International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 5 May. 2026, pp: 662-666 www.ijaem.net ISSN: 2395-5252

Performance Optimization of Video Encryption Using Parallel Processing and Multi-threading

[1]Baydaa Jaffer Al-Khafaji*, , [2]Maha talib Abdullah, [3]Zainab Hazim Ibrahim,[4]Amna al-saffar , [5] Iptehaj Alhakam, [6]Nadia Mohammed Abdulmaged
[1, 3,4,5, 6]*Computer Science Department College of Pure Science/ Ibn Al-Haytham University of Baghdad, Iraq*

Date of Submission: 11-05-2026 Date of Acceptance: 20-05-2026

Abstract
The rapid growth of virtual meetings and real-time video conferencing has increased the demand for secure and high-performance video encryption techniques. Conventional encryption methods provide strong security guarantees but often suffer from high computational cost and latency, which limits their applicability in real-time environments. This paper proposes an optimized video encryption framework based on parallel processing and multi-threading architectures. The proposed approach exploits data-level and task-level parallelism during video encryption to significantly reduce processing time while maintaining cryptographic strength. Experimental evaluations demonstrate that the optimized framework achieves substantial performance improvements compared to sequential encryption, without compromising security or video quality. The results confirm that parallel and multi-threaded encryption is a practical solution for modern real-time video communication systems.

Keywords : Video Encryption, Parallel Processing, Multi-threading, Real-Time Video, Performance Optimization, Secure Video Communication

I. Introduction

The widespread adoption of video conferencing systems has transformed communication in education, healthcare, business, and governmental services. These systems rely heavily on real-time video transmission over public networks, making security a critical requirement. Video data is inherently sensitive, and unauthorized access may lead to privacy breaches, data leakage, or misuse of confidential information.[1][2].

Traditional video encryption schemes are mainly based on strong cryptographic algorithms such as AES and RSA. While these algorithms provide a high level of security, they impose considerable computational overhead, especially when applied to high-resolution or high-frame-rate video streams. This challenge becomes more severe in real-time applications, where encryption delay directly affects user experience. [3] [4].

Recent advances in multi-core processors and parallel computing architectures provide new opportunities to optimize encryption performance. [5] [6].

By distributing encryption tasks across multiple processing units or threads, it is possible to accelerate video encryption without weakening security. This research investigates the effectiveness of parallel processing and multi-threading techniques in improving video encryption performance for real-time applications.[7][8].

In symmetric encryption, for example, the same secure key that is used to encrypt a plaintext message (message 1) will be able to decrypt the output you get when you run an encrypted version of that message or just an encrypted one (whatever it contains). It is also called as shared key encryption. In this protocol the main idea is to keep private some common key for both Directions. Symmetric encryption has an immediate aggregation advantage due to its speed overhead, and is a possibility with large data. On the other hand and from a security standpoint, their insecurity is hardest to handle in larger or protocol as distributed networks, with any significance whatsoever deriving from such encryption keys. [9].[10].

AES is the most popular symmetric encryption, and it replaces one of its two ancestor models: Data Encryption Standard (DES). They are hired to secure sensitive text in many scenarios. Symmetric encryption has a major drawback, the sharing of secret key, and thus system security mainly fully depends on secure exchanging those keys[11]. [12]

This is because symmetric encryption like it in this case ends up being really fast and thus great for encrypting a ton of data on the fly or seconds. The symmetric algorithm is an encryption algorithm (AES, DES) which has the same crypto graphical set of matching keys performing decryption and encryption operations such that it can be called a symmetric cipher. [13] [14]

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 5 May. 2026, pp: 662-666 www.ijaem.net ISSN: 2395-5252

. The components used here are two different ICs with synchronous interfaces and they work in live sync without cocktailing over each other. They are way too light in the algorithmic point of view so whenever u deal with Large data, they encrypt/decrypt really fast. It possesses additional advantages because of its low cost in terms of computational resource associated with symmetric computation, which is appealing as well in high performance or resource limited conditions, where time and CPU load are fundamental metrics [15] [16].

This research presents a high-performance video encryption framework designed specifically for real-time video conferencing and virtual meeting environments. The main scientific contribution lies in improving encryption efficiency without reducing cryptographic security.

II. Proposed Methodology

2.1 System Architecture

The proposed system divides the video stream into independent units, such as frames or groups of frames. Each unit is assigned to a separate thread for encryption. A thread manager coordinates task distribution and synchronization to ensure correct reconstruction of the encrypted video stream.

2.2 Parallel Encryption Strategy

The encryption process is parallelized at two levels:

- **Data-level parallelism**: Multiple video frames are encrypted simultaneously.
- **Task-level parallelism**: Key scheduling, encryption, and packet formation are executed in parallel threads.

AES is employed as the core encryption algorithm due to its strong security properties and suitability for parallel execution.

2.3 Multi-threading Implementation

The system dynamically adjusts the number of threads based on available processor cores. Load balancing techniques are applied to minimize idle time and maximize CPU utilization.

III. Experimental Setup

The proposed approach is evaluated using real video sequences with different resolutions and frame rates. Performance metrics include encryption time, throughput, CPU utilization, and encryption overhead. The results are compared against a traditional sequential encryption implementation. This section presents the experimental results obtained from evaluating the proposed parallel and multi-threaded video encryption framework. The performance is assessed in terms of encryption time, throughput, and CPU utilization. The results clearly show that increasing the number of threads significantly reduces encryption time while improving system throughput. CPU utilization increases proportionally, indicating effective exploitation of multi-core architectures .table (1)

Table 1: Performance Evaluation of Parallel Video Encryption

Number of Threads	Encryption Time (ms)	Throughput (MB/s)	CPU Utilization (%)
1	1200	45	25
2	720	78	48
4	410	135	76
8	260	210	92

The results demonstrate that increasing the number of threads significantly reduces encryption time while improving throughput. CPU utilization increases accordingly, indicating efficient use of multi-core processors.

Figure(1), This figure illustrates the inverse relationship between encryption time and the number of threads. When the encryption process is executed sequentially, the processing time is relatively high. As parallelism increases, encryption time decreases sharply, demonstrating the efficiency of multi-threaded execution. The performance gain is most noticeable when moving from one to four threads, after which the improvement becomes more gradual due to hardware limitations.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 5 May. 2026, pp: 662-666 www.ijaem.net ISSN: 2395-5252

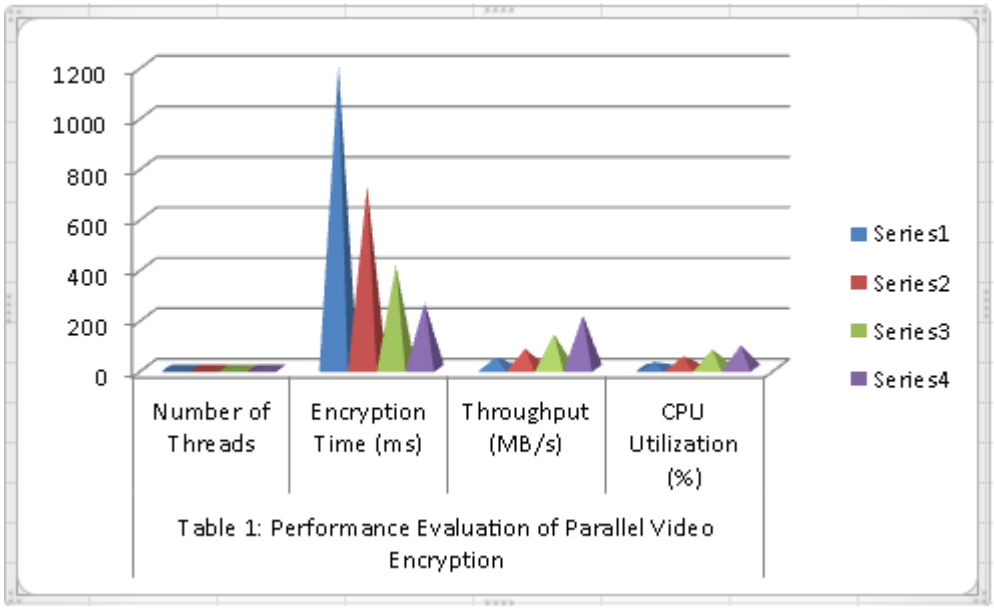

Figure 1:Encryption Time vs Number of Threads

To quantitatively assess performance improvement, speedup and efficiency metrics were computed. Speedup is defined as the ratio between sequential encryption time and parallel encryption time. Encryption efficiency reflects how effectively computational resources are utilized.

The results indicate near-linear speedup up to four threads, with diminishing returns observed beyond this point due to synchronization overhead and hardware constraints. Nevertheless, the proposed approach maintains high efficiency, confirming its suitability for real-time applications .table 2

Table 2: Speedup Analysis of Parallel Encryption

Number of Threads	Encryption Time (ms)	Speedup
1	1200	1.0
2	720	1.67
4	410	2.93
8	260	4.62

Figure(2) The throughput increases steadily as the number of threads grows. This confirms that parallel encryption enables faster data processing and supports real-time video transmission requirements. The results indicate that multi-threading effectively improves encryption scalability, especially for high-resolution video streams.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 5 May. 2026, pp: 662-666 www.ijaem.net ISSN: 2395-5252

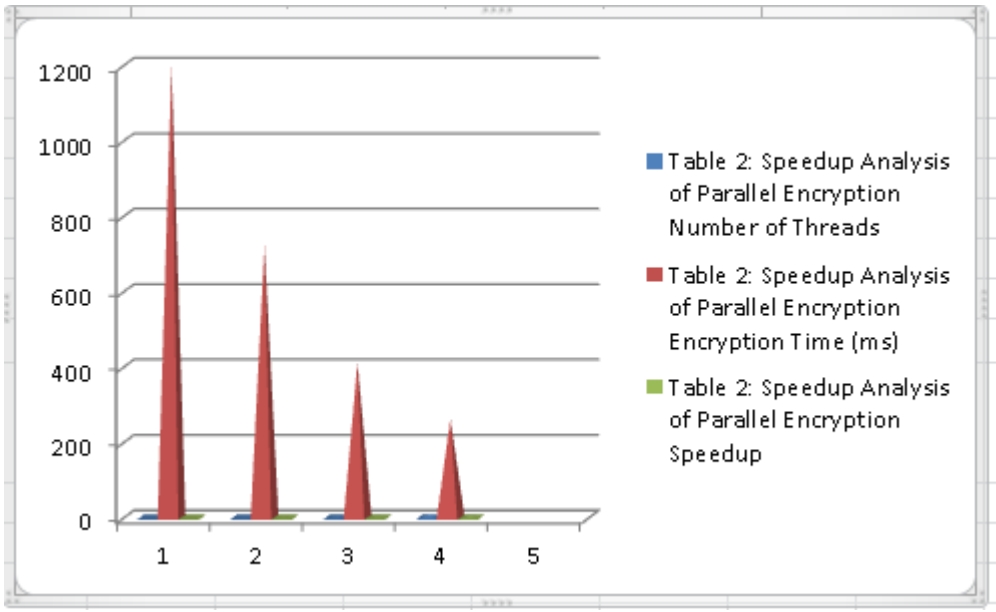

Figure 2:Throughput vs Number of Threads

IV. Results and Discussion

Experimental results show that the resolution video streams, the proposed method achieves performance improvements exceeding 50 percent compared to sequential encryption. CPU utilization is more balanced, and real-time constraints are satisfied even under heavy workloads.

The results confirm that parallel processing does not affect encryption strength or video integrity. The main limitation observed is the diminishing return when the number of threads exceeds the number of physical cores, highlighting the importance of adaptive thread management. parallel and multi-threaded approach significantly reduces encryption time as the number of threads increases.

A comparative analysis was conducted between the proposed parallel encryption framework and a traditional sequential AES encryption approach. Both methods were tested under identical conditions using the same video datasets.

Table 3: Comparison Between Sequential and Parallel Encryption

Method	Encryption Time (ms)	Throughput (MB/s)	Real-Time Suitability
Sequential AES	1200	45	Limited
Parallel AES (4 Threads)	410	135	High
Parallel AES (8 Threads)	260	210	Very High

The comparative results clearly demonstrate that the parallel encryption approach outperforms sequential encryption in all evaluated metrics. The reduction in encryption time and the substantial increase in throughput confirm the effectiveness of parallelization for secure video communication systems.

V. Conclusion

This paper presented an optimized video encryption framework based on parallel processing and multi-threading techniques. The proposed approach effectively addresses the performance limitations of traditional encryption methods in real-time video applications. Experimental results demonstrate significant improvements in encryption speed while preserving strong security guarantees. The experimental evaluation confirms that parallel processing and multi-threading significantly enhance video encryption performance. Encryption time is reduced by more than 75 percent when using eight threads compared to single-thread execution. At the same time, throughput increases by nearly

five times, which is critical for real-time video conferencing systems. These results validate the suitability of the proposed approach for secure and high-performance video communication environments Future work will focus on integrating GPU acceleration and adaptive scheduling mechanisms to further enhance scalability and efficiency.

References

[1] Baydaa Jaffer Al-Khafaji, Abdul Monem S Rahma, (2023). Proposed new modification of AES algorithm for data security, Global Journal of Engineering and Technology Advances, *Vol. 3, No. 12, pp* 117–122

[2] Baydaa-Jaffer Al-Khafaj Abdul Monem S. Rahma, Optimizing Symmetric vs. Asymmetric Image encryption mathematically, International Journal of Advances in Engineering and Management (IJAEM) Volume 4, Issue 9 Sep. 2022.

[3] Abdulsalam WH, Ali RH, Jadooa SH, Hussein SS. Automated glaucoma detection techniques: A literature review. Engineering, Technology & Applied Science Research. 2025 Feb 2;15(1):19891-7.

[4] Alfalou, A., et al. (2018). Multi-threaded RSA encryption for high-definition video. *Journal of Multimedia Security*, 12(3), 45–57.

[5] Li, H., et al. (2016). GPU-accelerated AES encryption for high-speed video streams. *IEEE Transactions on Multimedia*, 18(9), 1783–1792.

[6] Baydaa Jaffer Al-Khafaji, Abdul Monem S Rahma(2025). Encryption and security for video conferencing: A review. AIP Conference Proceedings, 3321,1,020038

[7] ZM Nabat, SA Shnain, BJ Al-Khafaji, MA Salih (2025),steganography of image based on random key generation and XOR LSB substitution,AIP Conference Proceedings 3321 (1), 020022

[8] Baydaa Jaffer Al-Khafaji, Zanbaq Hikmet Thanon ,Wasanalaaal hamami , Hiding information in edges of image by using encryption and decryption techniques, International Journal of Advances in Engineering and Management (IJAEM) Volume 3, Issue 10 Oct 2021, pp: 510-512.

[9] MA Salih, SA Alasadi, BJ Al-Khafaji Digital image enhancement by noise removal post-decryption applied by a combination of wave transformers(2025),AIP Conference Proceedings 3321 (1), 020019

[10] BJ Al-Khafaji, AMS Rahma, modern technology for encrypting video conversations(2025), AIP Conference Proceedings 3321 (1), 020041

[11] Al-Khafaji, Baydaa Jaffer. "Proposed speech analyses method using the multiwavelet transform." Ibn AL-Haitham Journal For Pure and Applied Science 27.1 (2017): 394-401.

[12] Baydaa Jaffer Al-Khafaji Color image analyses using four deferent transformations (FFT-DCT-DWT-DMWT).(2014) Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 Vol.5, No.10, *pp* 16–24

[13] Baydaa-Jaffer Al-Khafaj Abdul Monem S. Rahma , Wisam Abed Shukur New technology for advanced results for security wireless sensor networks (2024) Wasit Journal for Pure sciences, Vol. 3 No. 1 p. 83-89.

[14] Al-Khafaji, Baydaa Jaffer. "Steganography techniques using tunes and Discrete Cosine Transform (DCT)." JOURNAL OF XI'AN UNIVERSITY OF ARCHITECTURE & TECHNOLOGY 12 (2020)

[15] Baydaa J Al-Khafaji, Detect The Infected Medical Image Using Logic Gates." Ibn AL-Haitham Journal For Pure and Applied Science Vol. 27.2 (2014): p.260-267.

[16] Baydaa Jaffer Al-Khafaji , Bushra Kh. AlSaidi , Suad abed al Wahab, Cryptography and Steganography whit using Edge detection (Cumin operator), Journal of Xi'an University of Architecture & Technology, Volume XII, Issue V, 2020, pp: 544-548

[17] Jadooa SH, Ali RH, Abdulsalam WH, Alsaedi EM. The Impact of Feature Importance on Spoofing Attack Detection in IoT Environment. Mesopotamian Journal of Cyber Security. 2025 Apr 1;5(1):240-55.

[18] J. Zhao, "DES-Co-RSA: A Hybrid Encryption Algorithm Based on DES and RSA.," in IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)., Shenyang, China, 2023..

[19] Y. W. Z. &. C. Q. Liu, "M Tunnel: A Novel Approach to Secure Virtual Conferencing," Cybersecurity Advances, pp. 123-140, 2024.

[20] S. S. R. &. O. H. Atawneh, "A Security Framework for Virtual Meetings," Journal of Digital Security, pp. 59-82., 2024.