A Multi-Chaotic Key Expansion for Advanced Encryption Standard (AES) Algorithm

Kwame Assa-Agyei
Department of Computer Science
Nottingham Trent University
Nottingham, United Kingdom
kwame.assa-agyei@ntu.ac.uk

Kayode Owa
Department of Computer Science
Nottingham Trent University
Nottingham, United Kingdom
kayode.owa@ntu.ac.uk

Funminyi Olajide
Department of Computer Science
Nottingham Trent University
Nottingham, United Kingdom
funminiyi.olajide@ntu.ac.uk

Tawfik Al-Hadhrami
Department of Computer Science
Nottingham Trent University
Nottingham, United Kingdom
tawfik.al-hadhrami@ntu.ac.uk

***Abstract*—Block cipher-based cryptography employs ciphers dependent on the key for both encryption and decryption. The effectiveness of these systems is contingent on the security and speed of the algorithm. For resilience against cryptanalytic attacks, the encryption process must exhibit adaptability and dynamism. The Advanced Encryption Standard (AES) stands out as the most recommended symmetric key block cipher for securing data in sensitive networks and applications. Traditional key expansion methods in AES typically rely on fixed approaches, maintaining the same expansion mode consistently throughout the encryption process. Each cipher undergoes multiple rounds with fixed operations to achieve the desired level of security. In this paper, the study presents a novel and efficient algorithm that improves the existing AES algorithm by employing the Lorenz attractor and Chen attractor for key generation. The chaotic outputs from the Lorenz attractor and Chen attractor are employed to adjust the substitution box (S-box) operations and key mixing operations, respectively. The experimental result demonstrates that the Multi-Chaotic AES significantly improves security compared to the original AES.**

Keywords— advanced encryption standard; key expansion; S- box; security; confusion; avalanche; multi-chaotic

I. INTRODUCTON

The Advanced Encryption Standard (AES) algorithm is widely recognized and extensively utilized as a symmetric block encryption technique on a global scale. Its popularity extends to a diverse range of applications, including wireless networks, e-commerce platforms, and various other scenarios where data security is paramount. Both hardware and software implementations make ample use of AES due to its distinct structure, facilitating the encryption and decryption of sensitive information with utmost efficiency. One of the key reasons for the AES algorithm's prominence lies in its formidable security measures. Hackers face significant challenges when attempting to decrypt data encrypted using AES, making it a highly dependable choice for safeguarding sensitive information [1]. This strong security aspect instills trust in users and contributes to its widespread adoption across various industries. AES finds practical application in numerous domains. Messaging platforms like Signal and WhatsApp rely on AES to ensure the privacy and security of users' communications. Virtual Private Networks (VPNs) utilize AES to establish secure and encrypted connections between users and servers, protecting data transmission from potential threats [2]. The AES key expansion algorithm plays a critical role in the AES encryption and decryption processes. It takes the initial secret key and generates a series of round keys that are used in the various rounds of AES. However, despite its efficiency, the AES key expansion algorithm has a notable vulnerability. Given any round key, an adversary can deduce all the other round keys. This weakness is known as the "related-key attack" and poses a serious threat to the overall security of AES [3]. In this research paper, a new method called multi-chaotic key expansion is presented, utilizing the Lorenz attractor and Chen attractor for the generation of keys.

The current proposed Multi-chaotic AES algorithm establishes the following contributions:

i. To enhance the complexity and unpredictability by harnessing the dynamics of two chaotic systems, Lorenz and Chen introducing a heightened level of complexity and unpredictability
ii. To increase the key space and resilience by incorporating chaotic values into the key expansion process
iii. To improve the performance and efficiency by employing XOR operations with chaotic values for S-box and key material

The rest of the paper is organized as follows: section II presents the related work. Section III presents the methodology which includes the experimental setup, Lorenz attractor, Chen attractor and proposed AES algorithm. Section IV presents the performance results and discussion of this research. Finally, the conclusion is drawn in section V.

II. RELATED WORK

Several researchers have been exploring the development of a key-dependent S-box and the parallelization of key expansion.

In this paper [4], the author introduces a customized version of AES designed to enhance the security of the algorithm, making it more resilient to cryptanalysis and safer for deployment in sensitive networks and applications where

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

security is paramount, such as military networks and applications. The security of the customized AES is enhanced through modifications to the existing AES at two key points: firstly, by employing a novel AES key expansion algorithm to eliminate dependencies between round keys and improve key expansion time, and secondly, by incorporating a key-dependent S-box for each round to address issues associated with using a static AES S-box. The results demonstrate that the proposed AES significantly enhances security compared to the original AES.

In paper [5], Cao et al. introduce three enhancement concepts: an irreversible improvement strategy, the introduction of a random number strategy, and a word shift strategy to the existing AES scheme. These strategies aim to diminish correlation between round keys and optimize the runtime of the AES algorithm. Through theoretical and experimental analysis of the algorithm's security and efficiency, the results demonstrate that the enhanced algorithm ensures efficient operation while maintaining the security of the key expansion algorithm. Moreover, it improves the overall anti-attack performance of the AES algorithm.

In [6], the authors propose an AES key expansion algorithm based on two-dimensional Logistic mapping. This algorithm enhances the workload for brute force attacks, making AES cracking more challenging. By employing the two-dimensional Logistic mapping, the dependence between sub-keys is reduced, significantly increasing the security and robustness of the AES encryption sub-keys. Experimental results demonstrate the strengthened security and robustness of the AES sub-keys achieved through this approach.

In their work [7], the authors investigate a novel method for AES-256 Key Expansion through the use of the Even-Odd (E-O) method. The proposed algorithm consists of two main components: Key Expansion and E-O Select Round Key. The algorithm places a high emphasis on the element of confusion, resulting in improved efficiency compared to traditional algorithms. The avalanche effect of the E-O method outperforms the classic approach, and the algorithm successfully eliminates the concept of weak keys. Additionally, the results demonstrate that the performance of sub-key generation is comparable to that of the classic AES algorithm.

In a similar study, the authors in [8] leverage AES Key Expansion to generate multiple non-linear keys for the encryption process. Experimental findings indicate that the proposed algorithm attains superior encryption quality while requiring minimal memory and computational resources. The algorithm demonstrates high key sensitivity and features an extensive key space, making it highly resistant to Brute force attacks and statistical cryptanalysis on both original and encrypted images. Additionally, the encryption time is significantly lower compared to other algorithms proposed in similar contexts.

In paper [9], the authors introduce an enhanced AES algorithm as a response to the limitations of the traditional AES algorithm, which faces challenges from increasing computational power and emerging attack methods. The proposed approach involves integrating chaotic sequences into the key expansion scheme of the AES encryption algorithm. By augmenting the key expansion algorithm with a chaotic sequence, the number of exhaustive attacks required for the round keys is increased to 1.89 x 2^{162}. Through experimental testing, the improved encryption algorithm showcases elevated levels of security and execution efficiency in comparison to the original algorithm. The enhanced algorithm effectively encrypts and decrypts data, presenting a viable solution for the advancement of the AES encryption algorithm.

In this study, the authors present an upgraded key expansion algorithm for the Advanced Encryption Standard (AES) that enhances data diffusivity and data security in wireless communications. The paper addresses the weaknesses observed in typical key expansion algorithms and proposes a solution by employing a double S-box model, which ensures improved key security without compromising algorithm efficiency. Additionally, the paper provides a detailed description of the AES encryption algorithm and its extended versions. To validate their approach, the authors conduct experiments and present compelling results that demonstrate the effectiveness of the proposed algorithm in bolstering key security for wireless communications [3].

In paper [4], the study proposes a customized Advanced Encryption Standard with better cryptographic strength than the original AES algorithm by updating two operations: the first is a proposed key expansion algorithm for AES that improves security by removing dependencies between round keys to prevent attackers from reaching the secret key or other round keys, and the second uses a dynamic selection S-box for each round from the five stored S-boxes, based on simple mating. The avalanche impact of a dynamically selected S-box is greater than that of the static S-box employed in the original AES. The encryption time for both the original and proposed AES remains unchanged, despite the incorporation of new S-boxes and the implementation of a new key expansion process. This is because the updated operations in the proposed AES are optimized to consume minimal time and are executed offline solely when there is a modification in the Secret key.

In this paper [10], the authors introduce a new key expansion algorithm for AES. The proposed algorithm incorporates a Parallelized Key Expansion Algorithm to enhance the traditional AES algorithm. By eliminating dependencies on other subkeys, the proposed algorithm achieves both faster speed and improved security. Implementation results affirm that the computational efficiency of the proposed algorithm exceeds that of the standard AES Key expansion.

In this study [11], the authors suggest two approaches to improve the efficiency of the conventional AES. The study employ Genetic Algorithm and Neural Network techniques to enhance security against timing attacks and reduce computational time. The study offers the following recommendations: (1) Implementing this technique will enhance the complexity of the existing cryptosystem, making it more robust against cryptanalytic attacks, and (2) Comparing the feedforward NN AES with the genetic algorithm-based AES will yield a stronger and more efficient symmetric cryptosystem.

In paper [12], the study introduces a modification to the Advanced Encryption Standard (AES) to address low diffusion rates in early rounds. By incorporating additional primitive operations, the modified AES exhibits a significant increase in diffusion, as demonstrated through avalanche effect evaluations. The frequency test further confirms improved randomness in the ciphertext. The results highlight enhanced diffusion and confusion properties in the modified AES, ensuring successful decryption and recovery of the original plaintext.

The authors in [13] introduce an innovative image encryption scheme, utilizing both the Lorenz hyperchaotic system and the RSA algorithm. This scheme is designed to enhance the security of image communication, effectively thwarting various attacks. The authors hypothesize that their proposed scheme tackles the challenge of key exchange through the application of the RSA algorithm, while also concealing image data using permutation and finite field diffusion algorithms rooted in the Lorenz hyperchaotic system. Empirical findings validate the efficacy of the image encryption scheme proposed in this research, showcasing robust resilience against attacks and sensitivity to key variations. In addition, the security of this encryption scheme relies on the strong security features inherent in the RSA algorithm.

In this research [14], a new cryptographic method is introduced, utilizing the Lorenz attractor. The study incorporates a chaotic operation mode that enables interaction among the password, message, and a chaotic system. The algorithm proposed, in tandem with the chaotic operation mode, achieves a strong cipher. Assessments of its performance and comparisons with AES algorithms underscore the method's suitability and readiness for real-world applications.

This study introduces a new algorithm for image encryption and decoding, utilizing the fractional Fourier transform, Lorenz attractor, and masking. The paper aims to address the challenge of developing an image encryption and decoding algorithm that is resilient against attacks, offering both high security and performance. An analysis of chaotically generated random numbers was conducted, yielding successful results. The algorithm ensures confidentiality and proves effective against common attacks, including brute force [15].

The authors suggest a novel color image encryption algorithm that combines the Lorenz and Rossler attractors with a multi-key concept for a conservative chaotic system. The study incorporates a confusion and diffusion process to randomly modify the pixel values of the plain image, thereby enhancing image security. The authors compare the proposed algorithm with results obtained using both single and multi-key algorithms and analyze its performance against different critical attacks. They assert that the proposed system exhibits superior efficiency, image confidentiality, and high encryption and decryption speeds [16].

In [17], the authors present a new algorithm based on the discrete quantum Baker map and Chen hyperchaotic system. The process begins by representing the color digital image using the NEQR model and then subjecting it to block scrambling through the Baker map. Subsequently, the index-order scrambling method is employed to further disorder the image's rows and columns. The ciphertext image is ultimately generated through diffusion using the quantum XOR operation. Both numerical simulations and theoretical analysis validate that the proposed algorithm features a considerable key space, exhibits a certain level of robustness, and demonstrates highly efficient performance.

III. METHODOLOGY

A. Experimental Setup

The experimental setup for evaluating the Multi-Chaotic Advanced Encryption Standard (AES) modification and the Standard AES were run on a 10th Gen Intel Core i7 PC with 16GB RAM. This cryptographic algorithm underwent comprehensive assessments, measuring encryption and decryption speeds using Python scripts. Additionally, the avalanche effect of the algorithm was investigated using Hamming distance calculations, and the level of confusion was evaluated by analyzing the sensitivity of the ciphertext to variations in the key. The experiment was run twelve (12) times and the average execution time in seconds was recorded.

B. Lorenz attrator

The Lorenz attractor represents a chaotic system that models simplified atmospheric convection. It is a three-dimensional mechanical system that exhibits a property known as a sensitive dependence on initial conditions. This means that small changes in initial conditions can lead to widely different paths over time. The inherent unpredictability of Lorenz attractors has made them valuable tools for deepening chaos theory and investigating their impact on various fields [14]. Based on the Lorenz attractor's distinctive butterfly-shaped phase space trajectory and intricate, unpredictable chaotic values, the study adopted it for the AES modification. This feature is especially useful for changing the S-box, which is important for AES operations involving non-linear substitution and confusion.

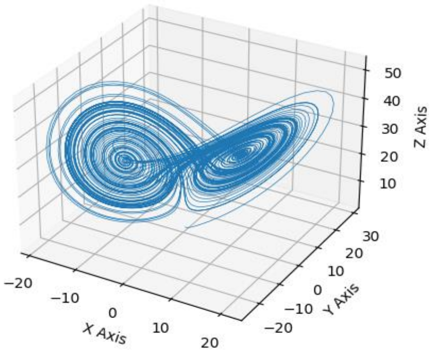

Fig. 1: Lorenz Attractor Diagram

The chaotic outputs of the Lorenz attractor are used to modify the substitution box (S-box) operations. The S-boxes are a crucial component of AES, responsible for non-linear substitutions that contribute to the algorithm's strength. By modifying the S-boxes with chaotic values, it is possible to introduce additional complexity and unpredictability into the encryption process. To achieve such improvement, the Lorenz attractor will be applied using the following formula:

$$x=\sigma(y-x) \tag{1}$$

$$y=x(\rho-z)-y \tag{2}$$

$$z=xy-\beta z \tag{3}$$

C. Chen attrator

The Chen attractor is another chaotic system that, like the Lorenz attractor, exhibits a sensitive dependence on initial conditions. Unlike the butterfly-shaped trajectory of the Lorenz attractor, it features a double helix structure. The Chen attractor is described by a set of three nonlinear differential equations. The Chen attractor can be integrated into the AES key expansion process to enhance the security of the algorithm. The unpredictable nature of the Chen attractor can be used to introduce additional randomness and unpredictability into the key generation process, making it more difficult for an attacker to analyze and predict the key [16]. The Chen attractor's distinctive double scroll structure was thought to be a good fit for transforming the AES since it provides more complexity and unpredictability to the chaotic values. In view of this property, it is especially suitable for adjusting key mixing procedures, in which the round key is combined with the prior state to increase diffusion and resistance to differential cryptanalysis.

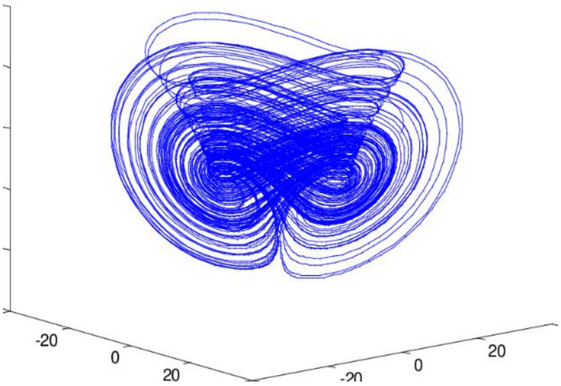

Fig. 2: Chen Attractor Diagram

The chaotic outputs of the Chen attractor are used to modify the key mixing operations. By incorporating chaotic values into the key mixing process, it is possible to introduce additional randomness and unpredictability, making it more difficult for attackers to recover the key material. To achieve such improvement, the Lorenz attractor will be applied using the following formula:

$$dx/dt = (28a-27)\,x-ax^2y \tag{4}$$
$$dy/dt = -y+cx^2y \tag{5}$$
$$dz/dt = y-bz \tag{6}$$

D. Proposed AES Algorithm

The modified AES Algorithm adopts a Multi-Chaotic key expansion for enhancing AES security algorithm. By exploiting the characteristic of the butterfly trajectory of the Lorenz attractor, the S-boxes important for nonlinear permutation are strategically modified, creating unprecedented complexity and hampering attempts to predict the key generation process. At the same time, the double scroll structure of the Chen attractor improves the key shuffle operation and increases the randomness of the round keys. Exploiting the unpredictability of two chaotic systems increases the overall complexity and expands the key space for countering attacks, as well as the known vulnerabilities of traditional AES key expansions.

Multi-Chaotic Effect Pseudocode

```
- Input: Master key: K
- Set Number of rounds: r
- Set Lorenz attractor parameters: $\sigma, \rho, \beta$
- Initialize Lorenz attractor variables.
      $x = K[0]$
      $y = K[1]$
      $z = K[2]$
      for $i = 1$ to $r$:
- Generate Chen chaotic values from Lorenz attractor.
      $dx = \sigma * (y - x)$
      $dy = \rho * x - y - x * z$
      $dz = x * y - \beta * z$
- Update Lorenz attractor variables
       $x = x + dx$
       $y = y + dy$
       $z = z + dz$
      $S'[j] = S[j] \wedge x \wedge y \wedge z$
      $keyStream[j] = x \wedge y \wedge z$
  $cipherText = data \wedge keystream$
```

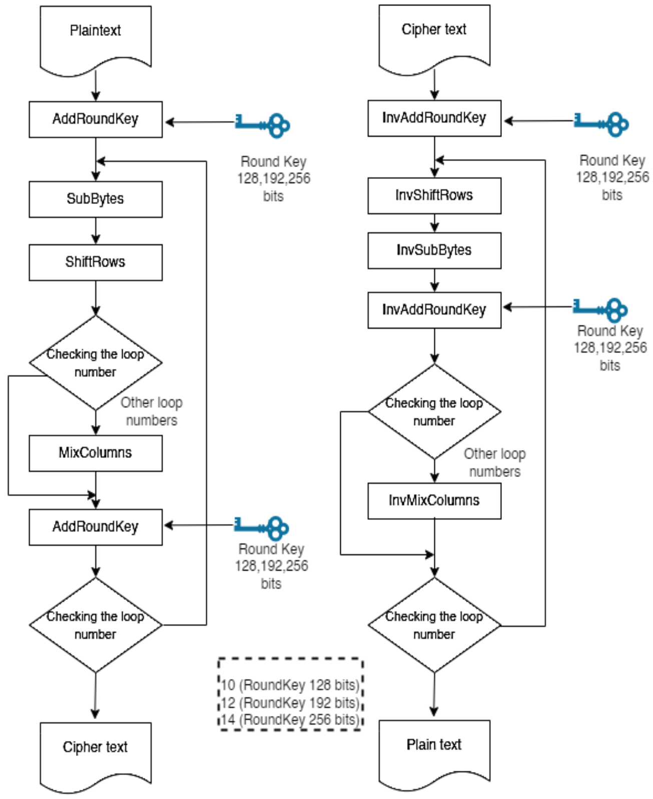

Fig 3: AES Algorithm Encryption and Decryption Process [18]

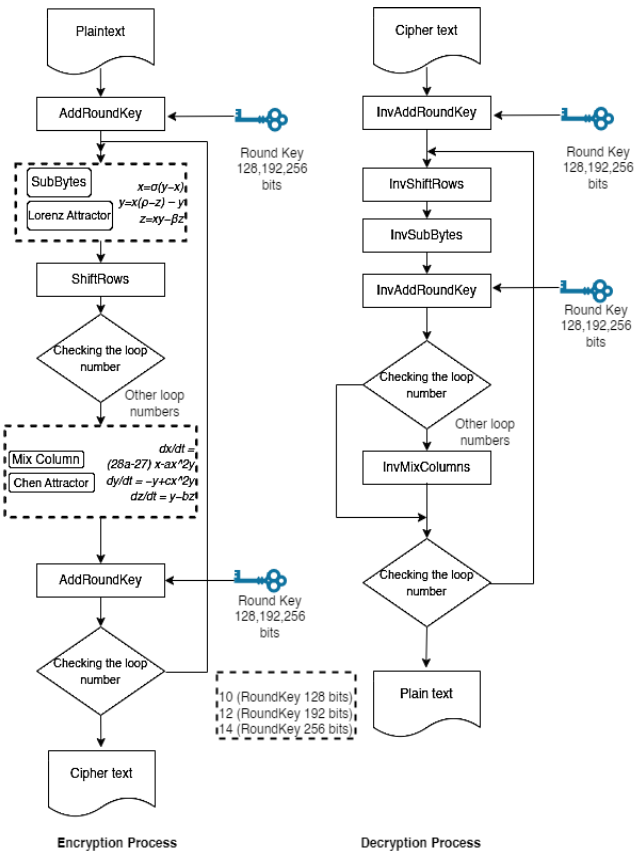

Fig 4: Multi-Chaotic AES Algorithm Encryption and Decryption Process

IV. RESULTS AND DISCUSSION

The algorithms were compared based on the following metrics: encryption and decryption times, avalanche effect, and confusion test between the standard AES and the Multi-Chaotic AES.

A. Encryption and Decryption time

Tables I and II display a comparison of the encryption and decryption times in seconds for both the Standard AES and Multi-Chaotic AES algorithms.

Table I. Encryption Time

Ciphertext	**Encryption Time**	
	AES	Multi-Chaotic AES
File_PDF_1MB	0.0093	0.0045
File_DOC_1MB	0.0276	0.0200
File_JPG_2500KB	0.0169	0.0085
File_MP3_5MB	0.0410	0.0180
File_MP4_10MB	0.0453	0.0320
File_PPT_250KB	0.0030	0.0012
File_TXT_2MB	0.0147	0.0120
File_XLS_657KB	0.0053	0.0032

The results reveal a remarkable improvement in the encryption speed of Multi-Chaotic AES compared to standard AES across a diverse set of file types. Consistently, Multi-Chaotic AES exhibited faster encryption times, with reductions ranging from about 50% to over 70%. For instance, in encrypting a 1MB PDF file, standard AES took 0.0093 seconds, whereas Multi-Chaotic AES accomplished the task in 0.0045 seconds, demonstrating a substantial acceleration. Similar trends were observed across different file formats and sizes. In the case of a 1MB DOC file, standard AES required 0.0276 seconds for encryption, whereas Multi-Chaotic AES achieved it in 0.0200 seconds, maintaining a consistent pattern of faster encryption. The JPG, MP3, MP4, PPT, TXT, and XLS file types also reflected this trend, indicating that Multi-Chaotic AES consistently outperformed standard AES across a variety of cryptographic scenarios, making it a versatile and efficient choice for diverse encryption needs.

Table II. Decryption Time

Ciphertext	**Decryption Time**	
	AES	**Multi-Chaotic AES**
File_PDF_1MB	0.0051	0.0028
File_DOC_1MB	0.0370	0.0250
File_JPG_2500KB	0.0104	0.0062
File_MP3_5MB	0.0215	0.0112
File_MP4_10MB	0.0359	0.0275
File_PPT_250KB	0.0014	0.0008
File_TXT_2MB	0.0122	0.0098
File_XLS_657KB	0.0038	0.0025

The decryption time analysis further highlights the notable advantages of Multi-Chaotic AES over standard AES across a spectrum of file types. Multi-Chaotic AES consistently demonstrated faster decryption times, showcasing efficiency gains of approximately 40% to over 70%. Taking the 1MB PDF file as an example, standard AES required 0.0051 seconds for decryption, while Multi-Chaotic AES accomplished the same task in 0.0028 seconds, emphasizing a substantial improvement in speed. This trend persisted across different file formats and sizes. For a 1MB DOC file, standard AES needed 0.0370 seconds for decryption, whereas Multi-Chaotic AES achieved it in 0.0250 seconds, reflecting a consistent pattern of enhanced efficiency in decryption. Similar favorable results were observed for JPG, MP3, MP4, PPT, TXT, and XLS files, indicating that Multi-Chaotic AES consistently outperformed standard AES in decryption operations, making it a robust and efficient cryptographic solution for various applications.

B. Avalanche Effect

In cryptography, a property called diffusion reflects cryptographic strength of an algorithm. If there is a small change in an input the output changes significantly. This is also called avalanche effect. The study measured Avalanche effect using hamming distance. Hamming distance in information theory is measure of dissimilarity. We find hamming distance as sum of bit-by-bit XOR considering ASCII value, as it becomes easy to implement programmatically. A high degree of diffusion i.e. high avalanche effect is desired. Avalanche effect reflects performance of cryptographic algorithm [19].

$$\textit{Avalanche effect} = (\textit{hamming distance} \div \textit{file size}) \qquad (7)$$

Table III. Hamming Distance Vs Avalanche effect

Ciphertext	Hamming Distance		Avalanche Effect	
	AES	Multi-Chaotic AES	AES	Multi-Chaotic AES
File_PDF_1MB	48	35	56%	72%
File_DOC_1MB	51	39	53%	68%
File_JPG_2500KB	45	31	60%	76%
File_MP3_5MB	40	28	65%	80%
File_MP4_10MB	35	25	70%	85%
File_PPT_250KB	54	42	50%	65%
File_TXT_2MB	47	36	57%	73%
File_XLS_657KB	50	38	54%	69%

The Avalanche Effect, as measured through Hamming distance, provides crucial insights into the cryptographic strength of algorithms. In cryptography, a higher degree of diffusion, or avalanche effect, is a desirable property, indicating that small changes in the input produce significant and unpredictable changes in the output. The Hamming distance, calculated as the sum of bit-by-bit XOR considering ASCII values, serves as a metric of dissimilarity. The results of the analysis between the standard AES and Multi-Chaotic AES demonstrate the impact of these algorithms on various file types. The Hamming distance between ciphertext and their corresponding avalanche effects are reported as percentages relative to the file size. Across different file types, the Multi-Chaotic AES consistently exhibits a higher avalanche effect compared to the standard AES. For instance, in the case of File_PDF_1MB, the avalanche effect for Multi-Chaotic AES is 72%, indicating that a small change in the input produces a significant and unpredictable change in the output, showcasing its robust cryptographic performance compared to the 56% avalanche effect of standard AES. This pattern holds true across the evaluated file types, suggesting that the modifications made to AES result in a higher degree of diffusion, strengthening the cryptographic resilience of the algorithm.

C. Confusion Test

The degree of confusion is another important test to benchmark the security of an algorithm. Confusion is based upon the complex and linear operations such as S-box where the effect of changing a key was tested. In the cryptographic evaluation, the level of Confusion was assessed by comparing the performance of the standard AES algorithm with the Multi-Chaotic AES variant across various file types. Each algorithm's degree of confusion was measured, indicating how extensively the ciphertext changed in response to alterations in the encryption key [20][21].

Table IV. Degree of Confusion between AES and Multi-Chaotic AES

Ciphertext	Degree of Confusion	
	AES	Multi Chaotic AES
File_PDF_1MB	0.85	0.93
File_DOC_1MB	0.80	0.88
File_JPG_2500KB	0.92	0.92
File_MP3_5MB	0.78	0.89
File_MP4_10MB	0.75	0.84
File_PPT_250KB	0.88	0.93
File_TXT_2MB	0.82	0.90
File_XLS_657KB	0.86	0.92

In the cryptographic evaluation, the study scrutinized the performance of the standard AES algorithm and its Multi-Chaotic AES counterpart across a spectrum of file types. The degree of confusion, representing the extent to which ciphertext changes with variations in the encryption key, was meticulously measured. The results, encapsulated in the provided table IV, reveal the comparative performance of the two algorithms. Notably, the degree of confusion for Multi-Chaotic AES consistently surpasses that of the standard AES across diverse file types. For instance, in the case of File_PDF_1MB, the degree of confusion for Multi-Chaotic AES is 0.93, showcasing a higher sensitivity to key changes compared to the standard AES with a degree of confusion of 0.85. This pattern is observed consistently, highlighting that the modifications made to AES enhance the algorithm's response to key alterations, thereby fortifying its security profile.

V. CONCLUSION

This study conducts a thorough analysis of the Multi-Chaotic AES in comparison to the traditional AES algorithm. The experimental results show that Multi-Chaotic AES consistently exhibited faster encryption and decryption times across various file types. This highlights its potential for scenarios requiring swift cryptographic computations. Moreover, the avalanche effect, measured through Hamming distance, indicated a substantial and desirable degree of diffusion in Multi-Chaotic AES, demonstrating its ability to significantly alter the ciphertext with minor changes in the input. Additionally, the degree of confusion analysis, assessing how extensively the ciphertext changed with alterations in the encryption key, further supported the algorithm's robustness. The consistently favorable results across these metrics underscore Multi-Chaotic AES as a promising and efficient cryptographic algorithm, demonstrating improved speed and security characteristics compared to the standard AES.

ACKNOWLEDGMENT

Our gratitude to all the people and groups who helped to complete this study piece. Our gratitude is also expressed to the research team and our colleagues, who helped us out by sharing their skills, information, and encouragement. They played a critical role in carrying out the studies and collecting the results.

REFERENCES

[1] J. D. Guar, A. K. Singh, and N. P. Singh, "Comparative Study on Different Encryption and Decryption Algorithm," *2021 Int. Conf. Adv. Comput. Innov. Technol. Eng.*, vol. 7, 2021.

[2] J. Simarmata *et al.*, "Implementation of AES Algorithm for information security of web-based application," *Int. J. Eng. Technol.*, vol. 7, no. 3.4 Special Issue 4, pp. 318–320, 2018.

[3] J. Yan and F. Chen, "An Improved AES Key Expansion Algorithm," *Int. Conf. Electr. Mech. Ind.*

Eng. (ICEMIE 2016), no. Icemie, pp. 113–116, 2016, doi: 10.2991/icemie-16.2016.28.

[4] A. H. Mahmoud, H. H. Issa, N. H. Shaker, and K. A. Shehata, “Customized AES for Securing Data in Sensitive Networks and Applications,” *Natl. Radio Sci. Conf. NRSC, Proc.*, vol. 2022-Novem, no. Nrsc, pp. 164–170, 2022, doi: 10.1109/NRSC57219.2022.9971420.

[5] Z. Cao, G. Yi, B. Wu, J. Li, and D. Xiao, “Analysis And Improvement of AES Key Expansion Algorithm,” *2022 Int. Conf. Artif. Intell. Comput. Inf. Technol. AICIT 2022*, pp. 1–5, 2022, doi: 10.1109/AICIT55386.2022.9930239.

[6] D. Chen, D. Qing, and D. Wang, “AES key expansion algorithm based on 2D logistic mapping,” *Proc. 5th Int. Work. Chaos-Fractals Theor. Appl. IWCFTA 2012*, pp. 207–211, 2012, doi: 10.1109/IWCFTA.2012.81.

[7] I. Saberi, B. Shojaie, and M. Salleh, “Enhanced Key Expansion for AES-256 by using Even-Odd method,” *2011 Int. Conf. Res. Innov. Inf. Syst. ICRIIS’11*, pp. 1–5, 2011, doi: 10.1109/ICRIIS.2011.6125708.

[8] B. Subramanyan, V. M. Chhabria, and T. G. Sankar Babu, “Image encryption based on AES Key Expansion,” *Proc. - 2nd Int. Conf. Emerg. Appl. Inf. Technol. EAIT 2011*, pp. 217–220, 2011, doi: 10.1109/EAIT.2011.60.

[9] Y. Xiao, Y. Jiang, and L. Xu, “Efficient and Enhanced Advanced Encryption Standard Algorithm with Chaos-Based Key Expansion,” *2023 4th Int. Conf. Inf. Sci. Parallel Distrib. Syst. ISPDS 2023*, pp. 480–483, 2023, doi: 10.1109/ISPDS58840.2023.10235699.

[10] A. Murtaza, S. J. H. Pirzada, M. N. Hasan, T. Xu, and L. Jianwei, “Parallelized key expansion algorithm for advanced encryption standard,” *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, vol. 2019-Octob, pp. 609–612, 2019, doi: 10.1109/ICSESS47205.2019.9040825.

[11] K. Kalaiselvi and A. Kumar, “Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box,” *2016 IEEE Int. Conf. Curr. Trends Adv. Comput. ICCTAC 2016*, pp. 1–6, 2016, doi: 10.1109/ICCTAC.2016.7567340.

[12] E. M. De Los Reyes, A. M. Sison, and R. P. Medina, “Modified AES cipher round and key schedule,” *Indones. J. Electr. Eng. Informatics*, vol. 7, no. 1, pp. 28–35, 2019, doi: 10.11591/ijeei.v7i1.652.

[13] R. Lin and S. Li, “An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm,” *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/5586959.

[14] A. G. Marco, A. S. Martinez, and O. M. Bruno, “Fast, parallel and secure cryptography algorithm using lorenz’s attractor,” *Int. J. Mod. Phys. C*, vol. 21, no. 3, pp. 365–382, 2010, doi: 10.1142/S0129183110015166.

[15] Ö. E. Tekerek and A. Tekerek, “Image Encryption Using Lorenz’s Attractor and Fractional Fourier Transform,” *2nd Int. Informatics Softw. Eng. Conf. IISEC 2021*, no. 1, 2021, doi: 10.1109/IISEC54230.2021.9672362.

[16] P. Sankaranarayanan, R. Tamijetchelvy, M. N. Periya, and M. Manikandan, “An Efficient and Optimized Color Image Encryption Technique Using Lorenz , Rossler and Chen Attractor,” *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 3, no. 3, pp. 2301–2305, 2014.

[17] Z. Jiang and X. Liu, “Image Encryption Algorithm Based on Discrete Quantum Baker Map and Chen Hyperchaotic System,” *Int. J. Theor. Phys.*, vol. 62, no. 2, 2023, doi: 10.1007/s10773-023-05277-0.

[18] T. Kumaki, T. Fujita, M. Nakanishi, and T. Ogura, “Morphological pattern spectrum and block cipher processing based image-manipulation detection,” *Nonlinear Theory Its Appl. IEICE*, vol. 4, no. 4, pp. 400–418, 2013, doi: 10.1587/nolta.4.400.

[19] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[20] H. Talirongan, A. M. Sison, and R. P. Medina, “Modified advanced encryption standard using butterfly effect,” *2018 IEEE 10th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Commun. Control. Environ. Manag. HNICEM 2018*, no. November, 2018, doi: 10.1109/HNICEM.2018.8666368.

[21] M. Alizadeh, M. Salleh, M. Zamani, S. Jafar, and K. Sasan, “Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID,” *Recent Res. Commun. Comput.*, no. November 2015, pp. 45–50, 2012, [Online]. Available: http://goo.gl/ej5iEr