© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1717594

Cryptographic Digital Video Security Using Modified Advanced Encryption Standard (AES)

FALUYI B. I.[1], OGUNTOYE, J. P.[2], ADEDEJI O. T.[3], ARULOGUN O. T.[4], FALOHUN A. S.[5], MAKINDE B. O.[6]

[1]*Department of Computer Science, The Federal Polytechnic, Ado-Ekiti, Ekiti State, Nigeria*

[2, 4, 5]*Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria*

[6]*Department of Computing and Informatics, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Department of Computer Science, Osun State College of Technology, Esaoke, Osun State, Nigeria*

Abstract- ***The proliferation of digital multimedia content has necessitated the development of secure methods for legal distribution to mitigate issues like alterations, exploitation, and illegal duplication during video communication. Crystography, a combination of cryptography and steganography, enhances information hiding security by encrypting data while concealing its presence. However, existing video steganographic techniques are vulnerable to attacks and suffer from high computational overhead. This study proposes an Advanced Encryption Standard (AES) modification combining Fast Fourier Transform (FFT), dubbed AES-FFT, to improve data hiding, encryption, and decryption time efficiency. Two video formats from YouTube were evaluated: an AVI video with 200 frames and an MP4 video with 402 frames. Many video applications require fast, real-time data hiding, necessitating techniques with low encryption/decryption time overhead. The results demonstrate AES-FFT's superior performance over traditional AES. For the AVI format, AES-FFT encrypted all frames in 0.5356 ms compared to 1.8552 ms for AES, and decrypted in 0.5204 ms versus 1.8408 ms for AES. Similarly, for the MP4 format, AES-FFT encrypted in 0.2363 ms versus 1.5360 ms (AES), and decrypted in 0.2200 ms compared to 1.5185 ms (AES). Lower encryption/decryption times indicate better performance, highlighting AES-FFT's significant speed advantage over AES for encrypting and decrypting video files securely. This technique's ability to enhance data hiding security while reducing computational overhead holds promise for efficient, secure digital video distribution across various applications.***

Keywords- ***Advanced Encryption Standard, Crystography Video Security, Fast Fourier Transform Encryption, Multimedia Data Security***

I. INTRODUCTION

The rise of digital multimedia content has brought about significant challenges in combating piracy and illegal exploitation of copyrighted material. Film piracy, in particular, poses a major economic threat to copyright owners and the entertainment industry (Tade &Mmahi, 2018). Piracy involves the unauthorized reproduction and distribution of intellectual property for financial gain, facilitated by the ease of digital duplication (Freitas, 1994; Nnamani, 2016). Protecting intellectual property rights for multimedia content has long been a complex issue without an ideal solution (Liu *et al.,* 2003; Zeilinger, 2018).

The growth of modern communication technologies necessitates robust security mechanisms to ensure the secrecy and safety of digital data, especially for digital products (Nnamani, 2016; Abolade*et al.,* 2023). These technologies aim to enhance the scope of control for rightful owners to assert authority over their intellectual property (Rao *et al.,* 2009). Encryption plays a crucial role in protecting various types of digital content, including videos, e-books, documents, and games (Liu *et al.,* 2003; Malgieri, 2018).

The Advanced Encryption Standard (AES) is a widely used symmetric block cipher encryption algorithm (Daemen &Rijmen, 2002). It employs variable key lengths of 128, 192, and 256 bits and performs various transformations, such as SubBytes, ShiftRows, MixColumns, and AddRoundKey (Gaton & Geetha, 2019). AES offers advantages over asymmetric ciphers like RSA and ECC in terms of processing

power, time, and key length (Parmar & Verma, 2017). However, AES has a computational overhead drawback due to its large secret key and consistent encryption method for all keys. To overcome the computational overhead associated with the standard AES technique when dealing with complex multimedia data like text, images, and videos, this study proposes incorporating the Fast Fourier Transform (FFT) to modify the AES algorithm (Hameed *et al.,* 2018).

The ubiquity of digital multimedia content in modern times has accentuated the pressing need to develop robust and secure methods for legal dissemination. This is crucial to circumvent nefarious activities such as unauthorized alterations, malicious exploitation, and unlawful duplication during video communication and distribution processes (Okolie, 2023). Crystography, an amalgamation of cryptography and steganography, presents an innovative approach to fortifying information hiding security (Okediran andOguntoye, 2023). It achieves this by employing a dual-pronged strategy of encrypting data while simultaneously obfuscating its very existence.However, despite the potential benefits of crystography, existing video steganographic techniques are beset by vulnerabilities that render them susceptible to various attacks (Dalal,& Juneja, 2021). Furthermore, these techniques are characterized by substantial computational overhead, which impedes their efficacy and practical utility. Consequently, there is an imperative need to explore and develop more efficient and secure alternatives that can circumvent these limitations (Yungaicela-Naula*et al.,* 2022). In this study, the proposed AES-FFT technique presents a promising solution. By synergistically combining the robust encryption capabilities of the Advanced Encryption Standard (AES) with the computational efficiency of the Fast Fourier Transform (FFT), this technique aims to enhance data hiding security while mitigating the computational overhead associated with traditional video steganographic methods.

II. LITERATURE REVIEW

Video encryption algorithms have become an important area of research due to the increasing application of video data and the need for security during transmission (Dumbere&Janwe, 2014). Various approaches have been proposed to provide security for information disseminated over networks, including encryption, authentication, and digital signatures. Specifically for video data, encryption methods have been adopted to protect against unwanted interception and viewing during transmission(Sarker *et al.,* 2012).

The Advanced Encryption Standard (AES) is one of the most prominent and secure cryptographic algorithms for encrypting electronic data (Hameed *et al.,* 2018). As a symmetric block cipher established by the U.S. National Institute of Standards and Technology (NIST), AES offers advantages such as a strong encryption standard and efficient implementation.However, AES also has certain limitations when handling complex multimedia data like video. These include computational overhead, the use of a fixed S-Box (a potential weakness), and pattern problems (Hameed *et al.,* 2018). Additionally, AES can be inefficient for video encryption due to its slowness property (Abaas &Shibeeb, 2015).

Researchers have proposed various modifications to the AES algorithm to improve its performance and suitability for video encryption. One approach involves a new Fast Fourier Transform (FFT) representation-based cryptographic system for multimedia data security (Again & Caglayan, 2006). This system maps the FFT structure based on discrete orthogonal transforms and efficiently implements encryption within the core of the FFT, providing flexibility in shuffling sensitive information and dual key security.Another modification focuses on replacing the slowest transformations in the original AES, such as mix columns, with a new Henon map chaotic-based mask and one mix columns transformation (Abaas &Shibeeb, 2015). This approach aims to reduce encryption and decryption time while enhancing the security level and increasing the key space.

Vijayarajan*et al*. (2019) presented a fingerprint biometric key-based AES for personalized image cryptography. Their bio-key generation scheme used fingerprint matching for user authentication and a passcode for key generation. The experimental results demonstrated better encryption and decryption

performance compared to other key-based encryption techniques.Oke*et al.* (2019) proposed a crystographic technique combining cryptography (Enhanced AES) and steganography (Space Insertion Text Semagram) for secure electronic voting systems. They addressed confidentiality using the crystographic algorithm and post-election auditing using the SHA-256 cryptographic hash function. Performance evaluation showed the effectiveness of the integrated techniques in handling confidentiality and post-election auditing verification.Hafsa *et al.* (2022) proposed an Improved AES (IAES) algorithm specifically designed for real-time video security. This method eliminates the shift-row and sub-byte transformations, replacing them with a mix-row operation to reduce run time. It also incorporates the Henon chaotic map in the key generation procedure to provide more randomness, using the SHA-3 hash algorithm to generate the initial conditions of the chaotic attractor.

These empirical studies highlight the potential of FFT-based techniques and modified AES algorithms in enhancing multimedia security, particularly for video encryption applications. The proposed methods aim to improve security, reduce computational overhead, and address limitations of traditional approaches.

III. METHODOLOGY

In digital video security, the need for efficient and robust encryption techniques is paramount. Video data, owing to its substantial file sizes, is typically stored in compressed formats such as AVI and MP4. However, this compression alone does not provide adequate security, leaving the video content vulnerable to unauthorized access and interception during transmission or storage. To address this concern, this study proposes a modified encryption algorithm tailored specifically for securing compressed video data.The methodology employed in this research revolves around the development of an enhanced Advanced Encryption Standard (AES) algorithm, referred to as AES-FFT. This approach utilized the Fast Fourier Transform (FFT) to integrate encryption within the core of the compression process, thereby providing an additional layer of security while preserving the advantages of video compression.The AES-FFT algorithm was designed to operate directly on compressed video files in AVI and MP4 formats. The proposed technique aims to achieve a seamless integration of security and data compression, resulting in efficient and secure video transmission and storage.

To evaluate the performance of the developed AES-FFT algorithm, a comprehensive experimental setup was employed. A dataset comprising various video files in AVI and MP4 formats was obtained, representing a diverse range of video content and compression levels. The encryption and decryption processes were then carried out using the AES-FFT technique, and the resulting performance metrics were compared against the standard AES algorithm.The primary performance indicators considered in this study were encryption and decryption time. This is to assess the computational efficiency of the proposed AES-FFT algorithm and its suitability for real-time video applications, where timely encryption and decryption are critical.

The conceptual model of the proposed cryptographic scheme for digital video security is illustrated in Figure 1. However, the current study primarily focuses on the encryption and decryption aspects using the AES-FFT algorithm, while the integration of steganographic techniques falls beyond the scope of the current work and is earmarked for future research endeavours.

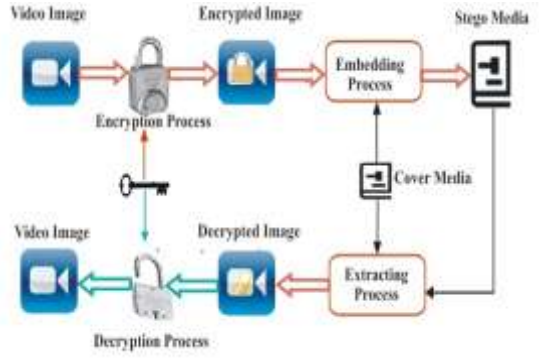

Figure 1: A Conceptual Model of the Developed Crystographic Scheme

Figure 2 illustrates the schematic diagram of the cryptographic processes, depicting the workflow of the encryption and decryption processes using the AES-FFT technique. The compressed video data undergoes encryption using the AES-FFT algorithm, and the resulting ciphertext is transmitted or stored

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1717594

securely. While the overarching objective of this research is to develop a comprehensive cryptographic focuses on the encryption and decryption aspects using the AES-FFT algorithm.

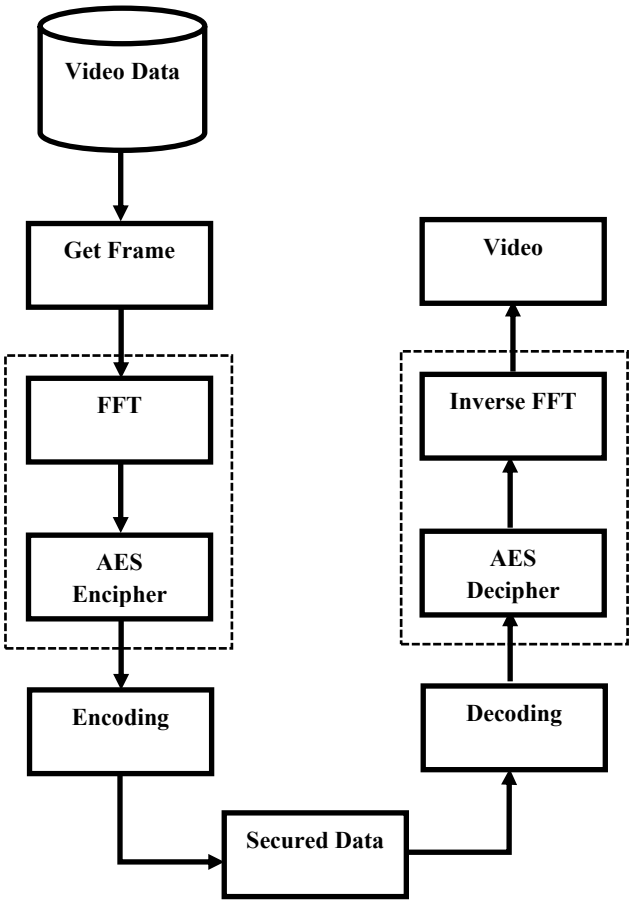

Figure 2: Schematic diagram of the cryptographic processes

3.1 Video Acquisition and Pre-processing

The video data corpus for this study comprised uncompressed video files in AVI and MP4 formats, which are among the most commonly used video formats with high-definition resolution and compatibility for DVD distribution. These videos were acquired from online sources, specifically YouTube, ensuring the selection of popular videos with consistent resolution characteristics for reproducibility purposes.

The acquired video data underwent a pre-processing phase before being subjected to encryption. Initially, the video files were decomposed into their constituent frames, and two additional copies of these frames were created – one set with embedded bit-1 and another with embedded bit-0. This step facilitated the subsequent evaluation of the proposed encryption scheme's performance under different data embedding scenarios.The raw video signal from the acquired data was digitized into a time-series of RGB colour images using a video capture board. Each RGB colour image was then transformed into the YUV colour space, which separates the luminance (grayscale) information represented by the Y component from the chromatic (colour) information represented by the U and V channels. Additionally, a difference (D) image was computed by calculating the absolute value of the difference between consecutive frames. This D image captures the motion information within the video stream, highlighting moving objects.

Subsequently, the four image representations (YUVD) were successively subsampled at each time step, generating representations at lower and higher resolutions. This multi-resolution approach facilitated the analysis of the encryption scheme's performance across varying levels of detail and enabled the evaluation of computational efficiency trade-offs.The pre-processed video data, comprising the multi-resolution YUVD representations, served as the input for the encryption phase of the proposed cryptographic scheme.

3.2 Fast Fourier Transform (FFT)

To obtain the FFT coefficients of the frames, the Fast Fourier Transform (FFT) was applied to the image frame $I(x, y)$. Following application, the image features include the real part (x_n), imaginary part (C_k), magnitude value ($\omega(k)$), and phase angle $\left(\frac{2n+1}{2N}\pi k\right)$. FFT is fast, and the real part (x_k) of the obtained coefficients increased its efficiency. The Fast Fourier Transform (FFT) is as follows:

$$C_k = \frac{2}{N}\omega(k)\sum_{n=0}^{N-1} x_n Cos\left(\frac{2n+1}{2N}\pi k\right), \qquad 0 \le k \le N-1 \quad (3.1)$$

$$x_k = \sum_{k=0}^{N-1} C_k Cos\left(\frac{2n+1}{2N}\pi k\right), \qquad 0 \le n \le N-1 \quad (3.2)$$

As a researcher, I would rewrite the section on "Advanced Encryption Standard (AES)" as follows:

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1717594

3.3 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric-key algorithm that operates on a column-major order matrix of bytes. The encryption and decryption processes follow a series of well-defined steps, as outlined below:

Encryption Process:

Step 1: Derive a set of round keys from the cipher key using the key expansion algorithm.

Step 2: Initialize the state array with the block of plaintext data.

Step 3: Add the initial round key to the starting state array using an XOR operation.

Step 4: Perform the tenth and final round of state manipulation, which consists of the following operations:

SubBytes: A non-linear substitution step that replaces each byte with another according to a predefined substitution table (S-box).

ShiftRows: A transposition step that cyclically shifts the bytes in each row by a certain offset.

MixColumns:A linear mixing operation that combines the bytes in each column using a fixed polynomial multiplication over the Galois Field (GF(2^8)).

AddRoundKey: An XOR operation that combines the current state with the corresponding round key.

Step 5:Copy the final state array as the encrypted data (ciphertext)

The decryption process follows the inverse operations of encryption in reverse order, using inverse functions like InvSubBytes, InvShiftRows, and InvMixColumns. The round keys are applied in reverse order, starting from the last round key.

3.4 Video Compression and AES-FFT Integration

To address the high dimensionality and spatial redundancies inherent in video data, a hybrid approach was adopted, integrating the Fast Fourier Transform (FFT) with the Advanced Encryption Standard (AES) algorithm. Specifically, the frames of bands extracted from each video file were decomposed using the FFT, facilitating the extraction of motion vectors for efficient compression of the frames before subjecting them to the AES transformation.

After the FFT decomposition, the inverse FFT was applied, and the resulting coefficients were used as modification factors in the ShiftRowsand MixColumns operations of the AES algorithm. The basic structure of this modification process is depicted in Figure 3.

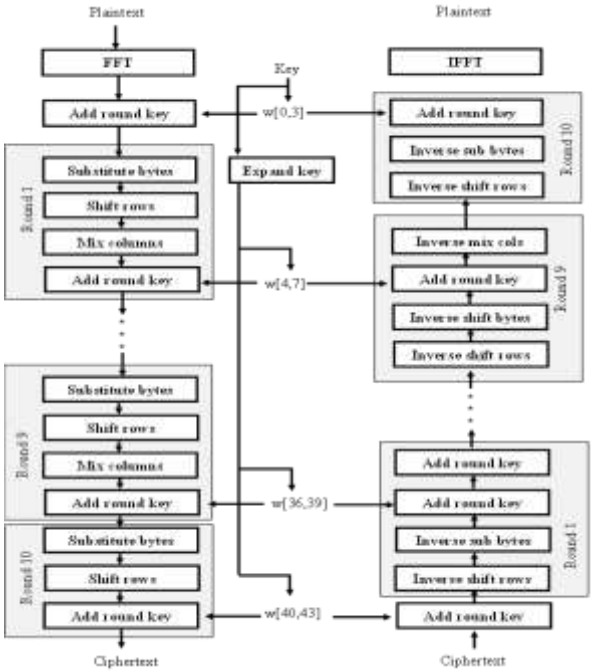

Figure 3: Basic Structure of AES-FFT

ShiftRows Modification:

The ShiftRows operation was modified based on the parity of the element at the first row and first column of the state matrix. If this element was even, the first and fourth rows remained unchanged, while each byte in the second and third rows of the state was cyclically shifted right by a different number of positions. Conversely, if the element was odd, the first and third rows remained unchanged, and each byte in the second and fourth rows was cyclically shifted right by a different number of positions.

MixColumns Modification:

In the original AES algorithm, the MixColumns operation operates on each column of the state matrix independently. Each column is treated as a four-term polynomial over the finite field GF(2^8), and it is multiplied modulo (x^4 + 1) with a fixed polynomial a(x) = {03}x^3 + {01}x^2 + {01}x + {02}.

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1717594

In the modified AES-FFT approach, after obtaining the state matrix from the ShiftRows step, the rows and columns were interchanged. This transposition was followed by the application of the standard MixColumns operation on the transposed matrix.

3.5 Implementation of the Video Encryption

The developed technique for secure digital video encryption and decryption using the AES-FFT approach was implemented using MATLAB R2018a,. The experiments were conducted on a Windows 10 Enterprise 64-bit Operating System, equipped with an Intel Pentium® CPU T4500 @ 2.30GHz Central Processing Unit, 4GB RAM, and a 500GB hard disk drive.The implementation process encompassed several stages, including video data loading, pre-processing, encryption, and decryption.

IV. RESULT AND DISCUSSION

This section presents the results obtained from the implementation and evaluation of the developed AES-FFT technique, which aimed to achieve improved data hiding, encryption, and decryption for digital video security. The experiments were conducted using two widely-used video formats: AVI and MP4. The AVI video format comprised 200 frames, while the MP4 video format consisted of 402 frames.The performance of the proposed AES-FFT technique was analyzed and compared with the conventional AES algorithm in terms of encryption and decryption times. Table 2 summarizes the obtained results for both video formats.

For the AVI video format, the AES-FFT technique demonstrated significantly faster encryption times, requiring only 0.5356 milliseconds (ms) to encrypt all frames, compared to 1.8552 ms for the AES technique. Similarly, the decryption process was accelerated, with the AES-FFT technique achieving a decryption time of 0.5204 ms, while the AES technique required 1.8408 ms for the same task.The performance advantage of the AES-FFT technique was also evident in the MP4 video format. The encryption time for all frames was 0.2363 ms, substantially lower than the 1.5360 ms required by the AES technique. Likewise, the decryption time for the AES-FFT technique was 0.2200 ms, outperforming the AES technique, which took 1.5185 ms to decrypt all frames.

Table 2: Performance based on Encryption and Decryption Time

Video Format	Encryption Time (ms)		Decryption Time (ms)	
	AES	AES-FFT	AES	AES-FFT
AVI	1.8552	0.5354	1.8408	0.5204
MP4	1.5360	0.2363	1.5185	0.2200

These results demonstrate the effectiveness of the proposed AES-FFT technique in achieving faster encryption and decryption times compared to the conventional AES algorithm. The integration of the Fast Fourier Transform (FFT) with the AES algorithm, along with the modifications to the ShiftRows and MixColumns operations, contributed to the observed performance improvements. In several video applications, fast processing speed and real-time effects are crucial requirements, as highlighted by Liu *et al.* (2020). The faster encryption and decryption times achieved by the AES-FFT technique can potentially enable more efficient and responsive video security solutions, particularly in real-time or time-sensitive scenarios.

The performance of an encryption technique is critically evaluated based on its encryption and decryption times, where shorter durations are desirable for efficient operations (Kansal and Mittal, 2014; Maqsood *et al.,* 2017). The proposed AES-FFT technique demonstrated superior performance compared to the conventional AES algorithm in terms of encrypting and decrypting video files.Notably, the encryption and decryption times for the MP4 video format were shorter than those for the AVI video format. This observation can be attributed to the inherent structural differences between these video formats, as highlighted by Alattar *et al.* (1999). Consequently, the AES-FFT technique exhibited faster processing speeds, a crucial requirement for many video applications that demand real-time effects and responsiveness.

The encryption and decryption time evaluations presented in Table 2 reveal that the integration of the Fast Fourier Transform (FFT) with the Advanced Encryption Standard (AES) algorithm resulted in a significant reduction in processing times for both the

AVI and MP4 video formats. This improvement can be attributed to the efficient compression capabilities of the FFT, which helped mitigate the computational overhead associated with the AES technique when handling complex multimedia data, such as video (Suresh and Dhanapathi, 2016; Hameed *et al.,* 2018).Figures 4a and 4b provide graphical representations of the encryption and decryption time performances, respectively, for the AES and AES-FFT techniques. These visual aids clearly illustrate the superior performance of the proposed AES-FFT approach, substantiating the effectiveness of the hybrid technique in achieving faster encryption and decryption times compared to the conventional AES algorithm.

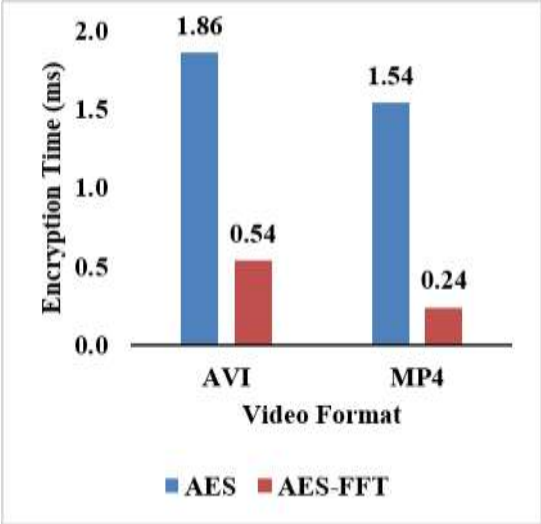

Figure 4a: Encryption Time

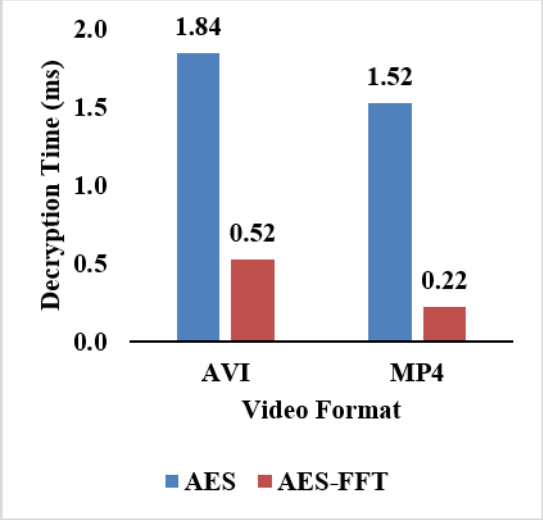

Figure 4b: Encryption Decryption Time

The reduced processing times achieved by the hybrid approach have the potential to enable more efficient and responsive video security solutions, particularly in real-time or time-sensitive applications (Lian*et al.,* 2008; Tsakanikas and Dagiuklas,2018).The performance enhancements achieved through the integration of FFT with AES can potentially enable more seamless and secure video transmission, storage, and processing in various domains, such as multimedia communication, surveillance systems, and content distribution networks (Liu *et al.,* 2020; Oguntoye*et al.,* 2023).

To further substantiate the performance improvements observed with the AES-FFT technique, an inferential statistical analysis was conducted using a paired-sample t-test. This analysis aimed to determine the level of significance in the performance difference between the AES-FFT and AES techniques for encryption and decryption times.

The null hypothesis (H0) stated that there is no significant difference between the AES-FFT and AES encryption techniques, while the alternative hypothesis (H1) posited a significant difference between the two techniques. The hypotheses were tested at a 5% level of significance, as suggested by Tabachnick and Fidell (2013).

Table 3: Summary of T-test Result for AES and AES-FFT technique

Parameter	t	Degree of Freedom *(df)*	p-value	Comment
Encryption and Decryption Time	-215.808	3	0.000	Significant

The results of the paired-sample t-test, presented in Table 3, revealed a p-value of 0.000 for the encryption time at a 95% confidence level. Since the p-value (0.000) is less than the α-value (0.05), the null hypothesis is rejected, and the alternative hypothesis is accepted, in line with the decision criteria

established by Hosmer *et al.* (2013). This inferential statistical analysis provides quantitative evidence to support the observed performance improvements achieved by the AES-FFT technique over the conventional AES algorithm. The integration of the Fast Fourier Transform (FFT) with AES resulted in a statistically significant reduction in encryption time, highlighting the efficacy of the proposed hybrid approach in addressing the computational challenges associated with multimedia data encryption (Alattar *et al.,* 1999; Kansal & Mittal, 2014).

The statistical significance of the results not only substantiates the practical implications of the AES-FFT technique but also strengthens the theoretical foundation for exploring and developing advanced encryption techniques that utilized the synergies between signal processing and cryptographic methodologies (Maqsood *et al.,* 2017; Gupta*et al.,* 2023; Atanda*et al.,* 2023).

From a theoretical perspective, this study contributes to the existing body of knowledge by demonstrating the feasibility and advantages of integrating signal processing techniques, such as the Fast Fourier Transform, with cryptographic algorithms like AES. The hybrid approach not only addresses the computational challenges associated with multimedia data encryption (Alattar *et al.,* 1999; Kansal and Mittal, 2014) but also opens up avenues for further exploration and optimization of multimedia security solutions (Maqsood *et al.,* 2017).The theoretical implications extend beyond the specific domain of video encryption, as the principles and methodologies employed in this study can potentially be adapted and applied to other multimedia formats or security applications (Jiang*et al.,* 2024;Kheddar*et al.,* 2024). Furthermore, the study paves the way for future research in developing advanced encryption techniques that utilise the strengths of various signal processing and cryptographic algorithms, ultimately enhancing the security and efficiency of multimedia data protection (Hameed *et al.,* 2018; Suresh and Dhanapathi, 2016).

V. CONCLUSION, RECOMMENDATION AND FUTURE WORK

5.1 Conclusion

This research aimed to develop an efficient and secure encryption technique for digital video data, addressing the computational challenges associated with multimedia data encryption and decryption. The proposed AES-FFT technique integrated the Fast Fourier Transform (FFT) with the Advanced Encryption Standard (AES) algorithm, using the efficient compression capabilities of FFT to mitigate the computational overhead of AES when handling video data.

The experimental results demonstrated the superior performance of the AES-FFT technique in achieving faster encryption and decryption times compared to the conventional AES algorithm. For both AVI and MP4 video formats, the AES-FFT technique exhibited significantly reduced processing times, with encryption times. These improvements were attributed to the effective integration of FFT with AES, along with modifications to the ShiftRows and MixColumnsoperations.Inferential statistical analysis using a paired-sample t-test further substantiated the performance differences between the AES-FFT and AES techniques, revealing a statistically significant reduction in encryption time achieved by the proposed approach. The AES-FFT technique can potentially enable more efficient and responsive video security solutions, particularly in time-sensitive scenarios.

5.2 Recommendation

Based on the research findings and conclusions, the following recommendations are proposed:

1. Implement the AES-FFT technique in real-world video security applications to evaluate its performance under diverse operational conditions and resource constraints.
2. Conduct further investigations to assess the security robustness and potential vulnerabilities of the AES-FFT technique, ensuring its suitability for practical deployment in critical applications.
3. Explore the integration of the AES-FFT technique with other multimedia security mechanisms, such as watermarking or steganography, to develop comprehensive multimedia protection solutions.
4. Investigate the scalability and adaptability of the AES-FFT technique for different video resolutions, bit rates, and compression formats to broaden its applicability.

5.3 Future Work

The current research focused on the encryption and decryption aspects of the proposed cryptographic scheme using the AES-FFT technique. However, to achieve a comprehensive solution for digital video security, future work should address the full implementation of the Cryptographic Scheme, which involves the integration of steganographic techniques.Specifically, the DWT-MPSO (Discrete Wavelet Transform-Modified Particle Swarm Optimization) technique will be employed for embedding and extracting the stego object (encrypted video data). The combination of the AES-FFT technique for encryption/decryption and the DWT-MPSO technique for data hiding and extraction can provide an efficient authentication mechanism for proof of ownership and copy control of multimedia content.Future research efforts should focus on the seamless integration of these techniques, optimizing the overall performance and ensuring the security robustness of the complete Cryptographic Scheme. Additionally, extensive testing and evaluation under various real-world scenarios and multimedia formats should be conducted to validate the practical applicability and scalability of the proposed solution.

VI. ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the Tertiary Education Trust Fund (TETFund) for their generous sponsorship and support in attending the prestigious IBII Conference 2024. Their commitment to fostering academic excellence and promoting research endeavours has been invaluable in facilitating the dissemination of our findings to the broader scientific community.

REFERENCES

[1] Abaas, S. A., &Shibeeb, A. K. (2015). A new approach for video encryption based on modified AES algorithm. *IOSR J. Comput. Eng*, *17*(3), 2278-661.

[2] Abolade, J. O., Konditi, D. B., Mpele, P. M., Orimogunje, A. M., & Oguntoye, J. P. (2022). Miniaturized dual-band antenna for gsm1800, wlan, and sub-6 ghz 5g portable mobile devices. *Journal of Electrical and Computer Engineering*, *2022*.

[3] Agaian, S. S., & Caglayan, O. (2006). Fast encryption method based on new FFT representation for the multimedia data system security. In *2006 IEEE International Conference on Systems, Man and Cybernetics*. 2, 1519-1524.

[4] Alattar, A. M., Al-Regib, G. I., and Al-Semari, S. A. (1999). Improved selective encryption techniques for secure transmission of MPEG video bit-streams. In *Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348)*: 256-260.

[5] Atanda, O. G., Ismaila, W., Afolabi, A. O., Awodoye, O. A., Falohun, A. S., & Oguntoye, J. P. (2023). Statistical Analysis of a Deep Learning Based Trimodal Biometric System Using Paired Sampling T-Test. In *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)*. 1, 1-10.

[6] Daemen, J., &Rijmen, V. (2002). Security of a wide trail design. In *International Conference on Cryptology in India*. 1-11.

[7] Dalal, M., & Juneja, M. (2021). A survey on information hiding using video steganography. *Artificial Intelligence Review*, *54*(8), 5831-5895.

[8] Dumbere, D. M., &Janwe, N. J. (2014). Video encryption using AES algorithm. In *Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014*. 332-337.

[9] Freitas, D. (1994). The Fight Against Piracy.http://www.ipa-uie.org/copyright/copyrightpub/freitas.html

[10] Gaton, A. U. and Geetha, D. D. (2019). A Empirical Study of Security Issues in Encryption Techniques. *International Journal of Applied Engineering Research*. 14(5), 1049-1061.

[11] Gupta, M., Singh, V. P., Gupta, K. K., & Shukla, P. K. (2023). An efficient image encryption technique based on two-level security for internet

of things. *Multimedia Tools and Applications*, *82*(4), 5091-5111.

[12] Hafsa, A., Fradi, M., Sghaier, A., Malek, J., &Machhout, M. (2022). Real-time video security system using chaos-improved advanced encryption standard (IAES). *Multimedia Tools and Applications*, 1-24.

[13] Hameed, M. E., Ibrahim, M. M., & Abd Manap, N. (2018). Review on improvement of advanced encryption standard (AES) algorithm based on time execution, differential cryptanalysis and level of security. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1), 139-145.

[14] Hameed, M. E., Ibrahim, M. M., and Abd Manap, N. (2018). Review on improvement of advanced encryption standard (AES) algorithm based on time execution, differential cryptanalysis and level of security. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1), 139-145.

[15] Hameed, M. E., Ibrahim, M. M., and Abd Manap, N. (2018). Review on improvement of advanced encryption standard (AES) algorithm based on time execution, differential cryptanalysis and level of security. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1), 139-145.

[16] Hosmer Jr, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). *Applied logistic regression*. John Wiley & Sons.

[17] Jiang, D., Tsafack, N., Boulila, W., Ahmad, J., & Barba-Franco, J. J. (2024). ASB-CS: Adaptive sparse basis compressive sensing model and its application to medical image encryption. *Expert Systems with Applications*, *236*, 121378.

[18] Kadam, K. S., & Deshmukh, A. (2016). Video frame encryption algorithm using AES. *International Journal of Engineering Research*, *5*(6), 588-591.

[19] Kansal, S., and Mittal, M. (2014). Performance evaluation of various symmetric encryption algorithms. In *2014 international conference on parallel, distributed and grid computing*. 105-109.

[20] Kheddar, H., Hemis, M., Himeur, Y., Megías, D., & Amira, A. (2024). Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. *Neurocomputing*, 127528.

[21] Lian, S., Sun, J., Liu, G., & Wang, Z. (2008). Efficient video encryption scheme based on advanced video coding. *Multimedia Tools and Applications*, *38*, 75-89.

[22] Liu, K., Liu, W., Ma, H., Tan, M., and Gan, C. (2020). A real-time action representation with temporal encoding and deep compression. *IEEE Transactions on Circuits and Systems for Video Technology*, *31*(2), 647-660.

[23] Liu, Q., Safavi-Naini, R., and Sheppard, N. P. (2003). Digital rights management for content distribution. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume* 21, 49-58.

[24] Malgieri, G. (2018). 'User-provided personal content' in the EU: digital currency between data protection and intellectual property. *International Review of Law, Computers & Technology*, *32*(1), 118-140.

[25] Maqsood, F., Ahmed, M., Ali, M. M., and Shah, M. A. (2017). Cryptography: A comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*, *8*(6), 442-448.

[26] Nnamani, Sunday N. (2016), Effects of Music Piracy on the Nigerian Public: A Case Study of Enugu Urban. *World Journal of Social Sciences and Humanities*. Science and Education Publication (SciEP). 2(1), 15-19.

[27] Oguntoye, J. P., Awodoye, O. O., Oladunjoye, J. A., Faluyi, B. I., Ajagbe, S. A., &Omidiora, E. O. (2023). Predicting COVID-19 From Chest X-Ray Images using Optimized Convolution Neural Network. *LAUTECH Journal of Engineering and Technology*, *17*(2), 28-39.

[28] Okediran, O. O., &Oguntoye, J. P. (2023). Analysis of critical success factors for information security management performance. *LAUTECH Journal of Engineering and Technology*, *17*(1), 175-186.

[29] Okolie, C. (2023). Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns. *Journal of International Women's Studies*, *25*(2), 11.

[30] Parmar, N. J., & Verma, P. K. (2017). A comparative evaluation of algorithms in the implementation of an ultra-secure router-to-router key exchange system. *Security and communication networks*, *2017*.

[31] Rao, N.N., Thrimurthy, P. and Babu, B.R. (2009). A Novel Scheme for Digital Rights Management of Images Using Biometrics', *IJCSNS International Journal of Computer Science and Network Security,* 9(3):157 – 167.

[32] Sarker, M. I. H., Khan, M. I., Deb, K., & Faruque, M. F. (2012). FFT-based audio watermarking method with a gray image for copyright protection. *International Journal of Advanced Science and Technology*, *47*, 65-76.

[33] Suresh, M. and Dhanapathi, J. (2016). Memory Efficient Fft Computation with Error Tolerance Sdc-Sdf Architecture. *International Conference on Emerging Trend in Engineering and Management Research.* 63-69.

[34] Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2013). *Using multivariate statistics* (Vol. 6, pp. 497-516). Boston, MA: pearson.

[35] Tade, O., and Mmahi, O. P. (2018). Movie Piracy Networks at Alaba International Market, Lagos, Nigeria. *International journal of offender therapy and comparative criminology*, *62*(1), 274-285.

[36] Tsakanikas, V., &Dagiuklas, T. (2018). Video surveillance systems-current status and future trends. *Computers & Electrical Engineering*, *70*, 736-753.

[37] Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., &Zareei, M. (2022). Towards security automation in software defined networks. *Computer Communications*, *183*, 64-82.