces near-uniform intensity changes across the frame, a desirable property that implies strong resistance to statistical attacks. The UACI recorded in Experiment 1 (30.59%) falls somewhat below the ideal, suggesting that the distribution of intensity changes in that condition was less uniform, potentially due to differences in the input video's pixel intensity distribution or the encryption parameters employed. This discrepancy warrants further investigation to determine whether it is attributable to the source material characteristics or to systematic differences in the encryption process between experiments.

Shanon entropy analysis

Shannon entropy provides a measure of the randomness or unpredictability of an information source. For an ideal random source with 8-bit pixel depth, the maximum achievable entropy is 8.0 bits per pixel. Figure 3 shown the encrypted frame entropy values of 7.7433 (Experiment 1) and 7.7441 (Experiment 2) represent substantial gains over the original video entropy values of 7.3953 and 7.2383 was shown in Figure 4, respectively. The consistency of the encrypted entropy across both experiments (difference of less than 0.001 bits) indicates that the encryption process produces a highly stable and reproducible level of information randomness, irrespective of the source video characteristics. While the encrypted entropy values do not reach the theoretical maximum, the shortfall of approximately 0.26 bits is within a range commonly reported for practical cryptosystems and is unlikely to confer any exploitable statistical advantage to an adversary. The visual inspection of histogram distributions (Figures 3 and Figure 4) corroborates these findings, showing near-uniform pixel intensity distributions post-encryption.

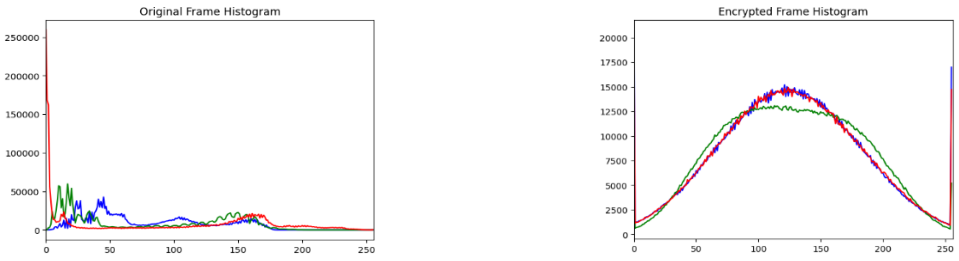

Figure 2. Pixel intensity histogram distributions for original (left) and encrypted (right) frames of tarot card video

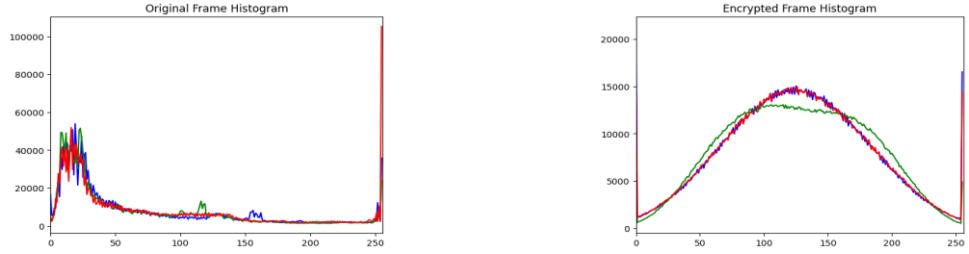

Figure 3. Pixel intensity histogram distributions for original (left) and encrypted (right) frames of crowded city video

Computational performance analysis

Per-frame processing times of 14,204 ms and 10,868 ms yield throughputs of 0.07 and 0.09 fps are far below real-time requirements. Dhingra and Dua [47] demonstrated that multi-threaded parallel confusion-diffusion can achieve 24 fps encryption at 768×768 resolution, highlighting the potential of parallelisation. Petrean et al. [48] similarly noted that computational efficiency must be balanced against security in practical

video cipher design. The ~30% reduction in per-frame latency in Experiment 2 relative to Experiment 1 may reflect lower frame complexity or differing resolution in the source material as shown in Figure 5 and Figure 6. These findings are characteristic of unoptimised research prototypes; hardware acceleration or algorithmic simplification would be required for real-time deployment.

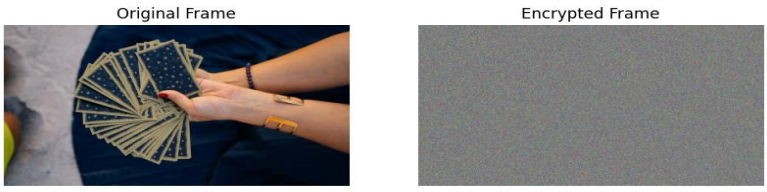

Figure 5. Difference between original video frame with the encrypted video frame (tarot card video)

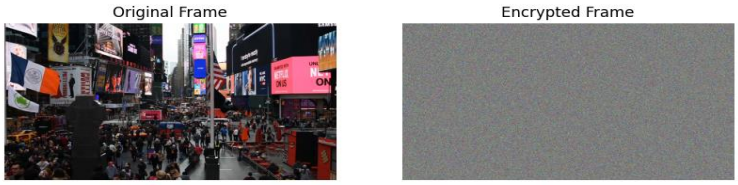

Figure 6. Difference between original video frame with the encrypted video frame (crowded city video)

Interpretation of Security Metrics

The NPCR values of 99.59% and 99.70% obtained in Experiments 1 and 2 exceed the critical threshold established by Zhang and Liu [49], confirming statistical resistance to differential attacks. This demonstrates a strong avalanche effect, a property originally formalized by Claude Shannon, whereby minor plaintext changes propagate unpredictably throughout the ciphertext. However, as noted by Alhakak, NPCR and UACI alone cannot guarantee robustness against chosen-plaintext or adaptive attacks, indicating the necessity of further cryptanalytic testing [50]. The UACI results (30.59% and 34.72%) show moderate deviation from the theoretical optimum of 33.46% for 8-bit images. While Experiment 2 slightly exceeds the ideal value, Experiment 1 falls below it, suggesting non-uniform intensity diffusion under certain input conditions. This indicates that the confusion–diffusion structure may not fully decorrelate specific pixel regions. Multi-round diffusion and inter-frame permutation strategies, similar to those proposed by Jiang et al., could improve consistency. Encrypted entropy values (~7.74 bits/pixel) demonstrate substantial improvement over the original sequences (7.24–7.40 bits/pixel). Although marginally below the 8-bit theoretical maximum described by Shannon, the stability of entropy across experiments suggests reliable ciphertext randomization independent of plaintext characteristics. This indicates strong statistical randomness, though minor non-uniformity remains compared to higher-dimensional chaotic models reported in recent literature.

Practical Implications and Optimisation Strategies

In its present form, the scheme is unsuitable for real-time applications such as live streaming or video conferencing, which typically require 24–30 fps. However, it remains suitable for offline or batch encryption scenarios where security outweighs latency, including archival protection, forensic video preservation, and post-capture medical data security. Performance improvements should prioritize parallelization. Multi-threaded CPU processing, as demonstrated by Báscones et al. [51], and GPU acceleration have shown substantial gains in chaotic encryption systems. Hardware-based acceleration using FPGA platforms, as explored by Guo and Wu [52], represents the most promising path toward real-time feasibility. Additionally, selective encryption strategies and lightweight chaotic maps may provide balanced security-performance trade-offs for constrained environments. Security evaluation should also be expanded to include key sensitivity analysis, key-space evaluation, correlation coefficient testing, and resistance to chosen-plaintext attacks, as recommended by Zhang and Liu [49] and Alhakak [50]. Broader validation across diverse benchmark video datasets would further establish robustness and generalizability.

Comparative Analysis and Performance Evaluation

When compared with recent chaos-based encryption schemes, the proposed method demonstrates competitive cryptographic strength alongside notable performance trade-offs. Table 5 summarizes the key metrics across comparable studies. The cryptographic results are encouraging: NPCR values of 99.59–99.70% align closely with established benchmarks, falling within the range of 99.6–99.8% reported across recent studies, indicating strong resistance to differential attacks. However, entropy values of approximately 7.74 bits/pixel are lower than the 7.99 bits/pixel achieved by Alkhonaini et al. [53] and Benrhouma et al. [55],

though competitive with Wang et al. [54]. This suggests marginally reduced uniformity in ciphertext distribution compared to leading implementations. The most significant limitation is computational performance. The software-only implementation achieved 0.07–0.09 fps, and notably, all comparable schemes in the literature provide no throughput data, indicating this metric remains largely unreported in current chaos-based video encryption research. This gap in performance reporting underscores the critical need to address implementation efficiency; the current prototype is single-threaded and unoptimised, factors that significantly impact throughput and represent the primary barrier to practical deployment.

Table 5. Comparative analysis of chaos-based video encryption schemes

Metric	Proposed	Alkhonaini et al. [53]	Wang et al. [54]	Benrhouma et al. [55]	Elkamchouchi et al. [56]
NPCR (%)	99.59 to 99.70	99.6	99.6	99.6	99.8
Entropy (bits/pixel)	7.74	7.99	6.37	7.91	N/A
Throughput (fps)	0.07–0.09	N/A	N/A	N/A	N/A
Implementation	Software (single-threaded)	Software	Software	Software	Software

4. CONCLUSION

This study demonstrates that the chaos-based video encryption scheme achieves strong cryptographic security with NPCR values of 99.59 to 99.70%, entropy of 7.74 bits/pixel, and UACI values approaching the theoretical optimum, validating its resistance to differential attacks and confirming the soundness of its underlying design. However, the scheme's practical utility remains constrained by software-only throughput of 0.07–0.09 fps, which falls below the 24–30 fps threshold for real-time applications. This performance limitation stems from implementation inefficiency rather than algorithmic weakness, suggesting that hardware acceleration and parallel processing could bridge the gap to real-time deployment. While the cryptographic strength is established, further analysis including key sensitivity testing, key-space evaluation, and chosen-plaintext attack resistance is required before the scheme can be considered fully validated for operational use.

ACKNOWLEDGEMENTS

This research funded by Universitas Dian Nuswantoro Grant Research No. 032/F.9/UDN-09/II/2026.

CREDIT AUTHORSHIP CONTRIBUTION STATEMENT

Cahaya Jatmoko: Conceptualization, Methodology, Writting – original draft & Validation. **Heru Lestiawan:** Conceptualization, Software, Writting – original draft & Project administration. **Fauzi Adi Rafrastara**: Software & Editing. **Lalang Erawan**: Writing – review & editing. **Candra Irawan**: Editing &Validation**. Mohamed Doheir**: Supervision.

DECLARATION OF COMPETING INTEREST

There are no conflict interest in this paper.

DATA AVAILABILITY

Data will be made available on request.

REFERENCES

[1] Y. S. Siregar, M. Khairani, H. Harahap, and Y. F. A. Lubis, "The Implementation Of Discrete Cosine Transform (DCT) And Blowfish Methods In Digital Video Security," *Sinkron*, vol. 7, no. 1, pp. 232–242, Feb. 2022, doi: 10.33395/sinkron.v7i1.11286.

[2] K. D. Sree, G. Gunti, A. K. Likith, and S. Palaniswamy, "Tampering Detection and Encryption: A Deep Learning Approach for Video Security," *2025 Int. Conf. Electron. Comput. Commun. Control Technol. ICECCC*, pp. 1–6, May 2025, doi: 10.1109/ICECCC65144.2025.11064151.

[3] V. R. Gatti, P. Shetty, B. Ravi Prakash, and H. Rama Moorthy, "Balancing Performance and Protection: A Study of Speed-Security Trade-offs in Video Security," *2024 Int. Conf. Recent Adv. Sci. Eng. Technol. ICRASET*, pp. 1–6, Nov. 2024, doi: 10.1109/ICRASET63057.2024.10895141.

[4] G. Tong, Z. Liang, F. Xiao, and N. Xiong, "A Residual Chaotic System for Image Security and Digital Video Watermarking," *IEEE Access*, vol. 9, pp. 121154–121166, 2021, doi: 10.1109/ACCESS.2021.3108196.

[5] Y. Qiu, J. Long, C. Ma, J. Luo, and Q. Xiao, "Security Protection of Video-GIS Data Based on Data Encryption and Digital Watermarking," *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, vol. XLVIII-4–2024, pp. 681–688, Oct. 2024, doi: 10.5194/isprs-archives-XLVIII-4-2024-681-2024.

[6] C. Kumar and S. Singh, "Security standards for real time video surveillance and moving object tracking challenges, limitations, and future: a case study," *Multimed. Tools Appl.*, vol. 83, no. 10, pp. 30113–30144, Sep. 2023, doi: 10.1007/s11042-023-16629-7.

[7] S. D. Achar, S. S. C, T. P, and S. Nandi, "Secure Video Streaming Techniques: A Performance Overview," *2023 IEEE Guwahati Subsect. Conf. GCON*, pp. 01–06, Jun. 2023, doi: 10.1109/GCON58516.2023.10183567.

[8] S. Q. Y. Al-Hashemi, M. S. Naghmash, and A. Ghandour, "Improving IP Video Surveillance Systems: The Shift to Digital Networks and Security Challenges," *SHIFRA*, vol. 2024, pp. 17–23, Mar. 2024, doi: 10.70470/SHIFRA/2024/003.

[9] S. Rampal, S. Umakanth, P. P. Gawali, S. Hemelatha, P. Aggarwal, and V. Mahalakshmi, "Digital Video Watermarking: Algorithmic Design and Performance Analysis," *2024 15th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT*, pp. 1–6, Jun. 2024, doi: 10.1109/ICCCNT61001.2024.10723872.

[10] A. Saini, S. Bhardwaj, R. Garg, and T. Kaur, "Systematic comparison of digital video watermarking aspects with techniques and algorithm designing issue," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 3, pp. 999–1010, 2024, doi: 10.47974/JDMSC-1646.

[11] K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, and A. Chattopadhyay, "Quantum Analysis of AES," *IACR Commun. Cryptol.*, vol. 2, no. 1, pp. cc2-1–36, Apr. 2025, doi: 10.62056/ay11zo-3y.

[12] Q. Deng, C. Wang, and H. Lin, "Chaotic dynamical system of Hopfield neural network influenced by neuron activation threshold and its image encryption," *Nonlinear Dyn.*, vol. 112, no. 8, pp. 6629–6646, Apr. 2024, doi: 10.1007/s11071-024-09384-3.

[13] L. Yang, X. Sun, B. Hamzi, H. Owhadi, and N. Xie, "Learning dynamical systems from data: A simple cross-validation perspective, Part V: Sparse Kernel Flows for 132 chaotic dynamical systems," *Phys. Nonlinear Phenom.*, vol. 460, p. 134070, Apr. 2024, doi: 10.1016/j.physd.2024.134070.

[14] S. Everett, "On the use of dynamical systems in cryptography," *Chaos Solitons Fractals*, vol. 183, p. 114952, Jun. 2024, doi: 10.1016/j.chaos.2024.114952.

[15] M. Lawnik and M. Berezowski, "New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography," *Symmetry*, vol. 14, no. 5, Apr. 2022, doi: 10.3390/sym14050895.

[16] T. Tan *et al.*, "Commutative encryption and watermarking algorithm based on compound chaotic systems and zero-watermarking for vector map," *Comput. Geosci.*, vol. 184, p. 105530, Feb. 2024, doi: 10.1016/j.cageo.2024.105530.

[17] T. Srour, A. M. El-Rifaie, M. A. M. El-Bendary, M. Eltokhy, A. E. Abouelazm, and B. Neji, "Multimedia privacy protection: an N-round cascaded cryptosystem based on merged multi-chaotic maps under various image attacks," *Front. Comput. Sci.*, vol. 7, May 2025, doi: 10.3389/fcomp.2025.1551166.

[18] "A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption," *Int. Arab J. Inf. Technol.*, vol. 18, no. 2, 2021, doi: 10.34028/iajit/18/2/12.

[19] P. S. Paul, M. Sadia, M. R. Hossain, B. Muldrey, and M. S. Hasan, "Cascading CMOS-Based Chaotic Maps for Improved Performance and Its Application in Efficient RNG Design," *IEEE Access*, vol. 10, pp. 33758–33770, 2022, doi: 10.1109/ACCESS.2022.3162806.

[20] T. Wang, B. Ge, C. Xia, and G. Dai, "Multi-Image Encryption Algorithm Based on Cascaded Modulation Chaotic System and Block-Scrambling-Diffusion," *Entropy*, vol. 24, no. 8, Jul. 2022, doi: 10.3390/e24081053.

[21] J. Zheng and T. Bao, "An image encryption algorithm based on cascade chaotic map and DNA coding," *IET Image Process.*, vol. 17, no. 12, pp. 3510–3523, 2023, doi: 10.1049/ipr2.12882.

[22] J. Zheng and T. Bao, "An Image Encryption Algorithm Using Cascade Chaotic Map and S-Box," *Entropy*, vol. 24, no. 12, Dec. 2022, doi: 10.3390/e24121827.

[23] R. Chen, X. Li, L. Teng, and X. Wang, "Selective region medical image encryption algorithm based on cascade chaos and two-dimensional Joseph traversal," *Phys. Scr.*, vol. 98, no. 3, p. 035227, Feb. 2023, doi: 10.1088/1402-4896/acbcf8.

[24] D. S. Laiphrakpam, R. Thingbaijam, K. M. Singh, and M. Al Awida, "Encrypting Multiple Images With an Enhanced Chaotic Map," *IEEE Access*, vol. 10, pp. 87844–87859, 2022, doi: 10.1109/ACCESS.2022.3199738.

[25] M. Kumar and Deepak. Ch, "Enhancing image security through a fusion of chaotic map and multi-level scrambling techniques," *Signal Image Video Process.*, vol. 19, no. 3, p. 235, Jan. 2025, doi: 10.1007/s11760-025-03814-4.

[26] M. N. E. Farandi, A. Marjuni, N. Rijati, and D. R. I. M. Setiadi, "Enhancing image encryption security through integration multi-chaotic systems and mixed pixel-bit level," *Imaging Sci. J.*, vol. 73, no. 3, pp. 363–380, Apr. 2025, doi: 10.1080/13682199.2024.2398954.

[27] Y. Li, X. You, J. Lu, and J. Lou, "A joint image compression and encryption scheme based on a novel coupled map lattice system and DNA operations," *Front. Inf. Technol. Electron. Eng.*, vol. 24, no. 6, pp. 813–827, Jun. 2023, doi: 10.1631/FITEE.2200645.

[28] J. Li *et al.*, "SED-UAV: A Synergistic Framework of Lightweight Chaotic Encryption and Multi-Scale Feature Detection for Secure UAV Applications," *IEEE Internet Things J.*, pp. 1–1, 2025, doi: 10.1109/JIOT.2025.3607318.

[29] S. B. Almobydeen, Y. Alemami, K. G. Al-Moghrabi, and A. M. Al-Ghonmein, "An Efficient and Secure Medical Image Encryption Approach for Cloud Settings Utilizing a Hybrid Multi-Chaotic System Coupled with Bogdanov Permutation," Nov. 28, 2025, *Social Science Research Network, Rochester, NY*: 5823848. doi: 10.2139/ssrn.5823848.

[30] X. Yang, L. Bao, D. Zhou, and Y. Si, "Construction and Attractor Analysis of Discrete Chaotic Systems Based on Julia Fractal Transformation," *Int. J. Bifurc. Chaos*, vol. 35, no. 02, p. 2550016, Feb. 2025, doi: 10.1142/S0218127425500166.

[31] M. Alfonso-Arsuaga, J. García-González, A. Castiella-Aguirrezabala, M. A. Alonso, and E. Garcés, "DyNeRFactor: Temporally consistent intrinsic scene decomposition for dynamic NeRFs," *Comput. Graph.*, vol. 122, p. 103984, Aug. 2024, doi: 10.1016/j.cag.2024.103984.

[32] D. Duc Trong, N. Dang Minh, L. Xuan Thang, and L. Dang Khoa, "Regularization of inverse problems by filtered diagonal frame decomposition under general source," *Inverse Probl.*, vol. 41, no. 11, p. 115007, Nov. 2025, doi: 10.1088/1361-6420/ae1998.

[33] V. Ye, Z. Li, R. Tucker, A. Kanazawa, and N. Snavely, "Deformable Sprites for Unsupervised Video Decomposition," presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 2657–2666. Accessed: Feb. 18, 2026. [Online]. Available: https://openaccess.thecvf.com/content/CVPR2022/html/Ye_Deformable_Sprites_for_Unsupervised_Video_Decomposition_CVPR_2022_paper.html
[34] X. Zhang, J. Di, and Y. Niu, "Image encryption scheme based on double permutation and DNA," *Multimed. Tools Appl.*, vol. 83, no. 19, pp. 57291–57316, Jun. 2024, doi: 10.1007/s11042-023-17392-5.
[35] G. L. Jones and Q. Qin, "Markov Chain Monte Carlo in Practice," *Annu. Rev. Stat. Its Appl.*, vol. 9, no. Volume 9, 2022, pp. 557–578, Mar. 2022, doi: 10.1146/annurev-statistics-040220-090158.
[36] S. Kheradmand *et al.*, "3D Gaussian Splatting as Markov Chain Monte Carlo," *Adv. Neural Inf. Process. Syst.*, vol. 37, pp. 80965–80986, Dec. 2024, doi: 10.52202/079017-2573.
[37] "Quantum-enhanced Markov chain Monte Carlo | Nature." Accessed: Feb. 18, 2026. [Online]. Available: https://www.nature.com/articles/s41586-023-06095-4
[38] F. S. Al-Duais and R. S. Al-Sharpi, "A unique Markov chain Monte Carlo method for forecasting wind power utilizing time series model," *Alex. Eng. J.*, vol. 74, pp. 51–63, Jul. 2023, doi: 10.1016/j.aej.2023.05.019.
[39] X. Gao, J. Mou, B. Li, S. Banerjee, and B. Sun, "Multi-image hybrid encryption algorithm based on pixel substitution and gene theory," *Fractals*, vol. 31, no. 06, p. 2340111, Jan. 2023, doi: 10.1142/S0218348X23401114.
[40] E. Levin and O. Fried, "Differential Diffusion: Giving Each Pixel Its Strength," *Comput. Graph. Forum*, vol. 44, no. 2, p. e70040, 2025, doi: 10.1111/cgf.70040.
[41] W. Wu, Y. Zhao, M. Z. Shou, H. Zhou, and C. Shen, "DiffuMask: Synthesizing Images with Pixel-level Annotations for Semantic Segmentation Using Diffusion Models," presented at the Proceedings of the IEEE/CVF International Conference on Computer Vision, 2023, pp. 1206–1217. Accessed: Feb. 18, 2026. [Online]. Available: https://openaccess.thecvf.com/content/ICCV2023/html/Wu_DiffuMask_Synthesizing_Images_with_Pixel-level_Annotations_for_Semantic_Segmentation_Using_ICCV_2023_paper.html
[42] M. Khan, F. Aljuaydi, L. Said, and M. Amin, "A secure chaotic cryptosystem for thermal Imaging: Logistic map-based encryption with substitution-diffusion and spatial decorrelation," *J. Radiat. Res. Appl. Sci.*, vol. 18, no. 2, p. 101546, Jun. 2025, doi: 10.1016/j.jrras.2025.101546.
[43] L. Wu, L. Wang, Z. Deng, Y. Zhu, and H. Wei, "Replace2Self: Self-Supervised Denoising Based on Voxel Replacing and Image Mixing for Diffusion MRI," *IEEE Trans. Med. Imaging*, vol. 44, no. 7, pp. 2878–2891, Jul. 2025, doi: 10.1109/TMI.2025.3552611.
[44] F. Wan, B. Xu, W. Pan, and H. Liu, "PSC diffusion: patch-based simplified conditional diffusion model for low-light image enhancement," *Multimed. Syst.*, vol. 30, no. 4, p. 187, Jun. 2024, doi: 10.1007/s00530-024-01391-z.
[45] M. R. Naufal, C. A. Sari, E. H. Rachmawanto, L. B. Handoko, F. O. Isinkaye, and W. S. T. Al-Dayyeni, "An Evaluation of Number of Pixels Change Rate (NPCR) in Symetric Cryptography Based on Data Encryption Standard (DES)," *2023 Int. Semin. Appl. Technol. Inf. Commun. ISemantic*, pp. 490–495, Sep. 2023, doi: 10.1109/iSemantic59612.2023.10295300.
[46] L. N. Hidayati, G. F. Fitriana, and I. F. Adam, "Perbandingan Keacakan Citra Enkripsi Algoritma AES dan Camelia Uji NPCR dan UACI," *JURIKOM J. Ris. Komput.*, vol. 8, no. 6, p. 274, Dec. 2021, doi: 10.30865/jurikom.v8i6.3624.
[47] D. Dhingra and M. Dua, "Novel multiple video encryption scheme using two-chaotic-map-based two-level permutation and diffusion," *Nonlinear Dyn.*, vol. 113, no. 10, pp. 12309–12335, May 2025, doi: 10.1007/s11071-024-10820-7.
[48] D.-E. Petrean, R. Potolea, and C. Oprisa, "Packed Code Detection using Shannon Entropy and Homomorphic Encrypted Executables," in *2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)*, Oct. 2024, pp. 01–08. doi: 10.1109/ICCP63557.2024.10793050.
[49] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, Jun. 2023, doi: 10.3390/math11112585.
[50] Z. Alhakak, "Medical Image Encryption Techniques: A Review," *Misan J. Eng. Sci.*, vol. 4, no. 1, pp. 86–105, Jun. 2025, doi: 10.61263/mjes.v4i1.133.
[51] D. Báscones, C. Gonzalez, and D. Mozos, "A Real-Time FPGA Implementation of the CCSDS 123.0-B-2 Standard," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, pp. 1–13, 2022, doi: 10.1109/TGRS.2022.3160646.
[52] L. Guo and S. Wu, "FPGA Implementation of a Real-Time Edge Detection System Based on an Improved Canny Algorithm," *Appl. Sci.*, vol. 13, no. 2, Jan. 2023, doi: 10.3390/app13020870.
[53] M. A. Alkhonaini, E. Gemeay, F. M. Zeki Mahmood, M. Ayari, F. A. Alenizi, and S. Lee, "A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata," *Sci. Rep.*, vol. 14, no. 1, p. 16701, Jul. 2024, doi: 10.1038/s41598-024-64741-x.
[54] T. Wang, B. Ge, C. Xia, and G. Dai, "Multi-Image Encryption Algorithm Based on Cascaded Modulation Chaotic System and Block-Scrambling-Diffusion," *Entropy*, vol. 24, no. 8, p. 1053, Jul. 2022, doi: 10.3390/e24081053.
[55] O. Benrhouma, A. B. Alkhodre, A. AlZahrani, A. Namoun, and W. A. Bhat, "Using Singular Value Decomposition and Chaotic Maps for Selective Encryption of Video Feeds in Smart Traffic Management," *Appl. Sci.*, vol. 12, no. 8, p. 3917, Jan. 2022, doi: 10.3390/app12083917.
[56] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," *IET Image Process.*, vol. 14, no. 2, pp. 397–406, Feb. 2020, doi: 10.1049/iet-ipr.2018.5250.

.