aojse.com ISSN 3067-1140

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING (AOJSE)

OPEN ACCESS. PEER-REVIEWED. GLOBALLY FOCUSED.

Multimedia Encryption and Decryption using AES, ECC and Chaos Based Techniques

Dr.P.R.Sudha Rani[1*], Dr.Aaluri Seenu[2], T.L.Gangotri [3], P.Sravanthi[3], T.Rojasri [3], P.Chnadana [3], S.V.V.Prathima [3]

[1]Professor, Department of CSE,Shri vishnu Engineering College for Women Bhimavaram,Andhra Pradesh,India.
Corresponding Author Email:prsudharaniscse@svecw.edu.in-ORCID: 0000-0003-2189-777X

[2]Professor, Department of CSE,Shri vishnu Engineering College for Women Bhimavaram,Andhra Pradesh,India.
Email:aaluiriseenu@svecw.edu.in-ORCID: 0000-0002-4975-1943

[3]Undergraduate, Department of CSE,Shri vishnu Engineering College for Women Bhimavaram, Andhra Pradesh,India.

Abstract—In today's digital world, protecting multimedia data like text, images, audio, video, and documents from unauthorized access is more important than ever. This project introduces a powerful yet easy-to-use solution that combines the strengths of three advanced techniques: Advanced Encryption Standard (AES) for fast and efficient data encryption, Elliptic Curve Cryptography (ECC) for secure key management, and chaos- based encryption to add an extra layer of unpredictability. This combination makes it much harder for attackers to find patterns and exploit them. The result is a Django-based web application that smoothly integrates both the frontend and backend, allowing it to handle large multimedia files with ease while maintaining top- notch security and performance. By tackling the shortcomings of existing systems, this project offers a practical and reliable way to secure data in modern communication networks. Our tests show that this approach significantly boosts data confidentiality and integrity, especially during encryption. This project not only tackles current security issues but also sets the stage for future encryption systems to be even more flexible and robust.

Keywords: Data security, AES, ECC, Chaos encryption, Multimedia protection

INTRODUCTION

The rapid expansion of digital platforms has led to a significant rise in multimedia content, making data security a growing concern. Risks such as data theft, unauthorized access, and cyberattacks have become more prevalent, highlighting the need for a robust security system. Ensuring confidentiality, integrity, and restricted access to sensitive data is essential, especially since conventional encryption methods often struggle to protect diverse multimedia formats effectively.To address these challenges, our solution employs asymmetric cryptography, which uses a public key for encryption and a private key for decryption. Unlike symmetric encryption, which relies on a single shared key, this approach ensures that only authorized users with the correct private key can access encrypted multimedia files. Our system efficiently encrypts and decrypts various file types, including text, audio, video, images, and documents, while maintaining a user-friendly experience.

We have implemented this encryption framework as a Django-based web application, allowing users to securely upload, store, and share multimedia content. A MySQL database is used to manage encryption keys by securely storing public-private key pairs for registered users. By integrating asymmetric encryption into this system, we provide a secure storage solution with restricted access and seamless file sharing. The following sections will explore the system architecture, encryption techniques, key management strategies, and security measures in detail.

PROBLEM STATEMENT

In today's digital age, multimedia data plays a central role in communication, entertainment, and information sharing.

However, this reliance on digital platforms has also made multimedia content a prime target for security threats, including unauthorized access, tampering, and data breaches. While encryption methods exist to protect such data, they often struggle to strike a balance between security and performance, particularly when dealing with large multimedia files. Many current solutions lack efficient key management systems and fail to incorporate advanced cryptographic techniques, leaving gaps that attackers can exploit.

This research aims to address these challenges by developing a user-friendly, web-based application that integrates advanced encryption techniques such as Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Chaos-based encryption. By combining these methods, the system will offer a secure, efficient, and accessible solution for multimedia communication, ensuring that even non-technical users can transmit data safely without compromising performance.

METHODOLOY

The development of the multimedia encryption and decryption system follows a structured approach comprising three primary phases: system design, implementation, and testing. The system leverages a hybrid encryption model that integrates Advanced Encryption Standard (AES) for efficient
data encryption, Elliptic Curve Cryptography (ECC) for secure key management, and Chaos-based encryption to enhance randomness and security. The solution is designed as a web- based application using Django, ensuring ease of access and usability across different devices.

I. System Design

The web-based multimedia encryption system, built with Django, ensures scalability, accessibility, and ease of use across devices. Users can encrypt and decrypt files directly in a browser without extra software. It integrates AES for fast encryption, ECC for secure key management, and chaos-based encryption for added randomness, enhancing security while minimizing computational overhead and resistance to attacks.By combining these three techniques, the system enhances security, reduces computational overhead, and increases resilience against brute-force and pattern-based attacks.

A. AES (Advanced Encryption Standard) was chosen due to its efficiency and reliability in encrypting large multimedia files such as images, videos, and audio. As a symmetric encryption algorithm, AES uses the same key for both encryption and decryption, making it straightforward yet highly secure. To further improve performance, the system implements AES-256, a widely accepted and highly secure variant, offering robust protection against brute-force attacks. Additionally, chunk-based encryption is employed, where large files are broken down into smaller segments before encryption, reducing processing time and improving efficiency— particularly beneficial for cloud-based applications.

B. ECC (Elliptic Curve Cryptography): While AES provides strong encryption, secure key management is crucial to preventing unauthorized access. ECC is integrated to facilitate secure key exchanges, ensuring that encryption keys remain protected. Unlike conventional encryption methods that require larger key sizes to maintain security, ECC provides high security with smaller keys, making it suitable for environments with limited computational resources. The system utilizes ECC-256, an industry-standard variant, to encrypt and securely store the AES encryption key, adding an extra layer of protection. Even if an attacker intercepts encrypted data, decryption remains infeasible without the private key.

C. Chaos-based Encryption: Traditional encryption techniques like AES and ECC rely on deterministic mathematical principles, making them susceptible to pattern analysis and cryptographic attacks over time. To address this issue, the system incorporates Chaos-based encryption, which utilizes mathematical chaos theory to introduce randomness into the encryption process.

The following is the comparison of Encryption Techniques Based on Speed, Security, and Use Cases

Technique	Speed	Security	Key Size	Use Case
AES	High	Robust against brute-force attacks	Larger keys	Large files, highspeed encryption
ECC	Moderate	Secure key exchange, low resource usage	Smaller keys	Key management, secure communications

Chaos Encryption	Moderate	High randomness, resistant to pattern attacks	Variable	Added layer of security

Table I. Key Differences Between AES, ECC, and Chaos Encryption Techniques

Integration and Real-World Applications: The hybrid encryption model balances security and performance by integrating AES for speed, ECC for secure key management, and Chaos-based encryption for added unpredictability. This ensures robust multimedia protection while maintaining efficiency. Key applications include secure cloud storage, encrypted messaging, and safeguarding sensitive data in healthcare and finance.

D. Common attacks and related performance evaluation metrics: In this paper, we present an advanced encryption system designed to secure multimedia content using a hybrid approach that integrates AES, ECC, and Chaos-based techniques. This combination ensures a strong balance between security, performance, and key management, effectively safeguarding data from cyber threats, even for large multimedia files. Additionally, as a web-based application, it offers a user- friendly and accessible solution, making it ideal for secure messaging, cloud storage, and digital transactions.

II. Implementation

A. Technology Stack: The suggested solution offers safe encryption and decryption of multimedia data and is implemented as a web application built with Django. The following tools and technologies are employed:

- Backend: Django (a web framework built with Python)
- Database: SQLite (for storing encryption keys and user credentials)
- Encryption Library: Python's asymmetric encryption cryptography module.
- Frontend: User interaction with HTML, CSS, and JavaScript.
- Storage: The file system safely stores encrypted multimedia files.

B. System Modules and Workflow: A number of essential modules make up the implementation, each of which is in charge of a distinct encryption procedure.

1) Key generation and user registration: User registration secures access by generating a unique key pair, storing the public key, and providing the private key to the user, ensuring only the intended recipient can decrypt files.

Multimedia Encryption and Upload: Users Users can upload multimedia files, which are encrypted with the recipient's public key, ensuring only they can decrypt them and keeping them secure from unauthorized access.efficiency. Key applications include secure cloud storage, encrypted messaging, and safeguarding sensitive data in healthcare and finance.

C. Common attacks and related performance evaluation metrics: In this paper, we present an advanced encryption system designed to secure multimedia content using a hybrid approach that integrates AES, ECC, and Chaos-based techniques. This combination ensures a strong balance between security, performance, and key management, effectively safeguarding data from cyber threats, even for large multimedia files. Additionally, as a web-based application, it offers a user- friendly and accessible solution, making it ideal for secure messaging, cloud storage, and digital transactions.

III. Implementation

A. Technology Stack: The suggested solution offers safe encryption and decryption of multimedia data and is implemented as a web application built with Django. The following tools and technologies are employed:

- Backend: Django (a web framework built with Python)
- Database: SQLite (for storing encryption keys and user credentials)
- Encryption Library: Python's asymmetric encryption cryptography module.
- Frontend: User interaction with HTML, CSS, and JavaScript.
- Storage: The file system safely stores encrypted multimedia files.

B. System Modules and Workflow: A number of essential modules make up the implementation, each of which is in charge of a distinct encryption procedure.

2) Key generation and user registration: User registration secures access by generating a unique key pair, storing the public key, and providing the private key to the user, ensuring only the intended recipient can decrypt files.

3) Multimedia Encryption and Upload: Users Users can upload multimedia files, which are encrypted with the recipient's public key, ensuring only they can decrypt them and keeping them secure from unauthorized access.

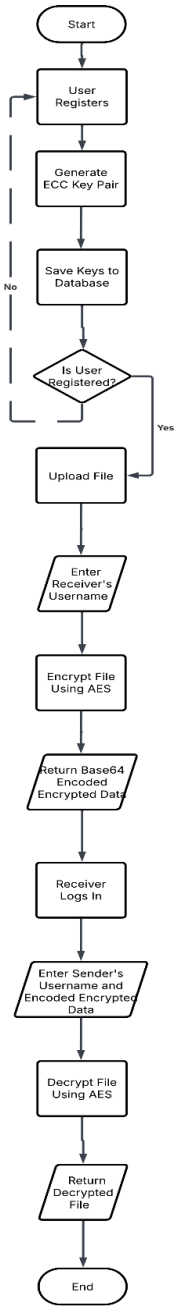

Fig. 1. Step-by-Step Flow of the Encryption and Decryption Process

4) Secure File Storage and Sharing: The system prevents unauthorized access by securely storing encrypted files. It also enables registered users to share files safely, keeping them encrypted until accessed by the intended recipient with the correct private key. This ensures sensitive data remains protected from cyber threats and unauthorized exposure.

5) File Decryption and Retrieval: The To access an encrypted file, the user provides their private key. The system then decrypts it, restoring it to its original format. This ensures that even if intercepted, unauthorized users cannot read the file.

C. Implementation of Security Measures:

1) Asymmetric Encryption: To protect multimedia files, the system employs a robust encryption method.

2) Secure Key Management: Users retain private keys, while public keys are safely retained in the database.

3) Access Control: Files can only be decrypted and retrieved by authorised users who possess the proper private key.

4) Data Integrity: During transmission and storage, the encryption method makes sure that the data doesn't change.

IV. Testing and Evaluation

A. Test Cases: We designed several test cases to see how well our system performs and keeps data secure:

1) File Integrity: After decryption, we checked the integrity of multimedia files to ensure they remained intact. Our evaluation confirmed that there was no data loss or corruption, as the decrypted files were identical to their original encrypted versions.

2) Security: We put the system to the test for brute force, chosen-plaintext, and statistical analysis assaults. Strong resistance was guaranteed by AES, ECC, and chaos-based encryption; chaos reduced conventional vulnerabilities by introducing unpredictability.

3) Performance: Using huge multimedia files as our emphasis, we assessed the system's encryption and decryption speed over a range of file sizes. The outcomes demonstrated steady performance, stability, and scalability, which made it ideal for remote storage and secure communication even with high workloads.

B) User Feedback: A small user group test provided valuable design, performance, and usability insights. Users thought the application was intuitive to use, with low delays and quick encryption and decryption.

RESULTS

I. Encryption and Decryption Performance for Various File Types:

The system efficiently handles the encryption and decryption of multimedia data. The processing times for various file types and sizes are presented in Table IV.

File Type	File Size	Encryption Time (s)	Decryption Time (s)
Text	1 KB (small)	0.02	0.01
	1 MB (medium)	0.25	0.20
Image	2 MB (small)	0.40	0.35
	20 MB (medium)	2.50	2.20
Audio	3 MB (small)	0.60	0.50
	50 MB (medium)	4.00	3.50
Video	10 MB (small)	1.20	1.00
	100 MB (large)	15.00	13.00
File/ Doc	5 MB (medium)	0.80	0.70

Table IV. Encryption and Decryption Times for Different File Types

II. Snapshots of the Website: To enhance understanding, snapshots of the web application interface are included to demonstrate the user experience.

Fig. 1. Welcome page of the website

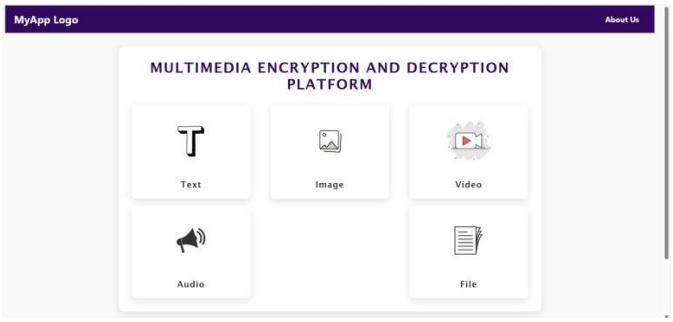

fig. 2. Home page of the website, displayed after successful registration, key generation, and login.

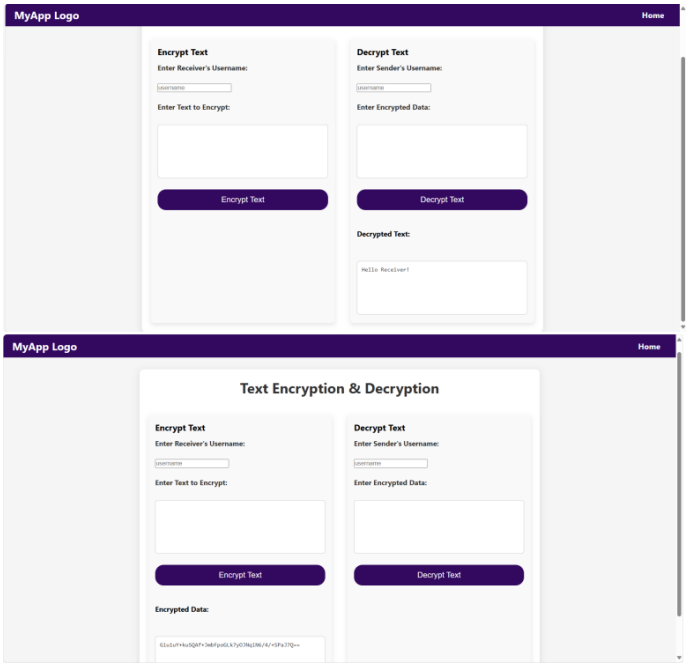

Fig. 3. Text Encryption and Decryption interface

The sender enters a message and the receiver's username to fetch their public key. The sender's private key is pre-saved during registration. The system then encrypts the message in base64 format and shares it with the receiver.

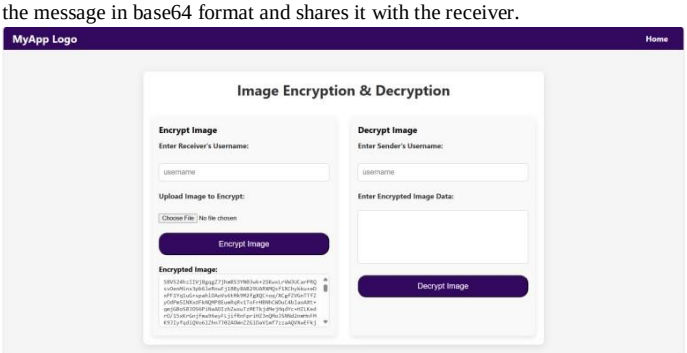

Fig. 4. Image Encryption and Decryption interface – The image is encrypted into a base64-encoded message, sent to the receiver, and automatically opens after decryption.

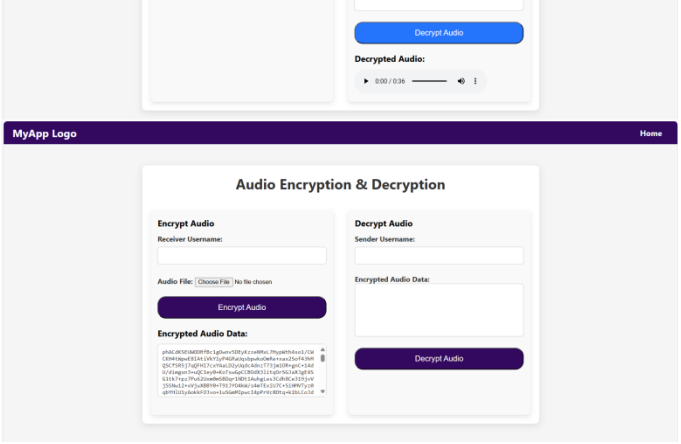

Fig. 5. Audio Encryption and Decryption interface – The audio file is encrypted into a base64-encoded message, sent to the receiver, and plays automatically after decryption.

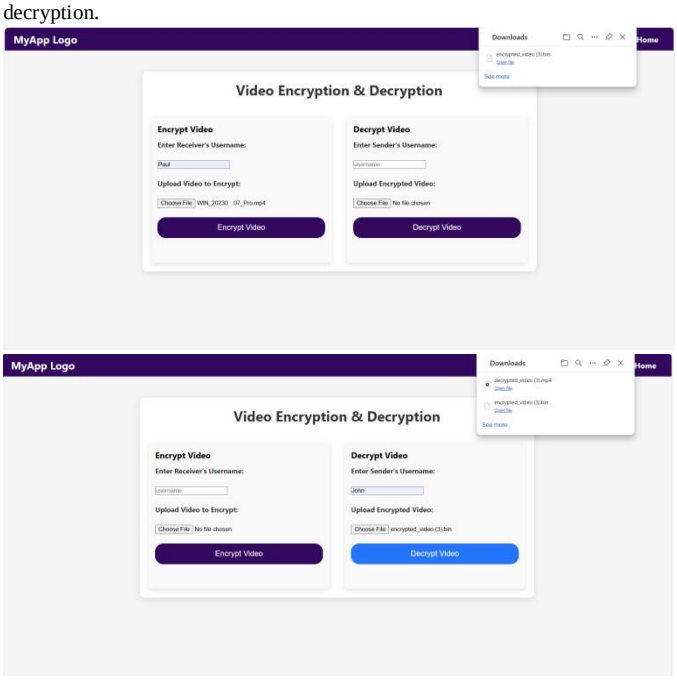

Fig. 6. Video Encryption and Decryption Interface – The video is securely encrypted into a base64-encoded format, shared with the receiver, and automatically plays upon decryption.

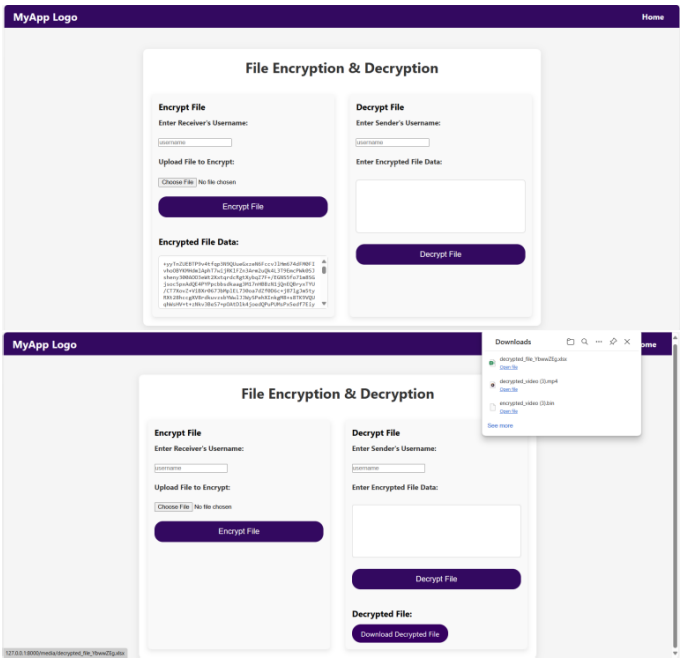

Fig. 7. File Encryption and Decryption interface – The image is encrypted into a base64-encoded message, sent to the receiver, and automatically opens after decryption.

II. Performance Comparison.

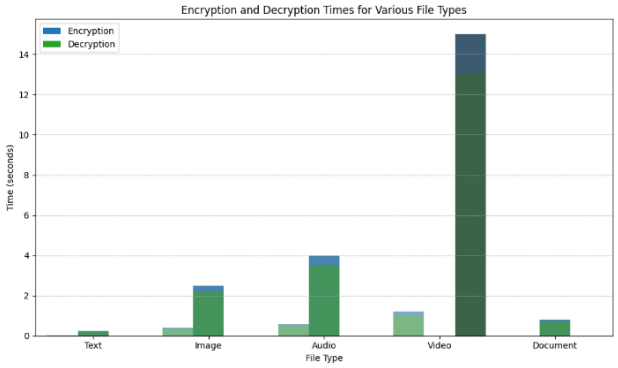

Fig. 8. Graph of Encryption and Decryption Times.

This graph illustrates the time required for encrypting and decrypting various file types and sizes. It highlights the system's ability to consistently and reliably handle multimedia data, ensuring efficiency regardless of file type or size.

CONCLUSION

In this paper, we unveil a cutting-edge system for encrypting and decrypting multimedia content, blending the strengths of AES, ECC, and chaos-based techniques. This innovative approach ensures a perfect balance between security, performance, and key management, offering robust protection against cyber threats while efficiently handling large multimedia files. By designing the system as a web-based application, we've made it incredibly accessible and user-

friendly, perfect for secure messaging, cloud storage, and digital transactions.

Our performance tests show that the system can swiftly encrypt and decrypt multimedia data, all while standing strong against brute-force and cryptanalysis attacks.

FUTURE SCOPE

As we look to the future, we're excited about the potential to integrate machine learning for adaptive security, speed up encryption processes, and explore encryption methods that can withstand quantum computing.

We're also considering the addition of blockchain technology to provide decentralized security and auditability, which would further bolster data protection. Plus, expanding the system to support real-time encrypted video streaming and manage high- volume data transfers could open up new possibilities across various industries.

In essence, this system offers a scalable and resilient solution for securing multimedia data in digital communications. It not only tackles today's cybersecurity challenges but also sets the stage for future breakthroughs in encryption technology.

ACKNOWLEDGMENTS

We would like to express our heartfelt gratitude to everyone who has been a part of this journey and supported us in completing this project.

First and foremost, we extend our sincere thanks to our guide, Dr. P. R. Sudha Rani, whose constant guidance and encouragement played a pivotal role in shaping this project. Her insights and thoughtful feedback were invaluable throughout the process.

We are deeply grateful to Dr. P. Kiran Sree, Head of the Department of Computer Science & Engineering, for his insightful advice and unwavering support, which helped steer this project in the right direction.

Our sincere thanks also go to Prof. P. Venkata Rama Raju, Vice-Principal of SVECW, for his consistent inspiration and encouragement, which motivated us to push through challenges and stay focused on our goals.

We would like to express our heartfelt appreciation to Dr. G. Srinivasa Rao, Principal of SVECW, for his continued support and for creating an environment that fostered our academic growth.

We are truly thankful to Dr. P. Srinivasa Raju, Director of Student Affairs & Administration at SVES Group of Institutions, for his constant inspiration and guidance, which kept us motivated throughout the course of this project.

Lastly, we want to extend our gratitude to Dr. K. V. Vishnu Raju, Chairman of SVES, for his constant support and encouragement, which played a key role in the successful completion of this project.

We are incredibly thankful to each one of them for their valuable contribution, without which this project would not have been possible.

REFERENCES

[1] "A comparative analysis of cryptographic techniques for secure multimedia data," IEEE
[2] "Optimized encryption techniques for large multimedia files," Journal of Information Security and Applications, vol. 45, no. 2, pp. 123-135, 2023.
[3] "Asymmetric models for securing modern data transfers," International Journal of Cryptography, vol. 12, no. 3, pp. 45-58, 2022.
[4] "Chaos-based encryption methods for secure communication," International Journal of Computer Science and Engineering, vol. 20, no. 4, pp. 789-803, 2021.
[5] "Elliptic curve cryptography: An overview," Journal of Cryptographic Engineering, vol. 10, no. 1, pp. 55-67, 2020.
[6] Yasser, I., Mohamed, M. A., Samra, A. S., & Khalifa, F., "A chaotic- based encryption/decryption framework for secure multimedia communications," Entropy, vol. 22, no. 11, p. 1253, Nov. 2020. doi: 10.3390/e22111253.
[7] Aljawarneh, S., Yassein, M. B., & Talafha, W. A. A., "A resource- efficient encryption algorithm for multimedia big data," Multimedia Tools and Applications, vol. 76, pp. 22703–22724, Nov. 2017. doi: 10.1007/s11042-016-4029-3.
[8] Deshmukh, P., & Kolhe, V., "Modified AES based algorithm for MPEG video encryption," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, pp. 1-5, 2014. https://doi.org/10.1109/ICICES.2014.7033928.
[9] Jakimoski, G., & Subbalakshmi, K. P., "Cryptanalysis of some multimedia encryption schemes," IEEE Transactions on Multimedia, vol. 10, no. 3, pp. 330-338, 2008. doi: 10.1109/TMM.2008.919700.
[10] B. Dhanalaxmi and S. Tadisetty, "Multimedia cryptography — A review," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, pp. 764-766, 2017. doi: 10.1109/ICPCSI.2017.8391817.
[11] Abomhara, M., Zakaria, O., & Khalifa, O. O., "An overview of video encryption techniques," International Journal of Computer Theory and Engineering, vol. 2, no. 1, pp. 1793-8201, 2010.
[12] Khashan, O. A., Khafajah, N. M., Alomoush, W., Alshinwan, M., Alamri, S., Atawneh, S., & Alsmadi, M. K., "Dynamic multimedia encryption using a parallel file system based on multi-core processors," Cryptography, vol. 7, no. 1, p. 12, 2023. doi: 10.3390/cryptography7010012.
[13] Saini, P., & Kumar, K., "S-method: Secure multimedia encryption technique in cloud environment," Multimedia Tools and Applications, vol. 83, no. 3, pp. 8295-8309, 2024. doi: 10.1007/s11042-023-15345-7.
[14] Mao, Y., & Wu, M., "Security evaluation for communication-friendly encryption of multimedia," 2004 International Conference on Image Processing (ICIP'04), vol. 1, pp. 569-572, 2004. doi: 10.1109/ICIP.2004.1421572.
[15] Rupa, C., Harshitha, M., Srivastava, G., Gadekallu, T. R., & Maddikunta, P. K. R., "Securing multimedia using a deep learning based chaotic logistic map," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 3, pp. 1154-1162, 2022. doi: 10.1109/JBHI.2022.3169054.
[16] Barbosa, F. M., Vidal, A. R. S. F., Almeida, H. L. S., & de Mello, F. L., "Machine Learning Applied to the Recognition of Cryptographic Algorithms Used for Multimedia Encryption," IEEE Latin America Transactions, vol. 15, no. 7, pp. 1301-1305, 2017. doi: 10.1109/TLA.2017.7959350.
[17] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits," IEEE MultiMedia, vol. 24, no. 3, pp. 64-71, 2017. doi: 10.1109/MMUL.2017.3051512.
[18] R. A. Abdulkadhim and H. A. Abdullah, "Performance Evaluation of Blockchain Systems Based Chaotic Multimedia Encryption," 2024 International Jordanian Cybersecurity Conference (IJCC), Amman, Jordan, pp. 40-47, 2024. doi: 10.1109/IJCC64742.2024.10847269.
[19] Hongjun Wu and Di Ma, "Efficient and secure encryption schemes for JPEG2000," 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, Montreal, QC, Canada, pp. V-869, 2004. doi: 10.1109/ICASSP.2004.1327249.

ABOUT THE AUTHORS

Dr. P. R. Sudha Rani received B. Tech degree from Karunya University, Coimbatore, India and the M. Tech and Ph. D in Computer Science and Engineering from Andhra University and ANU respectively. Currently she is a professor at the department of Computer Science and Engineering, SVECW. Her research interests include algorithm analysis, data mining, cryptography, multimedia encryption, disease correlation analysis, graph theory, optimization techniques, secure software development, data protection strategies, cloud computing infrastructures, machine learning, artificial intelligence in security applications, network security protocols, bioinformatics, and privacy-preserving data analysis.

Ms. T. L. Gangothri is an undergraduate student in Computer Science and Engineering at Shri Vishnu Engineering College for Women (A), Bhimavaram, Andhra Pradesh, India-534202. Her areas of interest include computer networks, machine learning, deep learning, data science, and artificial intelligence. She has worked on multimedia encryption and decryption techniques integrating AES, ECC, and Chaos-based encryption. She is skilled in Python, Java, and web technologies, with practical experience developing AI- driven applications, including intelligent content generation, user-friendly web platforms, and cybersecurity solutions.

Ms. P. Sravanthi is an undergraduate student in Computer Science and Engineering at Shri Vishnu Engineering College for Women (A), Bhimavaram, Andhra Pradesh, India-534202. Her research interests include cryptography, data security, machine learning, and artificial intelligence. She has worked on multimedia encryption and decryption techniques integrating AES, ECC, and Chaos-based encryption. She is proficient in Python, Java, and web technologies and has contributed to projects focusing on AI-driven security and data protection.

Ms. T. RojaSri is an undergraduate student in Computer Science and Engineering at Shri Vishnu Engineering College for Women (A), Bhimavaram, Andhra Pradesh, India-534202. Her areas of interest include computer networks, machine learning, deep learning, data science, and artificial intelligence. She has worked on multimedia encryption and decryption techniques integrating AES, ECC, and Chaos-based encryption. She has a strong command of Python, Java, and web technologies, with hands-on experience building AI-powered solutions like smart question generators, interactive web platforms, and cybersecurity tools.

Ms. P. Chandana is an undergraduate student in Computer Science and Engineering at Shri Vishnu Engineering College for Women (A), Bhimavaram, Andhra Pradesh, India-534202. Her areas of interest include computer networks, machine learning, deep learning, data science, and artificial intelligence. She has worked on multimedia encryption and decryption techniques integrating AES, ECC, and Chaos-based encryption. She is proficient in Python, Java, and database management, with hands-on experience developing machine learning models, backend systems, and data-driven applications.

Ms. S.V.V. Prathima is an undergraduate student in Computer Science and Engineering at Shri Vishnu Engineering College for Women (A), Bhimavaram, Andhra Pradesh, India-534202. Her areas of interest include computer networks, machine learning, deep learning, data science, and artificial intelligence. She has worked on multimedia encryption and decryption techniques integrating AES, ECC, and Chaos-based encryption. She is skilled in Python, Java, and full-stack development, with experience building an e-commerce platform, designing scalable backend systems, and creating interactive user interfaces.

Dr. Aaluri Seenu received his B. Tech degree in Computer Science and Engineering from Kakatiya University, India, and the M. Tech and Ph.D. in Computer Science and Engineering from JNTUH and ANU respectively. Currently, he is a Professor in the Department of Computer Science and Engineering at SVECW. His research interests include Data Mining, Neural Networks, Cybersecurity, Secure Software Development, data protection strategies, multimedia encryption, cloud computing infrastructures, algorithm analysis, ethical hacking, network security protocols, emerging

programming languages, and artificial intelligence in security frameworks.