IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

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

Mrs. P. Banuppriya M.E[1], J. Kaviya[2], C. Keerthana[3] ,P. Kowsalya[4], S. Kowsika[5]
[1]Assistant Professor, Department of CSE
[2,3,4,5] Students, Department of CSE
Mahendra Institute of Engineering and Technology Namakkal, Tamil Nadu, India

Abstract: *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 paper we can implement hybrid cryptography techniques which includes the Elliptical curve cryptography and Advance encryption standard (AES) algorithm to secure the multimedia data.*

Keywords: Network security, Cryptography, Multimedia, Asymmetric encryption, Sensitive data

I. INTRODUCTION

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 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, MP3for 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 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. 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

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

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. RELATED WORK

Khalid M. Hosny,et.al..[1] 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. o provides a thorough overview of the current state of security encryption schemes specifically made for digital multimedia technology, a thorough examination of the multi-media encryption algorithms and existing cryptography schemes will be carried out. The survey's findings will be utilized to improve our knowledge of the dependability and efficacy of safe multimedia encryption techniques and to help create more secure and effective encryption methods in the future. Digital images are digital media that can capture and store visual information. Images are increasingly used to transmit sensitive information across networks in various fields, such as medicine, defense, online banking, and telecommunications. There is a serious chance that unauthorized parties will steal this private information. The field of image encryption is growing because the aim is to protect these photos using encryption techniques so that enemies cannot access or decipher them.

Ibrahim Yasser,et.al,..[2] proposed novel chaotic-based multimedia encryption schemes utilizing 2D alteration models for high secure data transmission. It is suggested to use a unique perturbation-based data encryption for rounds of bewilderment and diffusion. Our chutnification structure is hybrid, meaning that media encryption is achieved by combining various maps. Control parameters for the permutation (shuffling) and diffusion(substitution) structures are generated by means of blended chaotic maps. In addition to maintaining the high encryption quality that chaotic replication may replicate, the suggested methods also have minimal residual clarity and key sensitivity. Extensive security and differential analyses documented that the proposed schemes are efficient for secure multimedia transmission as well as the encrypted media possesses resistance to attacks. Furthermore, statistical analyses utilizing established metrics for certain media types demonstrate that suggested encryption techniques can achieve low residual intelligibility with an abundance of nice, recovered statistics. Lastly, by contrasting the suggested schemes with some cutting-edge algorithms from the literature, the benefits of the proposed schemes have been brought to light. The comparative performance results demonstrated that our techniques are extra efficacious than their data-specific counterpart ways Ekhlas Abbas Albahrani,et.al,..[3] proposed method addresses the most recent advancements in audio encryption and provides the most extensive algorithmic assessments, taking into account criteria related to security, computational complexity, and quality analysis. The main focus of this study is to illustrate the many kinds of chaotic map-based audio encryption and decryption methods. Analogue and digital audio algorithms were presented, examined, and contrasted with an explanation of their key benefits and limitations. Numerous digital and audio projects have been discussed that use chaotic maps for audio encryption. These projects demonstrated significant sensitivity to beginning conditions, unpredictability, and quasi- random behavior. There was a comparison of the suggested methods in the key space, statistical analysis, and chaotic map sensitivity Prashant Mishra,et.al,...[4] 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. However, one of the most crucial aspects of network dependability these days is video data security because of the exponential growth of digital media transit within networks. Video encryption has already been

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

accomplished using block encryption algorithms and 1D- chaotic maps. Despite producing highly good results, 1D-chaotic maps have less dynamic behaviour, hence there were several limitations to the approach. This article suggests a video encryption method based on the Intertwining Logistic Map (ILM)- Cosine transformation to get around these problems. Based on the duration of the video and the frames per second (FPS) value, the input video was first divided into several frames. Subsequently, every frame was chosen, and a technique known as permutation/scrambling was used to lessen the association between the pixels. To provide even more randomness to the encryption process, each frame was additionally rotated by 90° in the opposite direction of the clock. Furthermore, row- and column-wise adjustments were applied to every image using a method known as the random order substitution technique. Ultimately, a frame selection key was used to jumble all of the encrypted frames, which were then combined to create an encrypted video that was sent to the user. This method's effectiveness was evaluated using the state.

Mark McCartney,et.al,..[5] studied surveys the state-of-the-art chaos-based picture encryption algorithms and divides them into spatiotemporal, temporal, and spatial domains. There is a discussion of the noteworthy advancements in the realm of picture encryption. Furthermore, in recent publications, comparative analysis is carried out to verify the evaluation matrices for measuring the security and performance of the encryption algorithms. New digital communication and network technologies are being adopted and developed quickly, which has shown great promise for better data interchange and storage over the Internet. Nonetheless, safeguarding personal information is equally crucial, which is why network security and data integrity have long been major concerns. Because of this, scientists have taken the necessary precautions to increase visibility and avoid security vulnerabilities. The majority of multimedia that is shared and saved online takes the form of photographs. Therefore, picture encryption ensures the validity and confidentiality of digital photos.

Mudassar Hussain Shah,et.al,..[6] created the technology for digital watermarking was invented by Lina the essay's author employed the ideas of unique wavelet transformation and chaos to create interactive watermarks. The picture is first subjected to a discrete wavelet transformation, the low-frequency portion is then eliminated, and then the mess sequence is employed to encrypt the small-frequency element. This is a non-blind recognition method where the initial image is used for extraction. The device is tested using the NC coefficient and high noise to signal ratio (PNSR). The findings indicated that a combination of a noisy attack, filtering, combined technical photography culture, etc. The watermark image has had a significant impact. The author employed the logistic solution of chaos for the data encryption technique. The algorithm is analysed based on the following principles: complexity, similarity, and unpredictability.

Mohamed Maazouz,et.al,..[7] Analyse the concepts based on the principles such as complexity, similarity, and unpredictability. The simulation of the chaos sequence has demonstrated that it meets the requirements of the encryption algorithm. presented a technique for image encryption. Discreet chaotic diagrams, which integrate permutation and replacement approaches, are used in the proposed method. The algorithm indicating that the original image was confirmed by a typical Lena picture. The simulation of the chaos sequence has demonstrated that it meets the requirements of the encryption algorithm. presented a technique for image encryption. Discreet chaotic diagrams, which integrate permutation and replacement approaches, are used in the proposed method. The algorithm indicating that the original image was confirmed by a typical Lena picture.

Subashanthini,et.al,..[8] suggested using a two-layer bit-level encryption in the time- frequency domain picture encryption system. A small portion of a plane slices the image in the to player, and each plane is then encrypted using a key created from the same chaotic map and jumbled using a chaotic map. Next, the low-frequency components of each segment are encrypted and jumbled using a Lifting Wavelet Transform, which comes after picture segmentation. The last layer is then encrypted and jumbled using a chaotic hybrid map. After the algorithm was subjected to several evaluations, the suggested work produced a maximum entropy of 7.99 and a near-zero correlation, demonstrating the program's resilience to statistical attacks. Additionally, the cryptosystem's key space is larger than 2128, meaning that a brute force assault cannot successfully defeat it. Furthermore, this method takes a mere 2.1743 seconds to encrypt a 256 × 256 sized 8-bit picture on a host system running Windows 10 on a 64-bit Intel(R) Core (TM) i5-7200U CPU running at 2.5 GHz with 8 GB of RAM.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

Dawood Shah,et.al,..[9] The diffusion module of the suggested architecture uses a unique kind of curve that depends on effective elliptic curve arithmetic operations. Thus, it produces high- quality pseudo-random numbers (PRN) and achieves optimal diffusion in encrypted audio files with minimal computational cost. A unique block cypher construction technique, involving multiplication and binary Galois field inversion as well as other well-known arithmetic operations, has been used for the confusion module. The recommended technique builds numerous substitution boxes (S-boxes) by employing a higher-order Galois field. As a result, replacing the original S-boxes with multiple ones creates effective data confusion and boosts the security of the ciphered audio. The results of the experiment, obtained from varying studies and time complexity, showed that the technique could fend off a wide range of threats.

Jungang-ro,et.al,..[10] proposed architecture's diffusion module makes use of a special type of curve that is dependent on efficient arithmetic operations on elliptic curves. As a result, it minimises computational cost while producing pseudo-random numbers (PRN) of excellent quality and achieving optimal diffusion in encrypted audio files. For the confusion module, a special block cypher construction method has been employed, involving multiplication and binary Galois field inversion along with other common arithmetic operations. The suggested method uses a higher -order Galois field to construct many substitution boxes (S- boxes). Therefore, adding more S- boxes to the original ones causes effective data confusion and increases the ciphered audio's security. The experiment's outcomes, which were derived from various research and time complexity.

III. BACKGROUND OF THE WORK

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. Because symmetric encryption methods can process huge files rapidly and are computationally efficient, they are frequently used to secure multimedia data. One example of this is the Data Encryption Standard (DES). High- definition video, audio, and image encryption are areas where DES excels, especially when it comes to cloud storage, content delivery networks (CDNs), and local media encryption. In many systems, it is the de facto norm due to its speed and efficacy, but safely distributing the encryption keys is a hurdle. Because of this, DES and asymmetric encryption are frequently combined. Multimedia applications employ asymmetric encryption techniques like RSA to safely exchange symmetric keys. Asymmetric encryption offers a safe method of managing and distributing encryption keys across untrusted networks but being slower and less effective when encrypting big files. For example, RSA can encrypt the session key that DES uses to encrypt the media streams in systems like secure video conferencing. Digital rights management (DRM) systems also frequently employ asymmetric algorithms to restrict access to copyrighted content, guaranteeing that only authorized users have access to the decryption keys. The basic encryption flow can be shown in fig 1

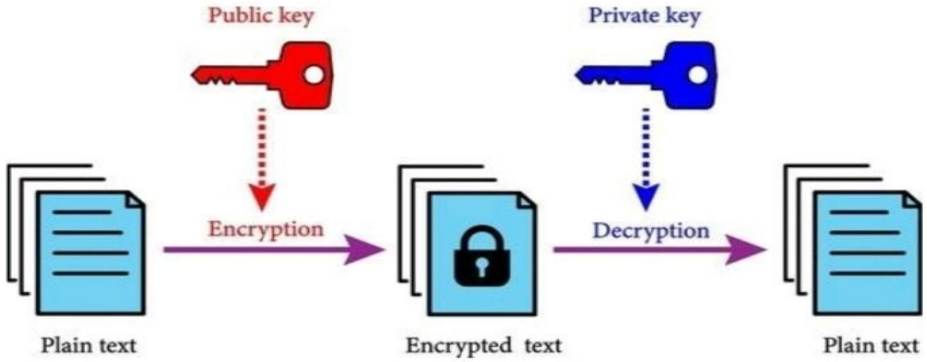

Fig 1: Cryptography process

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

IV. PROPOSED FRAMEWORK

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. 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. The symmetric key approach known as AES (Advanced Encryption Standard) is fast and effective; it is especially well-suited for encrypting huge multimedia files. AES can use key lengths of 128, 192, or 256 bits and encrypts data in set block sizes (128 bits). Because of its minimal computational overhead, it is frequently used for bulk data encryption and is recognized as one of the most secure encryption methods.

Compared to more conventional asymmetric techniques like RSA, ECC (Elliptic Curve Cryptography) offers robust security with shorter key lengths. ECC offers the same level of security as RSA but with much smaller keys, making it more efficient in terms of computation and storage. ECC generates public and private keys using elliptic curve theory. ECC is therefore especially well-suited for resource-constrained situations, as those seen in mobile devices and Internet of Things systems. Because AES is good at handling huge files, it is utilized in the hybrid technique to encrypt the real multimedia content (image, audio, or video), while ECC is used for safe key exchange. Performance is not affected, and multimedia data is safeguarded during transmission and storage thanks to this combination. The proposed Framework shown in fig 2.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

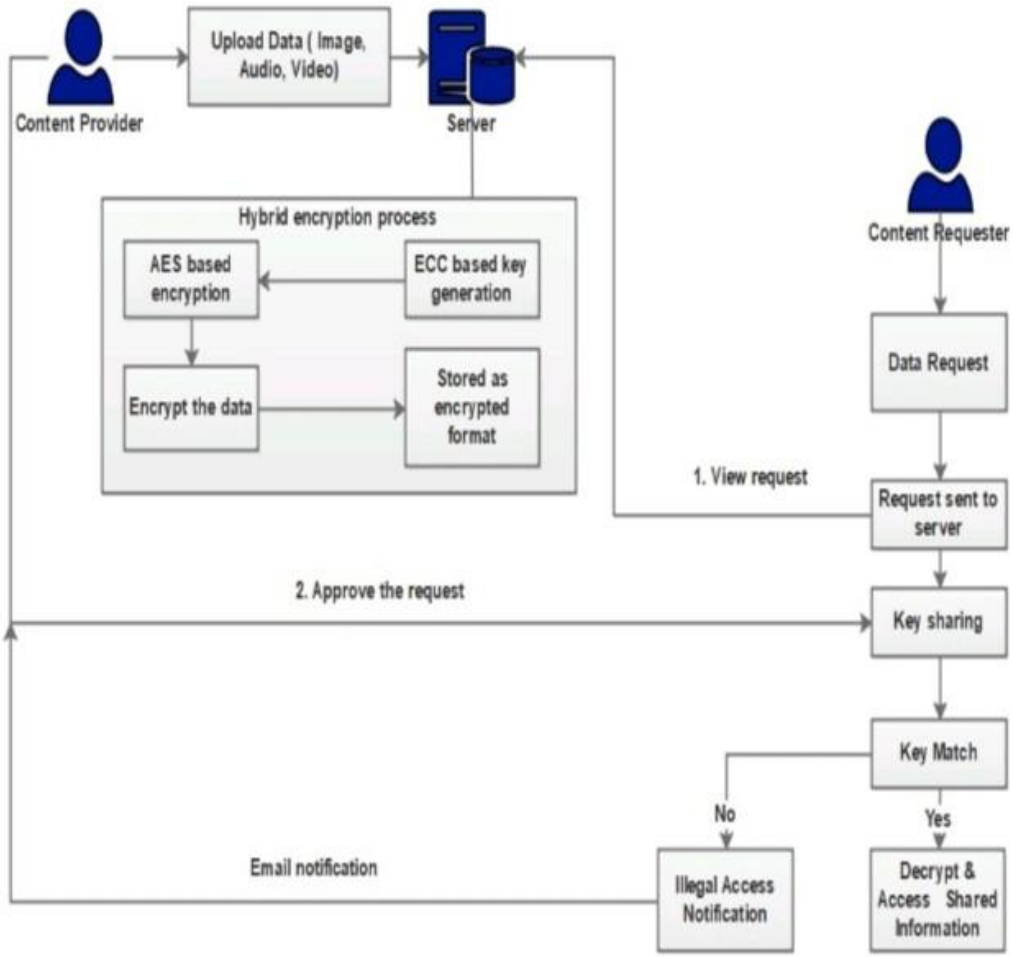

Fig 2: Proposed framework

GENERAL PROCEDURE OF ECC

Both parties agree to some publicly-known data items The elliptic curve equation Values of a and b Prime, p The elliptic group computed from the elliptic curve equation.

A base point, B, taken from the elliptic group Similar to the generator used in current cryptosystems.

Each user generates their public/private key pair

Private Key = an integer, x, selected from the interval [1, p-1]

Public Key = product, Q, of private key and base point (Q = x*B) AES ENCRYPTION

The AES cipher is also known as the block cipher. No successful attack has been reported on AES. Some advantages of AES are easy to implement on 8-bit architecture processors and effective implementation on 32-bit architecture processors. In addition, all operations are simple (e.g, XOR, permutation and substitution). AES encryption is performed in multiple rounds. Each round has four main steps including sub-byte, shift row, mix column and add round key. Sub- byte is the substitution of bytes from a look-up table. Shift row is the shifting of rows per byte length. Mix column is multiplication over Galois field matrix. Finally, in the add round key step, the output matrix of mix column is XORed with the round key. The number of rounds used for encryption depends on the key size. For a 128-bit key, these four steps are applied to 9 rounds, where the 10th round does not consider the mix column step. Since all steps are recursive, decryption is the reverse of encryption

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

Algorithm Procedure;

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm.

The four stages are as follows:

Substitute bytes Shift rows

Mix Columns

Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

Inverse Shift rows

Inverse Substitute bytes Inverse Add Round Key Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage. Each of these stages will now be considered in more detail fig 3.

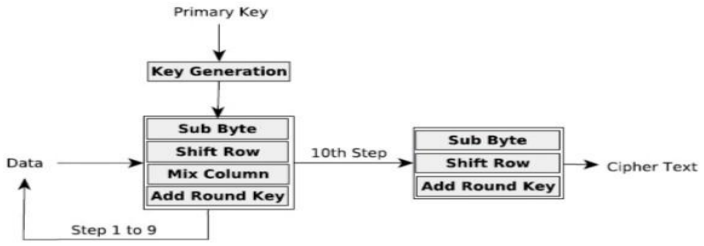

Fig 3: AES process

V. EXPERIMETNAL RESULTS

Despite significant advances in multimedia encryption techniques, current methods still face several challenges when it comes to security, computational efficiency, real-time performance, and flexibility over different multimedia formats. The traditional encryption algorithms RSA, AES, and Blowfish are very resource-intensive computationally and hence not suitable for encrypting big volumes of images. Pixel shuffling and chaos-based encryption often do not maintain the quality of the image after decryption; the image is distorted. Encryption in the frequency domain conflicts with JPEG/MPEG compression and hence loses effectiveness in practical applications. Table 1 shows the comparison table with proposed framework.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

Encryption Method	Security Strength	Computational Efficiency	Real-Time Performance	Compression Compatibility	Scalability Across Multimedia
AES (Advanced Encryption Standard)	High	Moderate	Moderate	Moderate	Limited (Best for Images)
RSA (Rivest-Shamir-Adleman)	Very High	Low (Slow for Large Files)	Poor	Poor	Poor
Blowfish	Moderate	High	High	Poor	Limited
Chaotic-Based Encryption	High	Moderate	Moderate	Poor	Limited
Pixel Shuffling (Image)	Low-Moderate	High	High	Poor	Only for Images
Selective Video Encryption	Moderate	High	High	High	Only for Video
Proposed Hybrid (ECC + AES)	Very High	High (Optimized Key Management)	High (Real- Time Processing)	High (Compatible with Compression Standards)	High (Scalable for Image, Audio, Video)

TABLE 1: Comparison table

VI. 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.

REFERENCES

[1] Hosny, Khalid M., et al. "Multimedia security using encryption: A survey." IEEE Access11(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 KaramAlshekly, 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-cosinetrans formation-based approach to video encryption and decryption." Open Computer Science 12.1 (2022): 37-56.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

[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.
[6] Ghosh, Gopal. "A systematic review on image encryption techniques." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.10 (2021): 3055-3059.
[7] Maazouz, Mohamed, et al. "FPGA implementation of a chaos-based image encryption algorithm." Journal of King Saud University-Computer and Information Sciences34.10 (2022): 9926-9941.
[8] Mahalingam, Hemalatha, et al. "Dual-domain image encryption in unsecure medium—a secure communication perspective." Mathematics11.2(2023): 457.
[9] Shah, Dawood, et al. "An efficient audio encryption scheme based on finite fields." IEEE Access 9 (2021): 144385-144394.
[10] Yun, Junhyeok, and Mihui Kim. "JLVEA: Lightweight real-time video stream encryption algorithm for internet of things." Sensors 20.13(2020): 3627