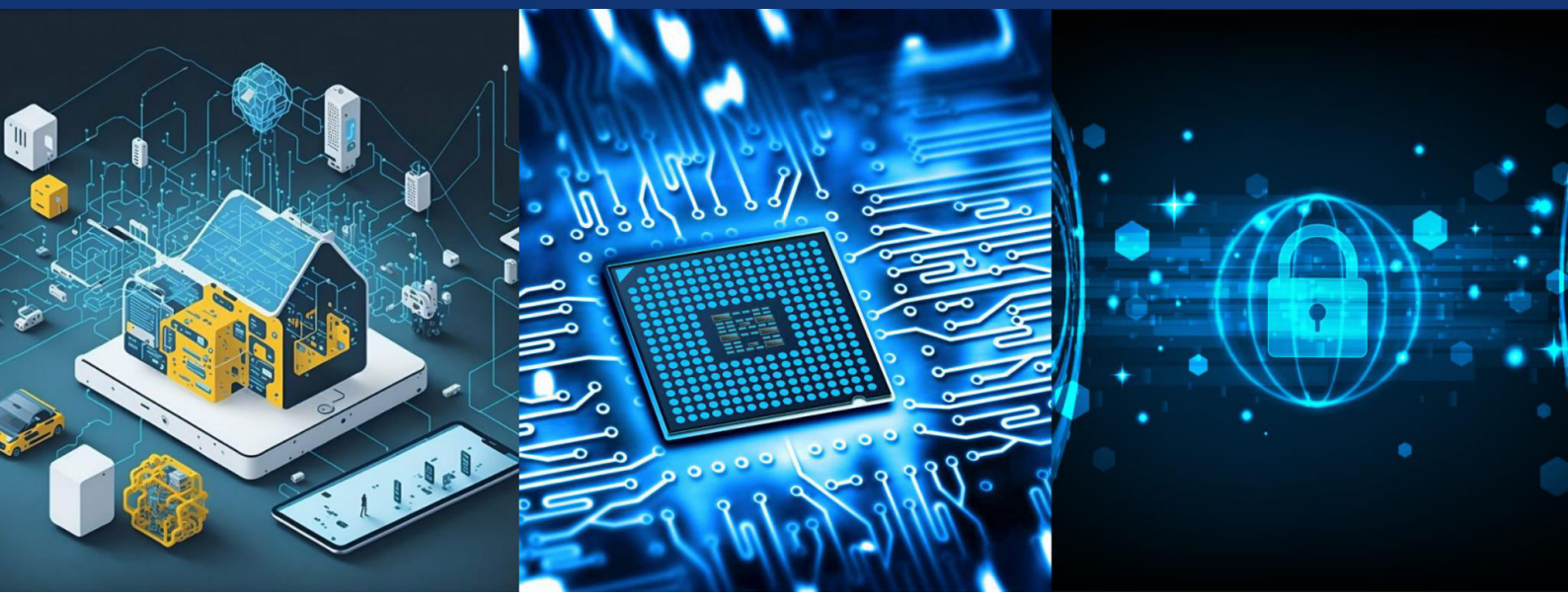
IJIRCCE

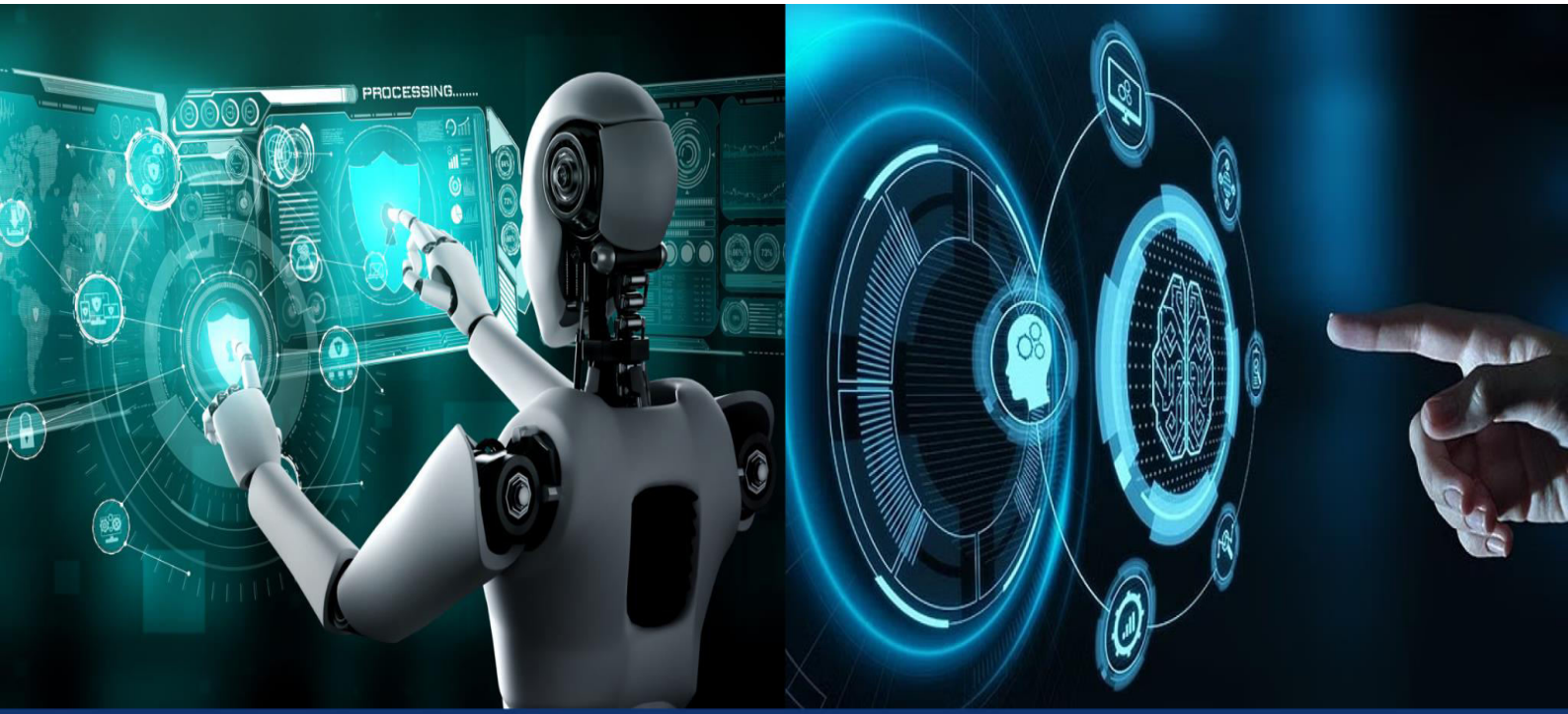
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304043

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Next-Gen Multimedia Encryption by Combining Symmetric and Asymmetric Cryptographic Techniques

Dr.P.Muthusamy, Mr.R.Velmurugan, Mr.C.Manikandan, Mr.R.Mohanprasath

Professor/HOD, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

ABSTRACT: As healthcare increasingly adopts digital transformation, securing multimedia medical data such as images, videos, and patient records has become essential to prevent unauthorized access and ensure patient privacy. Multimedia data security and privacy have grown critical due to the increasing reliance on digital media. Protecting sensitive data from unwanted access requires the use of encryption. The data structure, file size, and real-time processing requirements of images, audio, and video each provide different encryption issues.

The many encryption methods and algorithms for digital picture, audio, and video security are examined in this study Audio encryption frequently uses frequency masking or scrambling to protect media and transmission, while techniques like frequency domain encryption and pixel shuffling are proposed for images , Video encryption, which is crucial for streaming and content distribution, usually uses bitstream-level techniques and selective encryption to guarantee security and compliance with compression requirements. There is also discussion of the difficulties in obtaining real-time encryption and preserving quality throughout the encryption and decryption processes. In an increasingly interconnected world, these methods are essential for digital rights management, secure communications, and personal data security. So, in this project we can implement hybrid cryptography techniques which includes the Elliptical curve cryptography and Advance encryption standard (AES) algorithm to secure the multimedia data.

I. INTRODUCTION

Medical data security is crucial in safeguarding sensitive patient information, including health records, diagnostic results, treatment histories, and personal details. With the rapid digitization of healthcare, the volume and complexity of medical data are growing, making it more vulnerable to cyberattacks, data breaches, and unauthorized access. Data breaches in healthcare systems can expose critical personal information, leading to identity theft, fraud, and significant reputational damage. The challenge is compounded by the need for secure data sharing between different healthcare providers, insurance companies, and labs, where patient data must be exchanged across various systems while ensuring privacy and integrity. Additionally, healthcare organizations must comply with stringent regulatory frameworks such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), which mandate strict controls on how personal health information is stored, processed, and shared. With these concerns in mind, securing medical data involves implementing advanced encryption, access control mechanisms, and secure communication protocols to protect against unauthorized access and maintain patient trust. Moreover, ensuring that healthcare systems are both interoperable and secure remains a critical challenge as more healthcare providers adopt digital tools and technologies. With the rise of digital media consumption, multimedia cryptography has become more and more important for anything from personal video sharing to large-scale applications like streaming services, telemedicine, and secure monitoring. Multimedia files provide a number of other difficulties in addition to their size and complexity, like format compatibility and compression techniques. Encryption systems need to work with multimedia files that have been compressed (JPEG for images, MP3 for audio, or H.264 for video) in order to minimize their size. It's difficult to encrypt compressed media without significantly increasing overhead or impairing compression efficiency. A usability problem could arise if the encryption modifies the file structure excessively, making the material unusable with conventional decoders or players.

Data encryption is becoming a crucial component of data resource protection, particularly on intranets, extranets, and the Internet. Before digital data is communicated, it must first be encrypted using specific mathematical techniques and keys, and then it must be decrypted using the same mathematical procedures and keys to recover the original data from the cypher code. Ensuring user authentication as well as the integrity, correctness, and safety of data resources is the aim of security management. Moreover, the encryption and decryption of image-based data takes more work. The

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

same goal guides the development of the model for both encryption and decryption of images using appropriate user-defined keys. Overview and Need The necessity to safeguard particular communications and stored data against theft and misuse has been recognized by privacy and confidentiality considerations in a computer system. Using cryptographic algorithms is a good approach for safeguarding data that is shared or stored. Multimedia encryption involves the application of cryptographic algorithms to protect the confidentiality, integrity, and authenticity of multimedia data. Traditional cryptographic methods, including both symmetric and asymmetric encryption, are used to secure data, but each has its strengths and weaknesses. Symmetric encryption is fast and efficient for large data sets, but the key distribution problem poses a challenge in secure communication. On the other hand, asymmetric encryption solves the key distribution issue by using a pair of public and private keys, but it tends to be computationally expensive.

In the combined approach, the multimedia data is first encrypted using symmetric encryption, and then the symmetric key is encrypted using asymmetric encryption before being transmitted. Once the recipient receives the encrypted symmetric key, they can use their private key to decrypt it and access the multimedia content securely and efficiently. This hybrid approach leverages the strengths of both symmetric and asymmetric encryption, providing a balance of speed and security while protecting sensitive multimedia data from unauthorized access and tampering.

The study of mathematical methods for information security, including entity authentication, data integrity, secrecy, and data origin authentication, is known as cryptography. Plaintext is what a message is. Encryption is the technique of masking a message so that its content is hidden. Ciphertext is the message sent using encryption. Decryption is the process of converting ciphertext back into plain language. (05). Basic operations that can be carried out in encryption/decryption are: substitution and transposition. Due to advent of computers, these operations are carried out on binary bits. (04) With the help of the Internet, a global "Virtual Community" unrestricted by space and time has emerged. A person in one location can communicate with specialists anywhere in the world thanks to the Internet. You can ask professionals for their opinions by voice, video, or electronic mail. Furthermore, where data takes the form of images, telemedicine is gaining traction in the fields of radiology, pathology, critical care, and psychiatry. When sending some image-based data over the Internet, confidentiality and security must be guaranteed. Ensuring user authentication and maintaining the integrity, correctness, and safety of data resources are the goals of security management. The same goals guide the construction of the encryption and decryption paradigm for images. With the aid of an appropriate user-defined key, the model for encryption and decryption of a picture is created with the goals of maintaining confidentiality and security in the transmission of image-based data as well as storage in the data warehouse

II. SYSTEM ANALYSIS

Existing System:

Numerous cryptographic approaches are already in use in the present multimedia encryption landscape to secure data that includes images, audio, and video.

Typically, these systems depend on conventional cryptographic methods, which can be either symmetric or asymmetric and cater to different requirements and scenarios.

Deep learning models, particularly CNNs, can be utilized for extracting key features from medical images before encryption. These features can be critical for guiding the encryption process and ensuring that the encrypted images retain the necessary information for later decryption and interpretation.

Limitations:

While fast for encrypting large files, it struggles with secure key distribution, requiring additional layers of protection. Securely managing and distributing symmetric keys in large-scale systems can be complex and prone to vulnerabilities. Asymmetric systems require careful handling of public and private keys, and a compromised private key can lead to significant data breaches. Integrating cryptographic methods into existing systems, such as legacy multimedia platforms, can be challenging and often requires significant infrastructure changes.

Proposed System:

Medical multimedia systems, which handle sensitive data such as medical images, videos, and patient records, require robust encryption techniques to ensure data confidentiality, integrity, and secure transmission.

A hybrid cryptographic strategy that combines Elliptic Curve Cryptography (ECC) with Advanced Encryption Standard (AES) offers a balanced solution to meet the growing demand for safe and effective multimedia encryption.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304043

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

By combining the benefits of symmetric and asymmetric encryption, this technique maintains great speed for big datasets and real-time applications while providing strong security for picture, audio, and video files.

Expected Merits:

The hybrid approach is adaptable for various applications, including large scale systems with multiple users. It supports a range of multimedia formats and use cases, from streaming services to secure storage.

III. SYSTEM REQUIREMENTS

Hardware Requirements:

- Processors: Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz (1 socket, 2 cores, 2 threadsper core), 8 GB of DRAM
- Disk space: 320 GB
- Operating systems: Windows® 10

Software Requirements:

- Server Side : Python 3.7.4(64-bit) or (32-bit)
- Client Side : HTML, CSS, Bootstrap
- IDE : Flask 1.1.1
- Back end : MySQL 5.
- Server : WampServer 2i
- OS : Windows 10 64 –bit

Software Description:

Python:

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages.

MySql

MySQL is an open-source relational database management system (RDBMS) widely used for managing and storing structured data. It is based on the Structured Query Language (SQL) and supports a wide range of applications, from small-scale projects to large, complex enterprise systems.

PyCharm:

PyCharm has a highly customizable user interface, allowing users to tailor the IDE to their specific needs and preferences. This includes customizing the color scheme, key mappings, and even the appearance of the code editor. PyCharm also supports various plugins and extensions, enabling users to add new functionality to the IDE or integrate with external tools and services. In addition to its development features, PyCharm also includes tools for project management, such as version control integration with Git, Mercurial, and Subversion. It also provides support for task management and issue tracking through integration with tools like Jira and Trello. PyCharm has a strong focus on code quality and maintainability, providing tools for code inspections, unit testing, and code coverage analysis. This can help developers catch errors and ensure that their code is maintainable and scalable over time. PyCharm also supports multiple Python versions and virtual environments, allowing users to switch between different versions of Python or create isolated environments for different projects. This can help ensure compatibility and prevent version conflicts between different projects. Overall, PyCharm is a comprehensive IDE that can greatly improve productivity and code quality for Python developers. Its extensive feature set, customization options, and focus on code quality make it a popular choice for Python development.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304043

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. LITRETURE SURVEY

- **Title :**Multimedia security using encryption: A survey (2023)
- **Author :** Hosny, Khalid M., et al.
- **Concept :** Proposed the system to review the state of secure and privacy-preserving encryption schemes applicable to digital multimedia, such as digital images, digital video, and digital audio
- **Limitation:** Slower and computationally intensive, making it impractical for encrypting large files
- **References:** Hosny, Khalid M., et al. "Multimedia security using encryption: A survey." IEEE Access 11 (2023): 63027-63056.

- **Title :** 3D chaotic map-cosine transformation-based approach to video encryption and decryption (2022)
- **Author : :** Dua, Mohit, et al
- **Concept :** Designed to transmit text and image data securely. Due to time constraints and enormous input data sizes, very little progress has been done in the field of video encryption
- **Limitation :** Computational complexity is high
- **References :** Dua, Mohit, et al. "3D chaotic map-cosine transformation-based approach to video encryption and decryption." Open Computer Science 12.1 (2022): 37-56.

- **Title :**A review on audio encryption algorithms using chaos maps-based technique (2022)
- **Author :**Albahrani, Ekhlas Abbas
- **Concept :** The main focus of this study is to illustrate the many kinds of chaotic map-based audio encryption and decryption methods
- **Limitation :** A limitation of Audio frames may be loss in transmission
- **References :** Albahrani, Ekhlas Abbas, Tayseer Karam Alshekly, and Sadeq H. Lafta. "A review on audio encryption algorithms using chaos maps-based techniques." Journal of Cyber Security and Mobility (2022): 53-82.

- **Title :**A chaoti-based encryption/decryption framework for secure multimedia communications (2020)
- **Author :** Yasser, Ibrahim, et al
- **Concept :** Proposed a novel chaotic-based multimedia encryption schemes utilizing 2D alteration models for high secure data transmission
- **Limitation :** Key distribution and management are difficult
- **References :** Yasser, Ibrahim, et al. "A chaotic-based encryption/decryption framework for secure multimedia communications." Entropy 22.11 (2020): 1253.

V. CONCLUSION

In conclusion for protecting multimedia data, including music, video, and photos, the hybrid encryption model that combines Elliptic Curve Cryptography (ECC) with Advanced Encryption Standard (AES) offers a very efficient solution. Through the utilization of symmetric and asymmetric cryptographic approaches, this method guarantees a strong equilibrium among security, speed, and effectiveness. Large multimedia files may be quickly and effectively encrypted with AES, which makes it appropriate for real-time applications and high-quality media. Meanwhile, even in contexts with limited resources, ECC guarantees secure key exchange with no computational expense. Many applications, including as cloud storage, encrypted phone communication, secure video streaming, and multimedia systems based on the Internet of Things, are ideal for the hybrid ECC AES architecture. It is the go-to option for next-generation multimedia encryption systems due to its scalability and capacity to handle huge data sets without compromising speed. ECC is a future-proof solution since it uses reduced key sizes, which also guarantee lower storage and bandwidth requirements, especially in contexts with limited bandwidth.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. Hosny, Khalid M., et al. "Multimedia security using encryption: A survey." IEEE Access 11 (2023): 63027-63056.
2. Yasser, Ibrahim, et al. "A chaotic-based encryption/decryption framework for secure multimedia communications." Entropy 22.11 (2020): 1253.
3. Albahrani, Ekhlas Abbas, Tayseer Karam Alshekly, and Sadeq H. Lafta. "A review on audio encryption algorithms using chaos maps-based techniques." Journal of Cyber Security and Mobility (2022): 53-82.
4. Dua, Mohit, et al. "3D chaotic map-cosine transformation-based approach to video encryption and decryption." Open Computer Science 12.1 (2022): 37-56.
5. Zia, Unsub, et al. "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains." International Journal of Information Security 21.4 (2022): 917-935.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details