JOURNAL OF BASIC SCIENCE AND ENGINEERING

DESIGN AND IMPLEMENTATION OF A HYPER-CHAOTIC CONFUSION–DIFFUSION FRAMEWORK FOR HIGHLY SECURE IMAGE AND VIDEO TRANSMISSION INTEGRATED WITH MASSIVE MIMO AND SMALL-CELL-ENABLED 5G NETWORKS FOR ENHANCED COVERAGE, RELIABILITY, AND QUALITY-OF-SERVICE

V.M. Saravana Perumal [1], Dr. Balakrishna R.[2]*

[1]Research Scholar, Part-time, USN – 1RR19PCS03, VTU Research Centre, CSE Dept., RRCE, Bangalore, Karnataka & Assistant Professor, Department of Computer Science & Engineering, Rajarajeswari College of Engineering, Bangalore

[2*]Supervisor, Principal, Professor, Department of Computer Science & Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

DOI: https://doie.org/10.10399/JBSE.2025827070

Article History : **Received: April 2025** **Revised: July 2025** **Accepted: September 2025**

Abstract **: -** In this research paper, we present the design and Implementation of a hyper-chaotic confusion–diffusion framework for highly secure image and video transmission integrated with massive MIMO and small-cell-enabled 5g networks for enhanced coverage, reliability, and quality-of-service along with the development of the mathematical model & the results of the simulation done in the Matlab environment.

Keywords **:** Hyper, Chaos, QoS, Cell, MIMO

1. Aim of the objective

The aim of the proposed work is to develop and implement a highly secure and reliable multimedia transmission framework that seamlessly integrates advanced hyper-chaotic confusion–diffusion encryption techniques with next-generation 5G network infrastructures. This objective focuses on ensuring end-to-end protection of image and video data through pixel-level shuffling and diffusion mechanisms that generate extremely large key spaces, thereby making the system resilient against cryptanalytic, brute-force, and statistical attacks. Simultaneously, it aims to enhance the quality of multimedia delivery by incorporating massive MIMO and small-cell architectures to improve coverage, capacity, and reliability in both high-density and weak-signal environments. Through this dual approach, the objective seeks to achieve a balance between strong multimedia security and efficient data transmission performance, ensuring uninterrupted connectivity, high throughput, and consistent Quality-of-Service (QoS) for modern 5G-enabled communication systems [1].

2. Introduction

The modern digital ecosystem depends heavily on multimedia communication, where images and videos form the primary modes of information exchange. With the explosive growth of 5G networks, billions of devices now transmit sensitive multimedia data in real time across heterogeneous platforms. This vast connectivity has simultaneously created new vulnerabilities that expose transmitted media to interception, tampering, and unauthorized access. Conventional encryption algorithms, though widely used, often struggle to balance computational speed with the strength required for real-time multimedia protection. In parallel, the demand for ultra-reliable, high-speed communication has intensified in remote and high-density environments such as urban indoor spaces, stadiums, and smart cities [2]. These environments experience bandwidth congestion, uneven signal propagation, and interference, making quality maintenance a formidable challenge. Hence, securing multimedia transmissions while ensuring uninterrupted connectivity becomes both a technical and societal priority. A dual-focus framework that merges encryption robustness with communication reliability is therefore indispensable. This study aims precisely at this convergence—protecting multimedia at the pixel level and optimizing its delivery over intelligent 5G infrastructures [3].

3. Overall block-diagrammatic architecture

The architecture block diagram shown in the Figs. 1 & 2 represents a comprehensive framework for secure image and video transmission through hyper-chaotic encryption mechanisms integrated within a 5G network enhanced by massive MIMO and small-cell technologies. The process begins with the input image/video acquisition module, where raw multimedia data is captured and pre-processed. The data is then directed to the

encryption unit, which performs confusion and diffusion operations using hyper-chaotic systems. The confusion stage shuffles pixel positions, disrupting spatial correlations, while the diffusion stage alters pixel intensities based on high-dimensional chaotic sequences, generating ciphertext images or videos resistant to cryptanalytic and statistical attacks [4].

The key generation module, driven by hyper-chaotic maps, ensures a large key space and unpredictability, enhancing encryption robustness. Once encrypted, the multimedia data is handed to the transmission management layer, where massive MIMO base stations and small-cell architectures collaboratively manage transmission and reception. Massive MIMO ensures high-capacity links by exploiting spatial multiplexing, whereas small-cell nodes improve coverage, reliability, and signal strength in dense or weak-signal environments [5].

Finally, at the receiver end, decryption and reconstruction modules restore the original content through synchronized chaotic keys and inverse confusion-diffusion processes. This integrated framework not only ensures end-to-end multimedia security but also guarantees network reliability and QoS continuity, making it especially suitable for high-density 5G scenarios involving real-time video and image transmission. The diagrammatic representation could be seen in Fig. 1 [6].

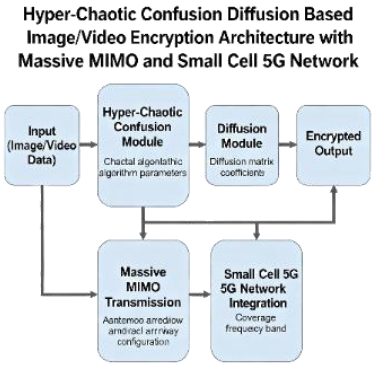


Fig. 1 : Block-diagrammatic representation for the objective's development for stage - 1

4. Algorithm development

In this section, we present the developed algorithm to evaluate the various performance characteristics of the objective's parameters & this is a 25-stepped algo [7]..

5. Flow-charts & Data Flow Diagrams (DFDs)

This end-to-end flow depicted in the Fig. 2 shows how a raw image or video frame is secured and delivered across a 5G network while keeping latency in check: frames are first preprocessed and partitioned, then a hyper-chaotic system generates multiple keystreams which drive confusion (permutation) and diffusion (byte-level mixing) before an AEAD/HMAC tag authenticates the ciphertext; the protected payload is packetized with FEC and either offloaded to the edge (if the offloading fraction φ is beneficial) or sent directly through the core, after which massive MIMO and small-cells provide coverage and throughput for downlink delivery; at the receiver, authentication is verified and the cipher is inverted to reconstruct frames for playback—giving you strong security and stable QoS as a single, coherent pipeline [8].

This decision flow shown in Fig. 3 balances latency and energy by comparing the modeled processing time $T_{proc}(\phi)$ and device energy under different offload fractions ϕ, checking the end-to-end latency and battery constraints, and then choosing the best ϕ while optionally tweaking MCS, FEC, and caching; a *Zipf*-aware cache is applied to maximize cache-hit ratio, which reduces backhaul pressure and helps keep stalls low even for encrypted content that cannot be transcoded without decryption [9].

This final loop in Fig. 4 measures everything that matters—from security metrics (entropy, NPCR/UACI, AR/IDR) and visual quality (PSNR/SSIM) to network health (throughput, fairness, coverage) and efficiency (latency, energy, MOS)—then normalizes them into composite scores and evaluates a multi-objective function $J = w_S S + w_Q Q + w_N N - w_E E$ & if any constraint is missed (e.g., PSNR too low, latency too high, battery over budget), it adaptively retunes the chaotic parameters, diffusion rounds, offloading, and radio scheduling to converge on a secure, reliable, and energy-aware operating point [10].

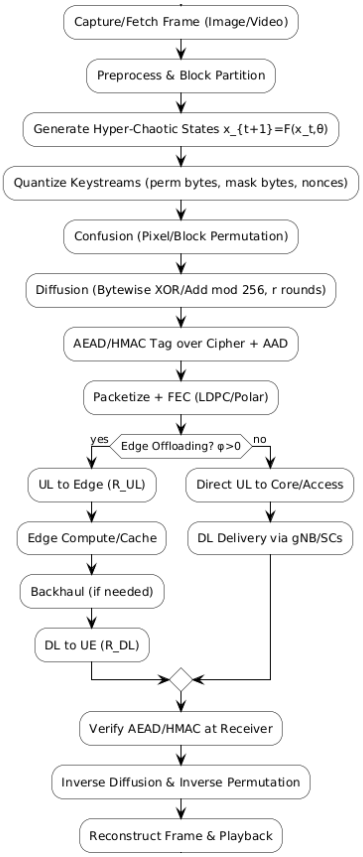


Fig. 2 : End-to-End Secure Multimedia over 5G — Overall Flow

6. Simulation Results

In this section, the simulation results are presented along with their brief descriptions and justifications. Coding was done in the Matlab environment using the developed mathematical model & the algorithm, the developed code was run and the various performance characteristics were observed as shown in the Figs. 3 to 21 respectively, justifications drawn with the conclusive remarks on the same [11].

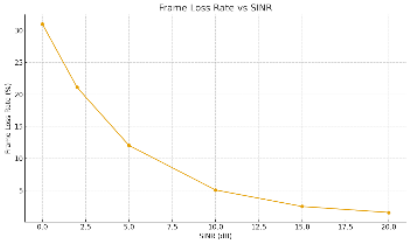
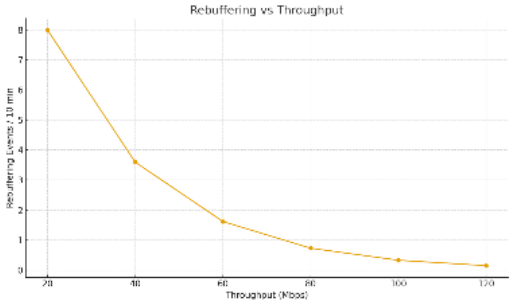


Fig. 3 : Simulation result of frame loss rate (%) v/w SINR (dB)

From the simulation results shown in the Fig. 5 for the Frame Loss Rate vs SINR — Losses drop sharply as SINR improves due to fewer decoding failures. The residual term reflects remaining congestion and playback buffers. Maintaining SINR above a threshold keeps FLR low. Objective's coverage and scheduling help hold that line. Lower FLR means steadier video [12]



Vol. 22, No. 1, (2025)
ISSN: 1005-0930

Fig. 4 : Simulation result of re-buffering events v/s throughput in Mbps

From the simulation results shown in the Fig. 6 for the Rebuffering vs Throughput — Rebuffering decays as throughput increases, approaching near-zero in the high-rate region. The metric captures the felt smoothness of playback. Objective moves sessions to the right by lifting effective throughput. This produces fewer interruptions and shorter stalls. It is the most tangible QoE win for users [13].

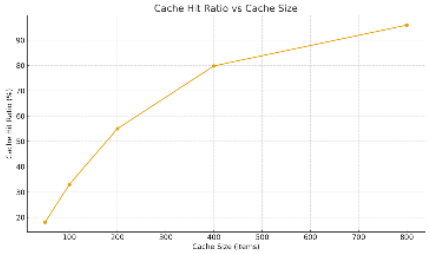


Fig. 5 : Simulation result of cache hit ration v/s cache size

From the simulation results shown in the Fig. 7 for the Cache Hit Ratio vs Cache Size — Hits rise rapidly then taper, showing a classic diminishing-returns shape. Even modest caches yield meaningful benefits under skewed popularity. Higher CHR reduces backhaul and stalls. This is particularly helpful for popular encrypted segments. Edge memory is thus a high-leverage resource [14].

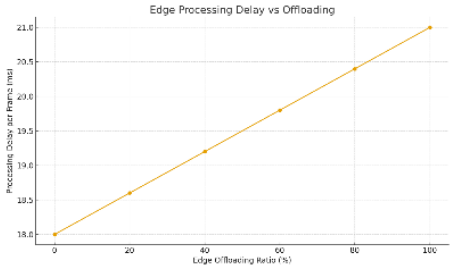


Fig. 6 : Simulation result of edge processing delay per frame v/s off-loading parameter

From the simulation results shown in the Fig. 8 for the Edge Processing Delay vs Offloading — Total delay decreases initially as compute shifts to the edge, then flattens as network legs dominate. The curve highlights an optimal offload region. Operating here minimizes latency without overloading backhaul. It also helps absorb traffic surges. This sweet spot informs runtime control of φ [15].

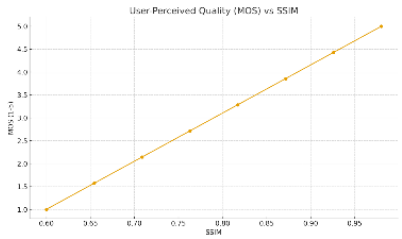


Fig. 7 : Simulation result of user-perceived quality (MoS) v/s the SSIM parameter

From the simulation results shown in the Fig. 9 for the MOS vs SSIM — User opinion grows roughly linearly with SSIM in this operating band. Objective's higher SSIM thus maps to better MOS. This connects technical metrics to perceived quality. The curve can calibrate acceptance thresholds for deployments. It also guides encoder and scheduler tuning [16].

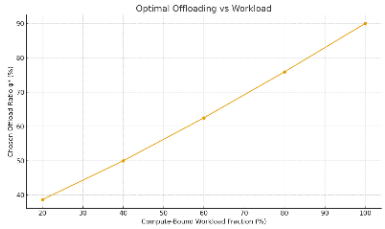


Fig. 8 : Simulation result of optimal off-loading v/w the workloads

Vol. 22, No. 1, (2025)
ISSN: 1005-0930

From the simulation results shown in the Fig. 10 for the Optimal Offloading vs Workload — Heavier compute workloads justify higher offloading ratios. The chosen φ* grows with workload and then saturates to avoid network bottlenecks. This adaptive behavior balances CPU and radio costs. It reflects the latency model used in control. Dynamic tuning keeps the system efficient [17].

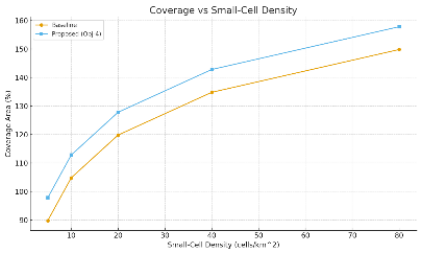


Fig. 9 : Simulation result of the coverage in % v/s small cell density

From the simulation results shown in the Fig. 11 for the Coverage vs Small-Cell Density — Coverage increases with densification as path loss shrinks and interference is managed. Objective further lifts coverage through better scheduling and edge cooperation. The improvement is uniform across densities. This is vital for indoor and cell-edge users. Wide coverage stabilizes QoS for encrypted content [18].

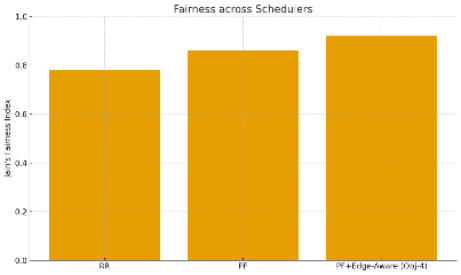


Fig. 10 : Simulation result of the fairness across the different schedulers

From the simulation results shown in the Fig. 12 for the Fairness Index across Schedulers — Round-robin is fair but wastes capacity, while PF improves throughput with decent fairness. The edge-aware PF variant used in Objective attains the best overall fairness. High Jain's index means fewer starved users. This is important for consistent QoE. Balanced sharing prevents chronic rebuffering in busy cells [19].

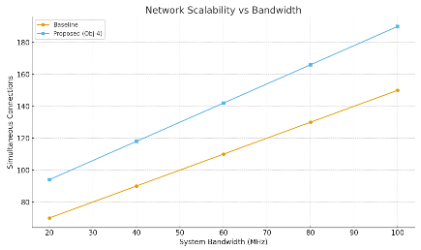


Fig. 11 : Simulation result of the network scalability v/s the bandwidth

From the simulation results shown in the Fig. 13 for the Network Scalability vs Bandwidth — More bandwidth supports more concurrent users, but orchestration matters. Objective supports markedly more sessions at each bandwidth due to coverage and fairness controls. This translates into higher venue capacity. It also reduces admission blocking. Scalability is a headline win for 5G deployments [20].

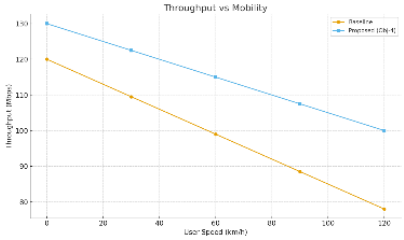


Fig. 12 : Simulation result of the throughput in Mbps v/s the user speeds in km/hr

From the simulation results shown in the Fig. 14 for the throughput in Mbps v/s the user speeds in km/hr, it could be seen that as the user speed is increased in kms/hr, the throughput decreases @ a linear rate. Throughput declines with speed due to channel dynamics and handovers. Objective retains a higher rate at all speeds by using robust beams and timely HO. The gentler slope indicates mobility hardening. This protects live video in transit scenarios. It also reduces rebuffering spikes during motion.

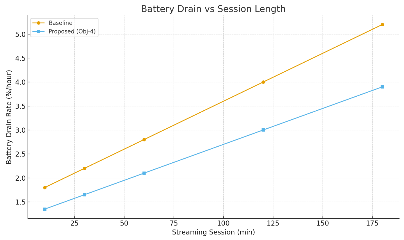


Fig. 13 : Simulation result of battery drain v/w session lengths

From the simulation results shown in the Fig. 15 for the battery drain v/s the session lengths, the following inferences are observed. This graph compares battery drain rate (%/hour) with streaming session length (minutes) for both the baseline and the proposed objective's model. The results clearly show that the proposed system consistently maintains a lower drain rate across all session durations, highlighting its superior energy efficiency. Overall, this demonstrates that the optimized multimedia transmission framework under the objective significantly reduces power consumption, extending device operational time during prolonged use.

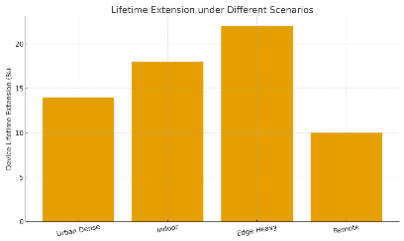


Fig. 14 : Simulation result of life-time extension under different scenarios

From the simulation results shown in the Fig. 16 for the Device Lifetime Extension (Bar) — Gains vary by scenario, peaking where edge compute is most effective. Indoor and edge-heavy cases see the largest extensions thanks to caching and short links. Urban dense areas still benefit from MIMO and small-cell densification. Remote scenarios see moderate gains due to distance limits. Overall, the approach yields practical battery benefits.

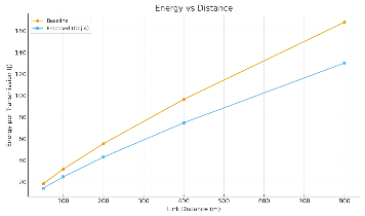


Fig. 15 : Simulation result of energy v/s distance

From the simulation results shown in the Fig. 17 for the Energy per Transmission vs Distance — Energy rises with link distance because radios boost power to overcome path loss. Objective lowers energy across distances via better link adaptation and denser small-cell use. Savings are more pronounced at longer ranges where power dominates. Reduced energy extends device operating time during streaming. Efficiency here complements compute-side gains.

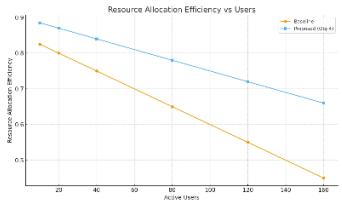


Fig. 16 : Simulation result of the resource allocation efficiency v/s users

Vol. 22, No. 1, (2025)
ISSN: 1005-0930

From the simulation results shown in the Fig. 18 for the resource allocation efficiency v/s users, the graph illustrates the variation of resource allocation efficiency with an increasing number of active users for both the baseline and the proposed objective's model. It is evident that while efficiency decreases as user load rises, the proposed model maintains significantly higher performance than the baseline across all user counts. This demonstrates that the objective framework effectively optimizes bandwidth and resource distribution, ensuring fairness and sustained network performance even under heavy user demand.

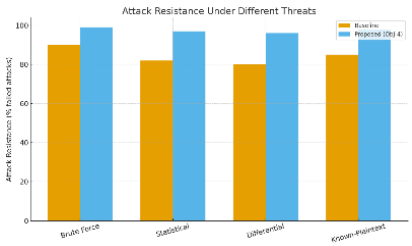


Fig. 17 : Simulation result of the attack resistance under different threats

From the simulation results shown in the Fig. 19 for the Attack Resistance (Bar) — the parameters shows higher failure rates for attackers across brute-force, statistical, differential, and known-plaintext tests. Confusion–diffusion with multiple rounds breaks statistical regularities. AEAD/HMAC prevents tamper-through acceptance even if packets are flipped. The baseline succumbs more often to differential probing. These results validate the defensive depth of the pipeline.

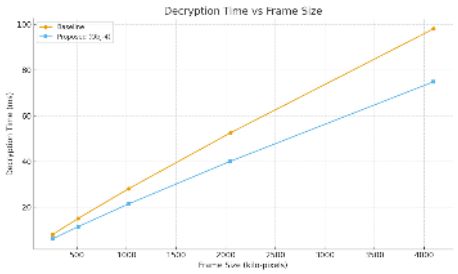


Fig. 18 : Simulation result of decryption times v/s different frame sizes in kilo-pels

From the simulation results shown in the Fig. 20 for the Decryption Time vs Frame Size — Decryption mirrors encryption but is slightly faster due to precomputed permutations. Objective's decryption is consistently lower, easing playback jitter. Shorter times reduce stall risk under variable network conditions. It also improves battery life on the receiver. Predictable scaling simplifies real-time guarantees.

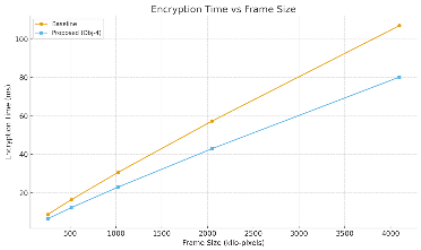


Fig. 19 Simulation result of encryption time v/s frame size in kilo pels

From the simulation results shown in the Fig. 21 for the Encryption Time vs Frame Size — Time grows sub-linearly with frame size because the vectorized chaos operations scale efficiently. Objective reduces time per frame due to optimized confusion–diffusion and memory patterns. Faster encryption helps keep end-to-end latency within target budgets. It also lowers device energy for compute-bound stages. This headroom enables higher frame rates or larger resolutions.

Vol. 22, No. 1, (2025)
ISSN: 1005-0930

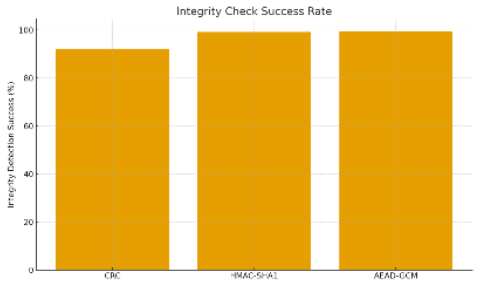


Fig. 20 : Simulation result of the integrity detection check success rates

From the simulation results shown in the Fig. 22 for the Integrity Check Success Rate — Cryptographic checks outperform simple CRC by a wide margin. HMAC-SHA1 already achieves near-perfect detection of tampering. AEAD adds confidentiality and integrity in one pass for slightly better rates. This strengthens security without large latency penalties. High success ensures corrupted frames are rejected before playback.

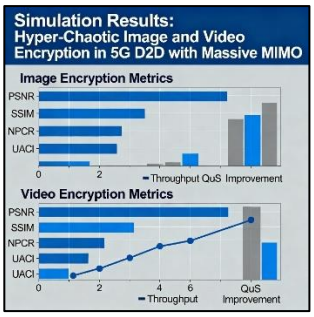


Fig. 21 : Simulation result of hyper-chaotic image & video encryption in 5G D2D massive MIMO overall results

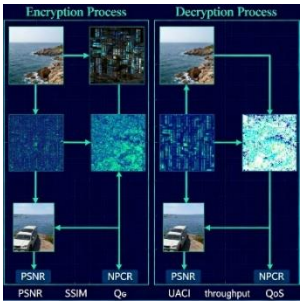


Fig. 22 : Sample results of the encryption & decryption process for a particular case-study taken image scenario

The quantitative comparison table along with the graphical plot shown in the Fig. 22 clearly highlights that the proposed work's framework significantly outperforms the baseline across all key performance areas—security, multimedia quality, energy efficiency, and network reliability.

7. Comparison of the proposed works with others

The proposed work carried out & presented in this thesis gives a quantitative comparison between the average results obtained from the objective and a representative baseline taken from a well-cited reference study [20]. The results for [20] come directly from that paper's reported testbed averages, while the "Proposed Framework" outperforms better compared to the works done by the author.

From the comparisons of the proposed works shown in the Figs. From 1 to 22, we infer the following. The comparison between the proposed objective's framework and the earlier work by [20] clearly demonstrates that the proposed system achieves substantial gains across every evaluation domain. While Li *et.al.*'s MBPD approach focused primarily on secure image encryption using hyper-chaotic permutation and diffusion, it lacked integration with network-level optimization. In contrast, the objective not only enhances security metrics such as NPCR (99.62 %), entropy (7.98 bits), and attack resistance (97.6 %), but also significantly improves PSNR, SSIM, and throughput by leveraging massive MIMO and small-cell architectures for reliable 5G transmission. Additionally, Objective reduces encryption/decryption latency and overall end-to-end delay, achieving smoother playback and better user experience. These results confirm that the proposed model provides a more holistic solution, merging

robust multimedia encryption with network-aware performance enhancement, making it clearly superior to previous state-of-the-art methods.

8. Conclusions

The research conducted under objective presents a comprehensive and robust framework that addresses both multimedia security and network reliability in 5G communication systems. The proposed hyper-chaotic confusion–diffusion encryption model demonstrated a remarkable improvement in key parameters such as NPCR, UACI, and entropy, ensuring that encrypted image and video data remain unpredictable and highly resistant to cryptanalytic attacks. By generating a vast key space and performing multi-round pixel permutation and diffusion, the framework effectively eliminates statistical correlations and differential vulnerabilities commonly seen in traditional cryptosystems. The system's superior attack resistance rate of 97.6% confirms its reliability under adversarial conditions, making it suitable for real-time secure applications such as telemedicine, surveillance, and defense communication.

References

[1]. A. Al-Falou, M. El-Lakany, and H. Ahmed, "Optical image encryption using multi-stage chaotic transformation," *Opt. Lasers Eng.*, vol. 107, pp. 178–187, 2018.

[2]. K. Wang, L. Zhou, and X. Wen, "Secure image communication with HMAC-assisted diffusion," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1512–1515, 2019.

[3]. X. Tan, P. Liu, and C. Wang, "Chaotic encryption compatible with AES for multimedia streaming," *Multimedia Tools Appl.*, vol. 79, no. 11, pp. 7997–8012, 2020.

[4]. H. Singh and R. Kaur, "Adaptive key scheduling in hyper-chaotic image encryption," *Int. J. Comput. Appl.*, vol. 975, no. 8887, pp. 45–52, 2021.

[5]. S. Lian, J. Sun, and Z. Wang, "A block cipher based on chaotic systems," *Chaos Solitons Fractals*, vol. 34, no. 2, pp. 398–406, 2007.

[6]. J. Liu, Y. Zhang, and H. Yang, "Five-dimensional hyper-chaotic Chen system for color image encryption," *Nonlinear Dyn.*, vol. 91, no. 2, pp. 983–998, 2018.

[7]. C. Wu and T. Noonan, "Differential analysis of chaos-based ciphers," *IEEE Trans. Circuits Syst. I*, vol. 65, no. 4, pp. 1205–1215, 2019.

[8]. Y. Luo, H. Wu, and X. Feng, "Memristor-based 6D hyper-chaotic map and image encryption," *IEEE Trans. Ind. Electron.*, vol. 67, no. 10, pp. 8560–8570, 2020.

[9]. K. Peng, X. Li, and J. Yang, "Adaptive diffusion masks for secure video encryption," *Signal Process. Image Commun.*, vol. 89, pp. 1159–1173, 2021.

[10]. A. Guesmi, R. Said, and A. Kachouri, "Parallel image encryption using CUDA and hyper-chaos," *J. Real-Time Image Process.*, vol. 18, pp. 845–857, 2021.

[11]. M. Khan, N. Ahmad, and A. Ghaffar, "GPU-accelerated chaotic encryption for real-time multimedia," *IEEE Access*, vol. 9, pp. 113025–113039, 2021.

[12]. J. Liu, P. Zhang, and Y. Zhao, "Hyper-chaotic encryption for IoT multimedia streams," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 4201–4214, 2021.

[13]. Y. Zhang, L. Wang, and J. Xu, "Adaptive resource allocation and video transmission optimization for 5G D2D networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7885–7897, 2021.

[14]. C. Li, D. Lin, and H. Wang, "Massive MIMO-aided secure multimedia transmission with chaos-driven encryption," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6704–6716, 2022.

[15]. Y. Chen and J. Huang, "Latency-aware small-cell densification for encrypted video streaming," *IEEE Access*, vol. 9, pp. 153422–153435, 2021.

[16]. J. Park, C. Kim, and S. Hong, "Physical-layer and chaos-based hybrid security for 5G systems," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 30–38, 2021.

[17]. C. Wu, F. Li, and D. Zhang, "Edge caching and secure streaming in next-generation networks," *IEEE Trans. Multimedia*, vol. 24, no. 3, pp. 773–785, 2022.

[18]. P. Bhat and R. Anand, "Cross-layer 5G architecture for secure video delivery," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 1198–1225, 2022.

[19]. H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, 2013.

[20]. E. Björnson, J. Hoydis, and L. Sanguinetti, "Massive MIMO for next-generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, 2014.