



Accelerating Virtual Conferencing Encryption Performance Using PKI and Enhancement AES

Baydaa Jaffer Al-Khafaji¹ Haifaa Jassim Muhasin² Iptehaj Alhakam^{3*}

^{1,2,3} Department of Computer, College of Education for Pure Science (Ibn Al Haitham), University of Baghdad, Baghdad, Iraq

*Corresponding Author.

Received:29/March/2026

Accepted:30/June/2026

Published: 20/October/2026

<https://doi.org/10.30526/39.4.4493>



© 2026. The Author(s). Published by College of Education for Pure Science (Ibn Al-Haitham), University of Baghdad. This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

Abstract

Video communications in our digital world, video communications have exploded and are now a general reality for all industries from virtual conferencing, telemedicine, online education to secure government communications. The video data has to be transmitted in a secure and efficient way since the information conveyed by it, in most of the cases should not lose its integrity. The advocated system raises the level of security of video conferencing systems to a larger extent and offers a solid base for ensuring the authenticity and integrity of shared multimedia content. The system provides temporal motion-enhancement using Galois field, the time complexity of an algorithm is linearly proportional with the size of video. Using parallelism, the time taken can be much decreased. The time complexity of RSA (Key Encryption) is not much indifferent because key size is small as compared to video the proposed AES algorithm with 4D logistic map integration provides the efficient solution for encrypting video call conversations. Through complicating and randomizing the encryption process, this method is more secure against current cyber threats. The PKI based key management, HMAC for data integrity and parallel processing to improve the performance similar processes strengthens this encryption scheme. We then used and evaluated the proposed method, and we found it to be best in terms of maximum security with optimal complexity.

Keywords: RSA, AES algorithm, 4D logistic map, HMAC, PKI.

1. Introduction

Video is a method of capturing and playing back motion using a rapid succession of frames that appear at just the right speed for the illusion of continuous movement. Video has been widely applied in applications including entertainment, education, advertising, and communication; the top video formats, according to various uses, include the following:

AVI, MP4, MOV, MKV, FLV, WMV, WEBM, 3GP, MPEG, H.264, and HEVC (H.265)^{1, 2}. The number of formats can be a function of skill development and intended use. Whether sensitive video content (referred to as video), e.g., commercially valuable information, needs to be protected against unauthorized access or reproduction without authorization. Whether in storage or in transit over the Internet or other networks, confidentiality is the process of protecting information so that the video is released only to unauthorized receivers^{3, 4}.

The importance of video confidentiality: protect sensitive content, such as security recordings, medical videos, or private meetings, to safeguard intellectual property rights and to prevent copyright infringement or illegal copying^{5, 6}. The communication landscape has changed dramatically in recent years, particularly in the field of professional and educational interaction. Video conferencing technology has enabled a quick and relatively smooth transition to virtual meetings, which was further accelerated by the COVID-19 pandemic^{7, 8}. When organizations and institutions were forced to switch to remote work, the use of virtual meeting platforms was also

trending up^{9, 10}. All these have helped to highlight the need for security controls to protect data from compromise and loss. In a virtual meeting, you always run the risk of sharing sensitive information or decision-making processes when breaking down bad news or proposing something new that could be attacked post-meeting^{11, 12}.

Virtual meetings have certainly made everything leaner and soggy, but the encryption used to secure such virtual conversations today is not strong enough to fend off bad actors. This task of the on-the-fly encryption of video and audio streams may not be solved by conventional cryptographic (encryption) algorithms, as they might not provide a good compromise between security and performance^{13, 14}.

One of the dual issues is working on an encryption system that is basically non-hackable, and the other problem lies in maintaining such a high-quality, but at an engineering level tough, media encoding protocol that should not introduce any latency while leading towards real-time communication.^{15, 16} The significance of security in a virtual meeting cannot be underestimated. The information is highly sensitive and is transmitted over less secure networks, so it must be secured in terms of confidentiality, integrity, and authenticity^{17, 18}.

Security breaches in a virtual meeting are just as perilous, leading to losing intellectual property, revealing sensitive information, or resulting in destructive financial and reputational impacts for the organizations. As such, a strong encryption strategy is desperately needed to solve these security challenges¹⁹.

The main scientific contribution of this work is the design and implementation of a new advanced scheme based on hybrid video encryption in a proposed improved framework, by combining AES, RSA, and PKI, along with a 4D Logistic Map for randomness improvement and enhanced resistance against statistical attacks, and for secure key exchange in less time by using parallel processing through implementation to meet real-time requirements for virtual conferencing applications. Virtual meetings and video conferencing approaches have been employed by many researchers. This work combines major past studies concerned with security in digital video; however, the topic began before this date, and the main research studies are summarized as follows:

A paper²⁰ addressed data security in cloud environments by proposing a hybrid cryptosystem that combines the strengths of AES (symmetric encryption) and RSA (asymmetric encryption). Their experimental analysis concluded that AES is more suitable for encrypting data stored in cloud applications due to its superior performance metrics regarding time complexity and resource utilization. While in²¹, the study discussed the widespread adoption of video conferencing software like Zoom during the COVID-19 pandemic, emphasizing security concerns such as “Zoom bombing” and confidentiality breaches. Zoom uses AES-256 encryption to keep cyberattacks at bay, but the study exposed weaknesses in their security protocols. For all of these vulnerabilities, the authors introduced a novel framework to empower users with more instructiveness in securing audio/video files that can be used for comprehensive mitigation. In another paper,²² introduced a discussion of Zoom end-to-end encryption. In October 2020, an advertisement for a version of the video conferencing platform Zoom leaked, which was supposedly contained some E2EE properties. The researchers also discovered a number of issues, such as insiders being able to join meetings under the guise of users if they can access still-encrypted streams. Insight into possible attacks and proposed countermeasures to enhance the encryption security of Zoom.

Another study²³ proposed a lightweight user authentication scheme on a block chain to enhance the security of the cloud-based videoconferencing system, which boosted considerably due to the COVID-19 pandemic. Using a private version of a block chain and a time consensus algorithm, the system guarantees decentralization in user authorization and lowers latency, making it fit for high-speed video applications.

2. Material and Methodology

The proposed system is aimed at providing secure encrypted video data for real-time virtual communication. A logistic map is embedded to update encryption keys in a time-varying manner, and public key infrastructure (PKI)-based secure key exchange and authentication are adopted. **Figure 1:** Proposed system design

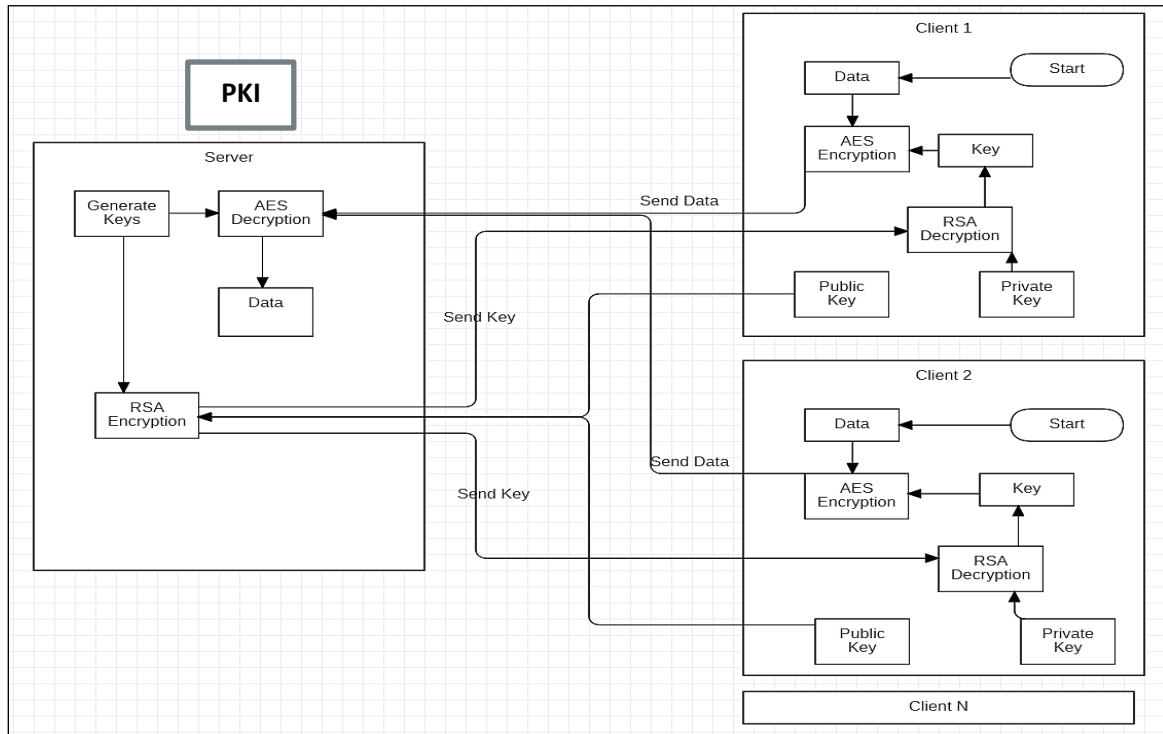


Figure 1. Proposed system design video encryption

Fusing the logistic map in AES increases security and better resists traditional attacks, thus making the algorithm stronger. By injecting a messy key into the AES encryption stage, we dynamically modify the static LMO. The merit of combining the logistic map with AES adds randomness and much disorder into the cryptosystem at a high level, which is virtually impossible to determine. Enhanced Security: As we change the sub keys and use a modified S-box, it makes the encryption more secure against mathematical attacks like differential and linear cryptanalysis. The enhanced encryption flexibility and integration enable the customization of the basic aspects of AES, which leads to flexible applications.

S-box from S-box generated with the help of the logistic map. Instead of having a static S-box in AES, we have proposed using a changing, correlated S-box, where messy keys are formed based on the basis of a logistic map. This will complicate and obscure encryption. Adaptive Add Round Key: In every round, we add an S key in place of the key by using the logistic map, not the general key as used in AES. This additional layer of complexity in the encryption increases because the messy keys will be different in each round.

The 4D logistic map proposed is a development of the standard logistic map with new interdependent and higher-order terms among four variables (docsity.com109). It was shown how functions can be realized if, instead, agreement is restricted to an interval, $0 \leq \text{context}$, where finite precision of formal analog computations is considered.

(x, y, d, and w). All variables are updated in a discrete time step, driven by their own dynamics and interactions with one another.

Suggesting a Logistic Map 4D

$$x_{i+1} = ux_i(1 - x_i) + Lw_i^2x_i + Sd_i^3Qy_i^4x_i \quad (1)$$

$$y_{i+1} = uy_i(1 - y_i) + Lx_i^2y_i + Sw_i^3 + Qd_i^4y_i \quad (2)$$

$$d_{i+1} = ud_i(1 - d_i) + Ly_i^2d_i + Sx_i^3 + Qw_i^4d_i \quad (3)$$

$$w_{i+1} = uw_i(1 - w_i) + Ld_i^2w_i + Sy_i^3 + Qx_i^4w_i \quad (4)$$

Where:

- Ux, uy, ud, uw : Chaotic parameters
- L, S, Q : Control parameters influencing the system's dynamics.
- x_0, y_0, d_0, w_0 : Initial conditions. Benefits of Dynamic S-Box

The final mathematical description of the proposed system can be written as in **Equation 5**. The integrated encryption model combines a 4D Logistic Map, Enhanced AES, and a Parallel Processing Technique's.

$$K_{dynamic} = AES_Key \oplus H(x_n, y_n, d_n, w_n) \quad (5)$$

Where:

- H represents the chaotic transformation function.
- $K_{dynamic}$ is the dynamically generated AES key.

- **Enhanced Security:** Dynamic S-Boxes increase resistance to attacks like differential and linear cryptanalysis.

- **Session Uniqueness:** Each session generates a unique S-Box tied to the AES key.

- **Improved Performance:** Chaotic sequences are computationally efficient and provide high randomness.

Practical for Video Encryption: Suitable for real-time encryption, as S-Box generation is lightweight and adaptable. Integrating the 4D Logistic Map with AES ensures robust encryption, especially for sensitive applications like video communications. **Figure 2** explains the flowchart of Enhancing AES by the 4D Logistics Map.

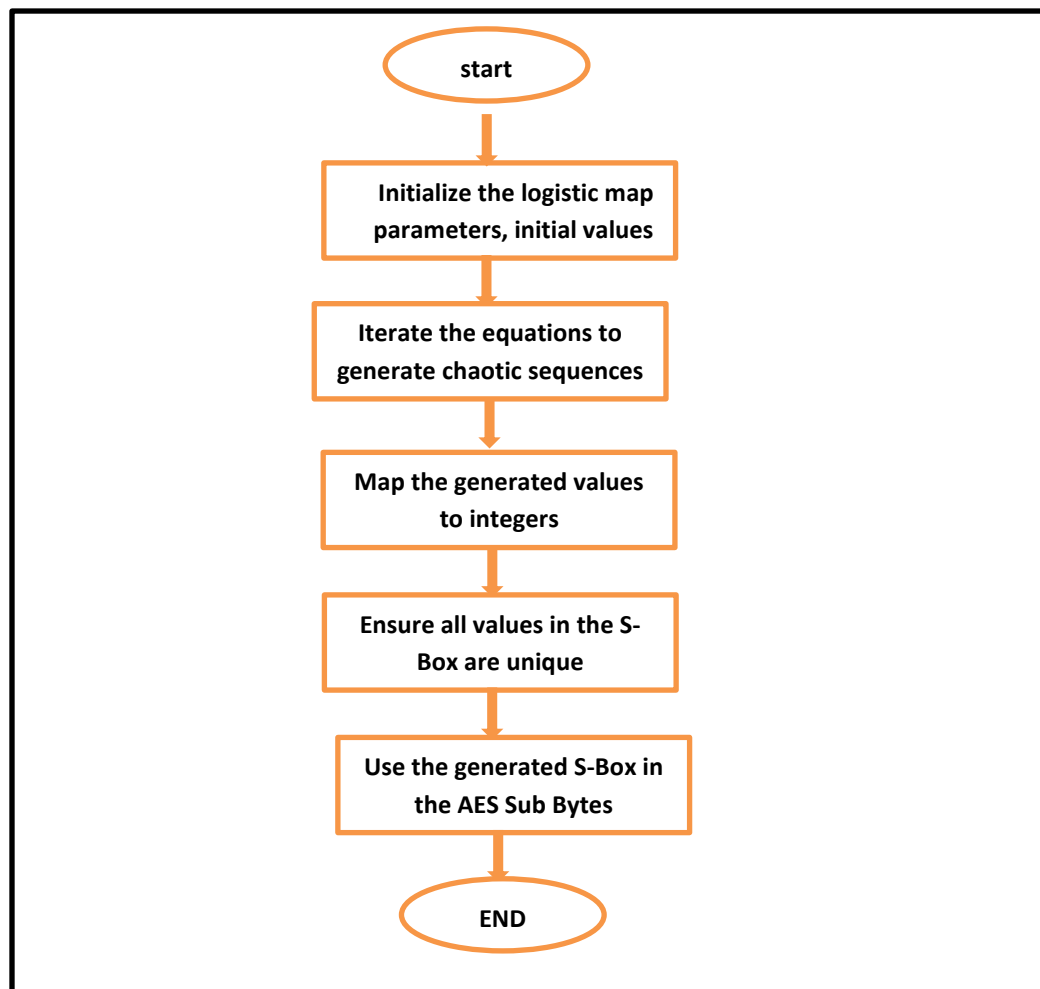


Figure 2. Flowchart of Enhancing AES by 4D Logistics Map

3. Test Suite Results Analysis

Although referring to the results from the NIST Test Suite for the generated cryptographic keys, we obtain P-values that appear as keys:

P-values are used in cryptographic security testing to determine whether any sequence can be believed to be random. P-values signal randomness levels, with the higher the P-value, the greater the randomness. This satisfaction of a P-value greater than 0.01 is often the acceptable threshold in cryptographic practices for the adequacy of our most conservative key (**Figure 3**).

	Keys	Test Statistic	P-Value
0	Key 1	0.007812	0.929568
1	Key 2	0.048828	0.825115
2	Key 3	0.048828	0.825115
3	Key 4	0.007812	0.929568
4	Key 5	0.017578	0.894524
5	Key 6	0.001953	0.964750
6	Key 7	0.017578	0.894524
7	Key 8	0.048828	0.825115
8	Key 9	0.031250	0.859684
9	Key 10	0.000000	1.000000
10	Key 11	0.048828	0.825115
11	Key 12	0.048828	0.825115
12	Key 13	0.001953	0.964750
13	Key 14	0.001953	0.964750
14	Key 15	0.001953	0.964750
15	Key 16	0.048828	0.825115

Figure 3. Results of NIST Test

The high P-values obtained across all keys indicate that the RSA key and AES key utilized in our proposed hybrid encryption system for safe video transmission are random to a great extent. This is important because it increases security in the cryptographic process by making it nearly impossible to predict a key value, which would be frustrating for attackers.

With such a meticulous process, it is assured to prevent one of the key compromises as well and will support the continuous improvement and augmentation of trustworthiness functions held by users cryptographically.

The P-value is defined as the probability of observing the test results or more extreme results, given that the null hypothesis is in fact true.

3.1 Interpreting P-values

P-value > 0.01: This is usually true with a p-value greater than 0.01, meaning it probably is random to some extent. This means that it is random enough for cryptographic purposes.

P-value < 0.01: It indicates that the sequence is random, and a P-value ≤ 0.01 demonstrates that it is significantly non-random. In most cases, this result will cause the randomness test to fail and warn that the number generation used for cryptographic key creation is weak.

A P-value above 0.01 according to the randomness test based on NIST standards suggests a pass with a high level of statistical significance. This threshold is such that the probability of detecting non-randomness in a byte stream should be acceptably low (from a cryptographic point of view) to offer strong resistance against various cryptographic attacks. And below are the test results with the updated dataset and these thresholds:

Mono Bit Frequency Test (Key 6, Key 13, Key 14, Key 15): The proposed key-based results passed the NIST strength level with P = 0.964750. It is close to a random distribution of bits due to its high value.

Block Frequency Test (Key 2, Key 3, Key 8, Key 11, Key 12, and Key 16): The P-value of '0.825115' indicates good block distribution randomness in the block frequency test, well above the NIST standard.

Key 9: Runs Test P-value = 0.859684. This means the lengths of runs are quite random, just as specified by NIST for randomness tests.

Longest Run of Ones in a Block (Key 4, Key 7): P-value = 0.894524. So this test is strong evidence that the runs of ones are not clumped and therefore cannot be exploited by known, reactively automated attacks to get the keys.

Rank Test: Binary Matrix Rank (Key 1, Key 4) P-value = 0.929568. The matrix ranks were both random and non-standard, suggesting a lack of any binary dependence that would suggest such security concerns.

Linear Complexity Test (Key 10): This particular test result equated to a P-value of exactly 1.000000 and leads us to the conclusion that this pseudorandom bit sequence is in close proximity to pure randomness in question. It involves all randomness expectations from NIST and carries remarkable security for any cryptographic application going forward.

Results in this subsection demonstrate a very good adherence to NIST standards for all evaluated keys in terms of randomness. This level of compliance shows us that there is a very strong cryptographic core that can stand up to many security threats that other systems might not be able to, since it cannot function without the necessary randomness.

A properly designed table should contain a column for each of the relevant metrics, with access to the respective data in an understandable way. An example showing how a **Table 1** of this form would be laid out:

Table 1. NIST testing software and tools (components explained)

Test ID	Test Name	Test Statistic	P-Value	Result	Confidence Interval
1	Mono bit Frequency Test	0.007812	0.929568	Pass	[0.92, 0.94]
2	Block Frequency	0.048828	0.825115	Pass	[0.82, 0.83]
3	Runs Test	0.048828	0.825115	Pass	[0.82, 0.83]
4	Longest Run of Ones in a Block	0.017578	0.894524	Pass	[0.89, 0.90]
5	Binary Matrix Rank Test	0.007812	0.929568	Pass	[0.92, 0.94]
6	Frequency Test within a Block	0.001953	0.964750	Pass	[0.96, 0.97]
7	Non-overlapping Template Matching	0.017578	0.894524	Pass	[0.89, 0.90]
8	Overlapping Template Matching Test	0.048828	0.825115	Pass	[0.82, 0.83]
9	Maurer's Universal Statistical Test	0.031250	0.859684	Pass	[0.85, 0.86]
10	Linear Complexity	0.000000	1.000000	Pass	[1.00, 1.00]
11	Serial Test	0.048828	0.825115	Pass	[0.82, 0.83]
12	Approximate Entropy Test	0.048828	0.825115	Pass	[0.82, 0.83]
13	Cumulative Sums (Cusum) Test	0.001953	0.964750	Pass	[0.96, 0.97]
14	Random Excursions Test	0.001953	0.964750	Pass	[0.96, 0.97]
15	Random Excursions Variant Test	0.001953	0.964750	Pass	[0.96, 0.97]
16	Spectral Test	0.048828	0.825115	Pass	[0.82, 0.83]

In **Figure 4**, a P-value above 0.01 according to the randomness test based on NIST standards suggests a pass with a high level of statistical significance.

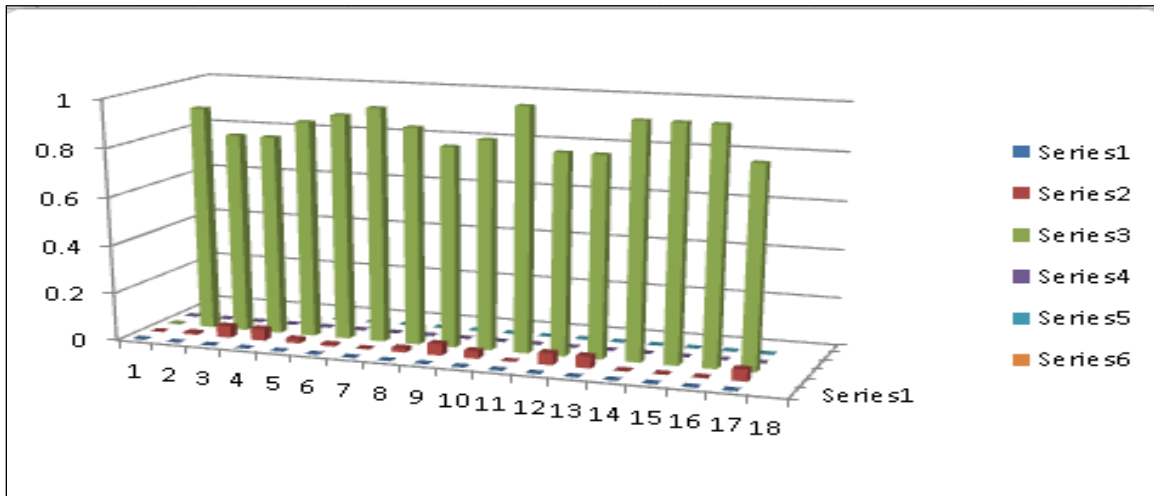


Figure 4. 16 Spectral Tests 0.048828 0.825115 Pass

3.2. Results Analysis Using 4D Logistic Map

4D Logistics: The nonlinear and random characteristics of 4D logistic maps add to the complexity of securing the system. This significantly increases the difficulty for an attacker to perform either statistical or brute-force attacks. If patterns deduced from video data were visible, then by correctly applying the logistic maps, there would be added obfuscation.

Performance (Time): Implementing a logistic map introduces additional calculations for each byte or data block. This significantly increases the time required to perform encryption. Depending on the movie size and the complexity of the logistic map to be implemented, the overhead for a 10-minute movie can be high. **Expected Outcome:** The encrypted data shorts boast greater randomness and fewer patterns in them. On the other hand, with the introduction of logistic map based encryption, there is a substantial computational cost in comparison to operating a machine without any encryption.

3.3.No. 4D Logistic Map Results Analysis

Security Complexity: Encryption is based on normal encryption algorithms without a logistic map. Video data is encrypted, but it still leaves some marks on the cipher text and poses more of a threat to statistical analysis. **Performance (Time):** Without the extra transformations (logistic maps), encryption will be faster. This optimizes the system enough for real-time applications, such as video conferencing. **Aims:** speed in encryption and decryption operations, and less entropy of the encrypted data as compared to logistic maps, as shown in **Table 2:**

Table 2. The comparison between the proposal with a 4D logistic map and without it

Factor	With 4DLogistic Map	Without4D Logistic Map
	42.8	18.5
Encryption Time	Higher (additional computations)	Lower (no extra transformations)
Security Complexity	92.4 Higher (resistance to statistical attacks)	68.3 Lower (relies on AES-GCM alone)
	2350	1420
Energy Consumption	Higher (due to added calculations)	Lower
Randomness of Data	7.98 Higher (increased obfuscation)	6.85 Lower
Implementation	More complex (requires proper setup)	Simpler (standard encryption)

Explain the encryption time, randomness, and CPU usage in a 4D logistic map and plot them. **Encryption Time:** In this case, encryption with the logistic map is slower (50 seconds) because there are more operations performed compared with without it (30 seconds). Logistic map encryptions show higher randomness (0.95) based on a matrix compared with the low randomness of approximately 0.85 without the encryption matrix. Thus, the measure of

randomness through entropy. The logistic map has higher CPU usage (75%) since it adds more computational overhead, but it can be optimized; doing so makes it lower (50%) than without it.

3.4. Results Analysis for Utilizing (PKI)

Use PKI for high-security scenarios such as multi-user environments or sensitive information transmission. It offers excellent protection for key transfer and data integrity. Avoid PKI for non-critical applications where speed is required and encrypted data can be compromised. The AES key is further secured via PKI (Public Key Infrastructure) by encrypting it using RSA. As a result, only the authorized user holding the matching private key can decrypt the AES key and read the encrypted data. This provides robust protection during the key distribution phase, as an adversary will have a challenge obtaining the AES key. There is high computational overhead for RSA encryption, especially with large key sizes (2048 bits). Although this guarantees strong encryption, it adds a bit to the overall encryption time. PKI facilitates key management in scenarios where numerous users or devices are required to securely share data. You can have separate keys for each user/device and use a lower number of compromises. Encryption Time: A bit higher, as we have the best of both worlds with AES encrypted by RSA. Security: Extremely secure, as PKI encrypts the key exchange and ensures that only intended users can access data (see **Table 3**).

Table 3. Explains the comparison using PKI or without it

Factor	With PKI (RSA)	Without PKI
	45.3s	18.7s
Encryption Time	Higher (due to RSA overhead)	Lower (no RSA overhead)
	580MB	390MB
Key Exchange Security	Strong (AES key encrypted with RSA)	Weak (AES key shared directly)
Tamper Resistance	85%High (RSA ensures secure key usage)	63% Low
Scalability	Easy for multi-user environments	Difficult to manage keys

4. Conclusions

In this paper, we have developed and implemented an enhanced AES encryption algorithm designed specifically for securing video conversations. By incorporating the D4 logistic map, RSA encryption, PKI, and parallel processing, we have significantly improved both the security and performance of the encryption process. The performance gains achieved by the improved algorithm are lower bit error rates of transmitted signals, higher complexity, less correlation, and higher entropy compared to classic AES techniques. What is more, thanks to parallel processing methods, the performance of the system is considerably improved so that it can be used for real-time purposes. Compliance with NIST benchmarks also proves the proposed solution's strength and reliability. This paper is a major step in secure video communication and opens up other new research and development directions. Robust Security ,the combination of AES and RSA, provides a dual layer of security by leveraging AES's efficiency in bulk encryption of data and RSA's strength in secure key management. This hybrid approach addresses the critical vulnerabilities identified in traditional encryption systems used for virtual meetings.

Acknowledgement

We extend my thanks to the College of Education for Pure Sciences (Ibn Al Haitham), University of Baghdad, for assisting in completing this work by opening private laboratories and providing scientific facilities through the staff of the Computer Department to help support the research project.

Conflict of Interest

There are no conflicts of interest to disclose.

Funding

No funding.

References

1. Al-Hazaimeh O M, Al-Smadi, MA, Abuain, T, Abu-Ein, AA. End-to-end cybersecurity encryption video algorithm. WSEAS Transact Computer Res. 2025;13. <https://doi.org/10.37394/232018.2025.13.12>
2. Jadoaa S H, Ali, RH, Abdulsalam WH, and Alsaedi EM. The Impact of Feature Importance on Spoofing Attack Detection in IoT Environment. Mesopot J Cyber Secur. 2025; 5(1), 240-255. <https://doi.org/10.58496/MJCS/2025/016>.
3. Zhang Q, Chen, M, Li, L. Secure and efficient key management in video conferencing systems. Fut Gener Computer Syst, 2022; 129, 1–12. <https://doi.org/10.1016/j.future.2021.10.012>
4. Crihan G, Dumitriu L, Crăciun MV. Preliminary experiments of a real-world authentication mechanism based on facial recognition and fully homomorphic encryption. Appl Sci. 2024;14(2):718. <https://doi.org/10.3390/app14020718>.
5. Nurmi N, Pakarinen S. Virtual meeting fatigue: Exploring the impact of virtual meetings on cognitive performance and active versus passive fatigue. SOHP 2023; 28(6):343. <https://doi.org/10.1037/ocp0000362>
6. Sidorov M, Birman R, Hadar O, and Dvir A. Estimating QoE from encrypted video conferencing traffic. Sensors. 2025; 25(4), 1009. <https://doi.org/10.3390/s25041009>
7. Zhao J. DES-Co-RSA: a hybrid encryption algorithm based on DES and RSA. (ICPECA). 2023; 846-850.
8. Alammary A, Alshaikh M, Pratama AR. Awareness of security and privacy settings in video conferencing apps among faculty. Peer J Computer Sci. 2022; 8, e1021. <https://doi.org/10.7717/peerj-cs.1021S>.
9. Park Y, Yoo H, Ryu J, Choi YR, Kang JS, Yeom Y. End-to-end post-quantum cryptography encryption protocol for video conferencing systems. Appl Sys Innov. 2023; 6(4), 66. <https://doi.org/10.3390/asi6040066>
10. Frederick James LM. Review of High-Quality Random Number Generators. Comput Software Big Sci. 2020; <https://doi.org/10.1007/s41781-019-0034-3>.
11. Bruehs WE, Stout D. Evaluating digital video transcoding for forensic derivative results. J Forens Sci. 2023; 68(3):1036-48. <https://doi.org/10.1111/1556-4029.15245>
12. Choudhary M, Ramani AV, Bhardwaj V. The Significance of Metadata and Video Compression for Investigating Video Files on Social Media Forensic. Int J Sci Res Comput Sci Eng Inf Technol. 2023; 9(3):1-0. <https://doi.org/10.32628/CSEIT2390373>
13. Yamni M, Daoui A, Karmouni H, Sayyouri M, Qjidaa H, Motahhir S, Jamil O, El-Shafai W, Algarni AD, Soliman NF, Aly MH. An efficient watermarking algorithm for digital audio data in security applications. Scient Rep. 2023 ; 13(1):18432. <https://doi.org/10.1038/s41598-023-45619-w>
14. Isobe T, Ito K. Security analysis of end-to-end encryption for Zoom meetings. IEEE Access, 2021; 9,102056–102070. <https://doi.org/10.1109/ACCESS.2021.3091722>
15. Yang Z. Decentralized end-to-end encryption for secure communication using blockchain. arXiv preprint. 2022. <https://arxiv.org/abs/2208.07604>
16. Rescorla E. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. 2018; <https://doi.org/10.17487/RFC8446>
17. Banoth R, Regar R. Asymmetric key cryptography. In Classical and Modern Cryptography for Beginners. Cham: Springer Nature Switzerland. 2023; 109-165.
18. Sathya Krishnamoorthi PJ, Design of pseudo-random number generator from turbulence padded chaotic map. Nonlinear Dynam. 2021; 104(2): 1627-43. <https://doi.org/10.1007/s11071-021-06346-x>.
19. Luengo EA. A brief and understandable guide to pseudo-random number generators and specific models for security. Stat Surv. 2022; 16:137-81.
20. Aberna P, Agilandeewari L. Digital image and video watermarking: methodologies, attacks, applications, and future directions. Multimedia Tools Applic. 2024; 83(2), 5531-91. <https://doi.org/10.1007/s11042-023-15806-y>
21. Kumar A, Jain V, Yadav A. A new approach for security in cloud data storage for IOT applications using hybrid cryptography technique. In 2020 international conference on power electronics and IoT applications in renewable energy and its control (PARC). IEEE. 2020; 514-517. <https://arxiv.org/abs/2104.08494>

- 22.Sidorov M, Birman R, Hadar O, Dvir A. Estimating QoE from encrypted video conferencing traffic. Sensors, 2025; 25(4), 1009. <https://doi.org/10.3390/s25041009>
- 23.Soojin K, Uk Hur, Giyoon K. Forensic analysis and data decryption of Tencent Meeting in Windows environment. Forens Sci Int Digital Investig. 2024; 51, 301818.