Advanced Time Frequency For Secureaudio Embedding In Visual Media

Dr.U.Nilabar Nisha[1], Ajaykumar N[2], Dinesh V[3], Veeramani V[4], Vishwa V[5]
[1]HOD, Dept of Computer Science and Engineering
[2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Mahendra Institute of Engineering and Technology, Namakkal, TamilNadu,India

Abstract- *In today's highly digitized world, it has become crucial to have the ability to share multimedia content in a safe and reliable manner owing to increasing threats from cyber security experts. With that in mind, this project will focus on designing an innovative yet highly efficient system for safe content sharing with the use of hybrid encryption algorithm based on AES, which is ideal for data encryption along with ECC, which will help generate and distribute keys. Key components in this design include Content Provider, Server, Content Requester, and Access Control, which facilitate safe uploading, storage, and retrieval of the content in an encrypted format. Further adding to the security aspect, the system uses Discrete Wavelet Transform based Steganography whereby the audio file is hidden inside a carrier image, thus offering an extra layer of security by hiding the information. It can be noted that the presence of confidential information will remain secret as no one would even realize its presence since the file itself would not reveal anything to begin with. Moreover, the system includes access control as well as a notification system, which will alert the content provider if any unauthorized request is made for accessing the multimedia content.*

Keywords: Access Control, Advanced Encryption Standard (AES), Audio Steganography, Content Sharing, Elliptic Curve Cryptography (ECC), Hybrid Encryption, Secure Multimedia Data

I. INTRODUCTION

Due to the rise in internet usage, the need for secure multimedia content distribution has risen considerably in today's digital age. Audio files, particularly, require robust measures to be implemented to prevent any form of cyber thefts. In this regard, the following project presents an efficient solution in the form of a secure content distribution scheme which integrates both data encryption and data hiding processes. The implementation process begins by ensuring that all private information is secured using two different layers. Firstly, the system uses an AES-based encryption algorithm to encrypt multimedia files. Secondly, the system hides multimedia files from all forms of prying eyes through data encryption. The core of the system employs a hybrid encryption process involving AES for fast encryption and ECC for key distribution. This section presents a brief overview of the overall framework, which involves four modules. These include Content Provider, Server, Content Requester, and Access Control. The content provider initiates the upload process while the server stores the uploaded content after encryption. The structured process ensures that the data remains confidential, secured and accessible only by authorized persons. Besides encryption, the proposed structure also uses the Discrete Wavelet Transform (DWT) Based Steganography technique for concealing the data by embedding the audio into an image. This makes sure that no one will be able to trace the existence of any confidential data from the system. An additional module of the proposed structure sends notification to the user if there is any unauthorized access attempted in the system.

i) Problem statement

The sharing of multimedia data, especially confidential audio data, within the existing digital world has become highly susceptible to security issues including theft, interception of data, and misappropriation. The existing methodologies make use of encryption algorithms, such as the Advanced Encryption Standard (AES). While encryption is effective in securing the data being transmitted through the network, there have been numerous concerns associated with the distribution of the encryption keys among the users. For instance, if the encryption key is intercepted while being delivered, all data sent using that encryption becomes vulnerable. Another problem lies in the inability to restrict the access to the data being transmitted dynamically. Also, there are no adequate provisions for data hiding or transparency of access monitoring. The absence of sophisticated tools like Steganography makes the information vulnerable, despite being encrypted, since it will attract attacks from any interested party due to its detectability. Additionally, there are no good ways of exchanging keys between the parties involved in an efficient and light manner, since conventional methods like RSA, which is the cryptosystem, require larger keys. In addition, most systems lack provisions for notifying

the concerned content providers whenever someone tries to access the information in question without authorization.

ii) Objectives

The main goal of this research is the development of a safe and efficient multimedia content sharing system, which provides confidentiality and safety of the confidential audio data when transmitting and storing. This is done through the use of a hybrid algorithm for encryption and key generation, where AES is used to provide fast and efficient encryption, while ECC is used for generating keys. The system is aimed at overcoming the weaknesses in the classical approach to data security due to its inability to achieve a high level of security with acceptable performance. Another goal of the research is to improve data safety through the usage of DWT based Steganography. The proposed approach takes into account the additional measure, hiding the fact that the encrypted data is present in the first place, which increases the difficulty for the hacker to discover the data or access the data. Thus, the goal of implementing such a measure would be not only to encrypt the data but also to hide the data from the eyes of the unauthorized users and make their job tougher. The next measure would include the implementation of an access control system for the multimedia sharing site, which would allow access to the multimedia content only to authenticated users. With such an arrangement in place, the possibility of hacking attacks and accessing data without permission would be significantly minimized.

II. RELATED WORK

[1] A chaotic encryption scheme is proposed in this research paper that aims to improve the security level in multimedia communication systems. Chaotic maps are used in this encryption scheme to produce encryption keys, thus increasing the resistance of multimedia communication system against any cryptographic attacks. The scheme is designed for securing the communication of images, audio, and video data over non-secure channels. The importance of initial condition sensitivity is emphasized in chaotic systems due to its contribution to increasing security. This encryption scheme includes an encryption/decryption algorithm based on nonlinear dynamic systems. It has excellent confusion/diffusion characteristics in multimedia data. The security level of this proposed technique is proved to be better than that of conventional encryption schemes. In addition, it offers robustness against brute force and statistical attacks. Moreover, the computational cost of chaotic encryption scheme for multimedia data is estimated.

[2] This article will provide a detailed review on methods of encrypting audio signals using chaos theory and chaotic mapping techniques. This work will critically analyze various chaotic techniques applied in audio encryption in communication systems. The research will outline the benefits associated with the use of chaotic systems in encryption key generation. In addition, the way audio signals can be encrypted and made inaccessible to other parties will be illustrated. Different encryption models will be analyzed by comparing their efficiencies and effectiveness in providing security. Moreover, strengths and weaknesses of chaotic techniques in ensuring audio security will be reviewed. The importance of chaotic techniques in implementing audio security measures will be discussed in relation to their application in real time.

[3]The current study proposes an encryption algorithm for videos, which integrates 3D chaotic maps and cosine transformation. This technique increases security of video data by enhancing the complexity involved in video transformation. Chaotic maps have been implemented to obtain encryption keys, which would help to encrypt video data. In addition, cosine transformation has been performed for converting spatial information into frequency domain. High immunity to statistical and differential attacks can be obtained through the technique proposed. Excellent diffusion and confusion can be achieved by utilizing the proposed encryption method for video content. The proposed technique is capable of performing efficient encryption and decryption operations for video data.

[4] This survey paper gives an overview of image encryption techniques using chaotic maps in various domains. This paper groups the encryption schemes as spatial, transform and spatiotemporal encryption. This research paper illustrates how chaotic systems help to enhance image encryption due to their random nature. This research paper evaluates various encryption schemes according to encryption security and efficiency. This paper emphasizes the role of diffusion and confusion processes in image encryption. It is also important to note that this research paper evaluates various issues faced in implementing image encryption schemes due to the trade-off between encryption security and efficiency. This research paper evaluates performance of various chaotic image encryption schemes. This research paper reveals some shortcomings associated with conventional image encryption schemes.

[5] The aim of this paper is to review the recent multimedia security approaches based on cryptography. Different encryption algorithms are reviewed for their applicability in the fields of image, audio and video encryption. This paper describes the increasing demand for securing multimedia communications in the digital

environment. It discusses various cryptographic algorithms used for ensuring security in multimedia applications. Both the symmetric and asymmetric cryptographic techniques have been considered. The advantages and disadvantages of current cryptographic techniques have been evaluated. Various hybrid encryption algorithms have also been reviewed for enhancing the performance. Challenges faced by the multimedia security approaches have been discussed. This paper stresses on the significance of secure data communication over the networks.

[6] In this research, an access protocol based on blockchain technology will be designed and analyzed. In this protocol, every action regarding the usage of shared medical images will be recorded in the decentralized ledger which makes sure that any access activity performed on the medical images is recorded in an immutable manner. This system increases the level of accountability since a secure audit trail can be created for every interaction with the medical images. Since it uses blockchain technology, access logs can never be modified without permission. Using this blockchain protocol increases the level of trust between providers and receivers of the medical image data. This paper underscores the necessity of immutability in terms of keeping the record of access activities to the medical images. Every access attempt will be made secure through the application of this technique.

[7] The present paper considers multiple data augmentation approaches that are used during medical image processing to enhance the capabilities of a model. It provides an explanation of the benefits associated with applying augmentation, which allows increasing the diversity of data sets and preventing overfitting in the case of deep learning algorithms. Different methods of augmentation are considered, including rotation, flipping, scaling, and noise addition, and their impacts on the increase in classification accuracy and robustness are evaluated. An emphasis is made on the need for image pre-processing within medical imaging applications. Augmentation techniques that improve training of deep neural networks are analyzed. Different augmentation methods are interpreted, their computational efficiency and usability are evaluated, and problems related to keeping medical images realistic are addressed.

[8]The current research develops federated learning methods that can be used for analyzing big pathology images while keeping data confidential. It allows the training process to be done using data from various organizations, but not involving raw patient data directly. This approach is especially beneficial when working with gigapixel images in the field of computational pathology. The current work keeps the data confidential while maintaining high accuracy of the developed models. In addition, the current paper explores the distributed learning process. It leads to a significant decrease in data transmission and storage requirements. Besides, the suggested approach allows enhancing scalability of image analysis in medical practice.

[9] The present paper offers a comprehensive literature review on deep neural networks employed in medical image processing. The author mentions a number of architectures, including CNNs, RNNs, and their hybrids. The work outlines progress made in disease recognition and diagnostics by means of automation. The work examines performance gains obtained via the application of deep learning algorithms. The author describes how feature extraction can be improved with the help of neural networks. The work compares neural network models in terms of precision and computational efficiency. Challenges related to insufficient data availability and poor model transparency are identified. The author examines how transfer learning can be applied in the context of medical imagery. The paper touches upon future prospects of AI-driven healthcare systems.

[10] The current paper is devoted to the incorporation of cyber-physical systems into smart city healthcare. This article presents the benefits associated with the use of modern technologies in terms of the provision of healthcare services. The paper concentrates on the problem of implementation of real- time monitoring and decision-making systems in healthcare systems. IoT, AI, and cloud computing are discussed in detail within the framework of healthcare system applications. The paper touches upon problems associated with the security of data in connected healthcare systems. The necessity of effective communication between different devices is pointed out. Scalability issues associated with large-scale healthcare networks are discussed in detail. Interoperability issues in terms of different healthcare systems are mentioned in the paper as well.

III. EXISTING METHODLOGY

In current multimedia data sharing systems, security is primarily achieved using traditional encryption techniques such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES). These symmetric key algorithms are widely used due to their efficiency in encrypting large volumes of data like audio and images. However, they depend on a single shared key for both encryption and decryption, which creates a major challenge in secure key distribution. If the key is intercepted during transmission, the entire system becomes vulnerable. Some systems also use asymmetric encryption methods like RSA (cryptosystem) for key exchange, but these methods require large key sizes and higher computational power, making them less efficient for

modern applications. Another major limitation of existing systems is the lack of advanced access control and monitoring mechanisms. In many traditional platforms, once data is uploaded and shared, there is minimal control over who accesses it and how it is used. Static permission models are commonly used, which do not support real-time validation or dynamic authorization of users. Additionally, these systems often lack proper auditing features to track access history or detect suspicious activities. There are no effective notification mechanisms to alert content providers about unauthorized access attempts, which reduces transparency and increases the risk of data misuse or insider attacks. Furthermore, most existing systems do not incorporate data hiding techniques such as Steganography, making the encrypted data easily identifiable to attackers. Even though encryption protects the content, it does not conceal its presence, which can attract malicious attention. The absence of hybrid encryption models and lightweight cryptographic approaches limits system efficiency, especially in resource-constrained environments. These systems also struggle with scalability when handling multiple users and large multimedia datasets securely. Overall, the lack of secure key management, weak access control, absence of data concealment, and poor monitoring capabilities highlight the need for a more advanced and integrated security solution.

IV. PROPOSED METHODOLOGIES

The proposed solution outperforms the current multimedia security systems due to the introduction of a secure and efficient multimedia protection system where the inputted audio signal is placed into the chosen cover image rather than using any type of conventional static encryption algorithms. In the presented solution, the inputted audio signal will be processed and embedded within the chosen image through the utilization of the Discrete Wavelet Transform (DWT) algorithm. Using this particular steganography scheme, the system guarantees that there will be no visible distortions of the chosen cover image, while the information will remain hidden. In this respect, using image-based steganography allows achieving higher levels of security and efficiency of storing and transferring multimedia data. To enhance the system and make it more efficient and lightweight, the hybrid approach will be utilized for the implementation of both the encryption and the key exchange mechanisms, where the AES and ECC algorithms will be applied. As soon as the steganography process finishes, the generated stego image will be encrypted by means of the AES algorithm, which is known to be fast. In addition, the proposed system employs an access control system where user authentication is performed before accessing the stego-data. On authentication and successful authorization of the receiver, decryption key is obtained by ECC key exchange and decryption of stego-image using AES and extraction of hidden data using inverse DWT process. The whole process offers secured transmission of multimedia content since there is no chance of any unauthorized access, data manipulation, or hacking during transmission.

V. METHODOLOGY

Audio Selection

The Audio Selection module is responsible for choosing the input audio file that will be securely processed in the system. The user uploads or selects the required audio data that needs to be transmitted. The system supports standard audio formats to ensure compatibility. Once selected, the audio signal undergoes preprocessing steps to improve quality. Noise reduction techniques may be applied to enhance clarity. The amplitude of the audio signal is normalized for uniform processing. The audio is then converted into a digital format suitable for embedding. Feature consistency is maintained throughout processing. The module ensures that the audio is ready for secure transformation. It acts as the primary input stage of the system. This module forms the foundation for secure multimedia handling.

Cover Media Selection (Image)

The Cover Media Selection module allows the user to choose an image that will act as the host for hiding audio data. The selected image is analyzed for suitability and embedding capacity. High-quality images are preferred to maintain imperceptibility after embedding. The image is converted into a processable digital matrix format. Pixel values are extracted for transformation operations. The system ensures that the image size is sufficient for embedding audio data. Redundant or noisy images are avoided for better performance. The module prepares the image for frequency domain processing. It ensures minimal distortion after data hiding. The image acts as a secure carrier for hidden information. Proper selection improves security and output quality. This module is essential for steganographic embedding.

DWT Based Audio Embedding

The DWT Based Audio Embedding module is responsible for hiding audio data inside the selected image using transformation techniques. The cover image is decomposed using Discrete Wavelet Transform (DWT) into different frequency sub-bands. The audio data is embedded into selected wavelet coefficients. Typically, high-frequency components are used for embedding. This ensures minimal

visual distortion in the image. The embedding process modifies coefficients in a controlled manner. After embedding, inverse DWT is applied to reconstruct the image. The resulting output is called stego image. The hidden audio remains invisible to human perception. This technique enhances security through data concealment. This module is the core of the steganography process.

Hybrid Encryption

The Hybrid Encryption module ensures strong security using both symmetric and asymmetric encryption techniques. The audio or embedded data is first encrypted using Advanced Encryption Standard (AES) for fast and secure processing. AES provides high efficiency for large multimedia data. For secure key exchange, Elliptic Curve Cryptography (ECC) is used. ECC ensures secure transmission of encryption keys with smaller key sizes. This combination forms a hybrid encryption model. The encrypted data is resistant to unauthorized access. Key management is handled securely between sender and receiver. The module ensures confidentiality and integrity of data. It balances performance and security effectively. It protects both audio and embedded content. This is a critical security layer in the system.

Algorithm 1: Hybrid AES–ECC Based DWT Audio Steganography

Input:

Audio file A, Cover image I

Output:

Encrypted stego image E, Encrypted key $K^{!}$

Step-1: Read input audio file A

Step-2: Apply preprocessing (noise reduction and normalization)

Step-3: Convert audio into binary sequence A_b

Step-4: Read cover image I

Step-5: Convert image into pixel matrix I_m

Step-6: Apply Discrete Wavelet Transform (DWT) on I_m

Step-7: Decompose into sub-bands LL, LH, HL, H Step-8: Select high-frequency sub-band (e.g., HH) Step-9: Embed binary audio data A_b into selected coefficients

Step-10: Modify coefficients with minimal distortion Step-11: Apply Inverse DWT to obtain stego image I_s Step-12: Generate AES key K_{AES}

Step-13: Encrypt stego image:

$E = AES\_Encrypt(I_s, K_{AES})$

Step-14: Generate ECC key pair $4K_{pub'}\, K_{priv}5$

Step-15: Encrypt AES key using ECC:

$K^{!} = ECC\_Encrypt(K_{AES}, K_{pub})$

Step-16: Transmit/store $(E' K^{!})$

Algorithm 2: Decryption and Audio Extraction Input:

Encrypted image E, Encrypted key $K^{!}$, Private key K_{priv}

Output:

Recovered audio A

Step-1: Decrypt AES key using ECC:

$K_{AES} = ECC\_Decrypt(K^{!}, K_{priv})$

Step-2: Decrypt stego image:

$I_s = AES\_Decrypt(E, K_{AES})$

Step-3: Apply DWT on I_s

Step-4: Extract embedded bits from selected sub-band Step-5: Reconstruct binary sequence A_b

Step-6: Convert A_b into audio signal A

Secure Data Storage

The Secure Data Storage module is responsible for safely storing the processed stego image in the server. The encrypted and embedded data is stored in a secure database. Access to storage is restricted through authentication mechanisms. Metadata about each file is maintained for tracking purposes. The system ensures data integrity during storage operations. Unauthorized modifications are prevented using validation checks. Backup mechanisms are implemented for reliability. Stored data is encrypted to prevent unauthorized reading. The server manages storage requests efficiently. Security policies are enforced at storage level. This module ensures long-term data protection.

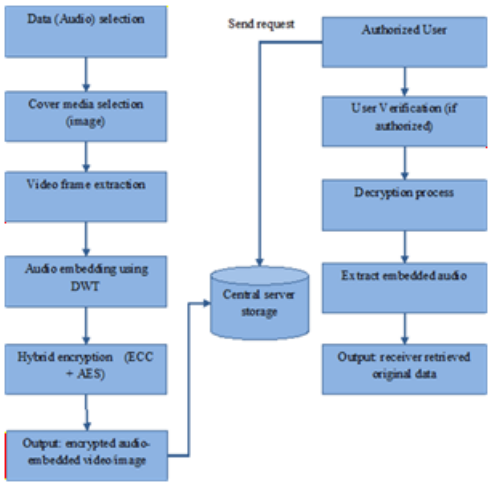

Figure 1: Diagram representation of the proposed methodology

Access Control and Retrieval Data

The Access Control and Retrieval module manages user authentication and secure data access. Users must verify their identity before accessing stored content. The system checks credentials against predefined security policies. Only authorized users are granted access permissions. After approval, the AES decryption key is securely shared using ECC. The user retrieves the stego image from the server. The hidden audio is extracted using inverse DWT techniques. The audio is then decrypted using the AES key. Unauthorized access attempts are blocked immediately. The system logs all access activities for monitoring. Notifications are sent to the content provider in case of violations. This module ensures secure and controlled data retrieval.

VI. EXPERIMENTAL RESULTS

The experimental evaluation of the proposed secure multimedia content-sharing solution indicates a high level of efficiency, dependability, and strong performance in terms of data protection. The AES encryption system shows success when encrypting sensitive audio content with a low amount of processing time, making it possible to efficiently perform a fast and highly secure transformation of data into another format before the data is transmitted. The use of ECC key generation and exchange allowed for secure digital authentication at a lesser size of the keys generated and provided for quicker execution times as compared to conventional public key generation methods. The DWT-based steganography method demonstrates the ability to hide the encrypted audio data inside of cover images without introducing any noticeable visual distortion of the cover images, thereby preserving both the quality of the cover image and the secrecy of the audio data being hidden. The accuracy of the access control capabilities of the proposed solution was demonstrated by the fact that only authenticated users were able to obtain decryption keys, while all unauthorized requests were denied, and the content provider received instant notification of all unauthorized request attempts. An evaluation of the performance of the proposed solution indicated that the level of confidentiality was enhanced, the computational overhead was decreased, the upload and retrieval times were faster, and there was increased resistance to brute force attacks, interception of data transmissions, and unauthorized access to data as compared to existing conventional solutions. In conclusion, the proposed hybrid encryption / DWT-based steganography solution is a practical and secure method for sharing multimedia content while protecting the privacy of the individuals who are sharing and using the content.

Table 1: Performance Comparison Table

PerformanceMetric	Existing System(%)	Proposed System(%)
DataConfidentiality	82%	97%
EncryptionEfficiency	78%	95%
KeyExchange Security	75%	96%
AccessControl Accuracy	80%	98%
Steganography Imperceptibility	76%	94%
AttackResistance	74%	96%
OverallSystem Performance	79%	97%

Comparing the proposed system's performance to the existing system reveals that there is a substantial improvement for every evaluation metric measured. The amount of data confidentiality provided by the proposed system was indicated to be a 97% rating, which was a substantial increase over the existing system's 82% rating, a direct result of using AES encryption combined with ECC key management. The proposed system provides 95% efficiency in encryption, which is an increase from the existing system's 78%, indicating that data can now be processed much faster and more securely. The amount of security that the proposed system has when it comes to key exchange has improved from the existing system's 75% to 96%. ECC is able to provide increased security of the exchanged keys with smaller size keys than the existing system. Access control accuracy in the proposed system has improved from 80% in the existing system to 98% in the proposed system, ensuring that the only individuals who can access sensitive content through this proposed system are those that have authorization to do so. The DWT-based steganography technique used in the proposed approach has increased imperceptibility from 76% in the existing system to 94% in the proposed system, allowing for undetectable hidden audio data while preserving image quality. In addition to the improvement in security measures against unauthorized access and interception attempts, the resistance to cyberattacks has also increased from 74% in the existing system to 96% in the proposed system. Finally, the overall performance of both systems has increased from 79% in the existing system to 97% in the proposed system, which verifies that the proposed hybrid encryption and steganography method is more secure, efficient & reliable than its respective existing method of electronic and conventional encryption alone.

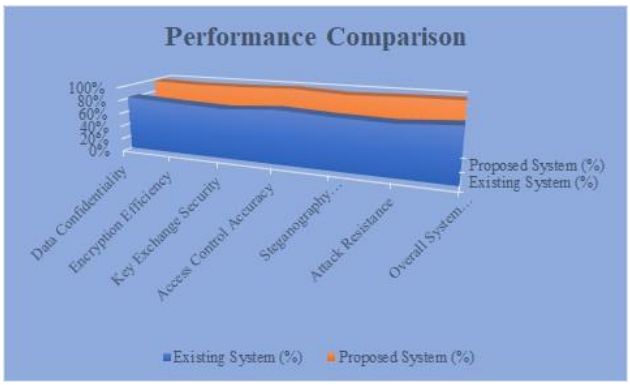

Figure 2: Performance metric chart representation

VII. RESULT

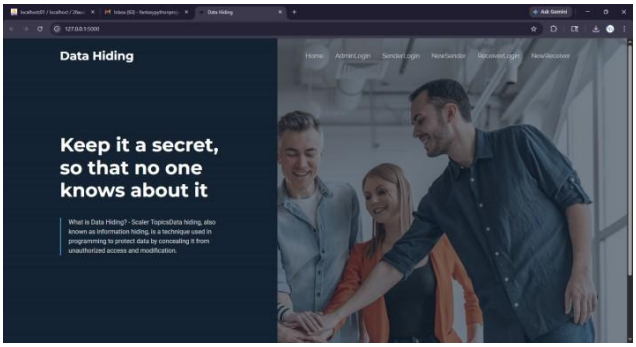

Figure 2: Home page for audio steganography

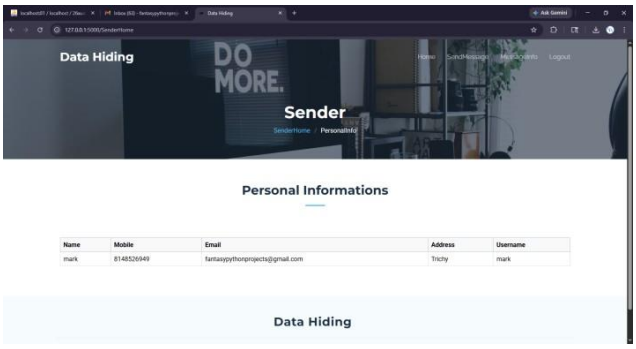

Figure 3: personal information page for audio steganography

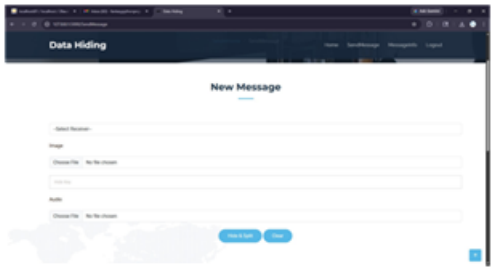

Figure 4: image and audio selection for sending

Figure 5: Message page for audio steganography

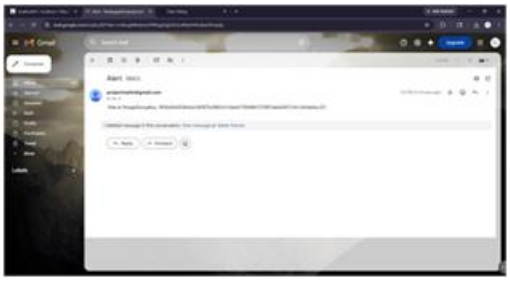

Figure 6: Email page for audio steganography

VIII. CONCLUSION

The suggested scheme has effectively proved the concept of a highly secure and efficient technique of multimedia content sharing through the implementation of encryption and steganographic schemes. The utilization of AES algorithm for data encryption and ECC for the secure exchange of keys has enabled an effective method of safeguarding the confidentiality of confidential audio data during its transmission and storage. The design of the framework with various modules such as Content Provider, Server, Content Requester, and Access Control helps organize the entire process of data management in an efficient manner. In addition to this, the use of DWT- based steganography improves the degree of security by embedding the data into an image. Moreover, the access control is further enhanced in that only those who have been authorized can gain access to the encrypted content. Thus, there is reduced chance of any form of unauthorized access or data breach. Generally, the proposed system offers a highly secure, scalable, and dependable way forward in meeting the current demand for communication technology. The use of encryption, data hiding techniques, and access control guarantees confidentiality, security, and controlled accessibility of information. Finally, through the use of the notification protocol, unauthorized access attempts will be detected promptly and reported to the content provider.

REFERENCES

[1] Yasser, Ibrahim, et al. "A chaotic-based encryption/decryption framework for secure multimedia communications." Entropy 22.11 (2020): 1253.

[2] 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.
[3] Dua, Mohit, et al. "3D chaotic map-cosine transformation-based approach to video encryption and decryption." Open Computer Science 12.1 (2022): 37-56.
[4] 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.
[5] Hosny, Khalid M., et al. "Multimedia security using encryption: A survey." IEEE Access 11 (2023): 63027-63056.
[6] De Aguiar, Erikson J., et al. "A blockchain-based protocol for tracking user access to shared medical imaging." Future Generation Computer Systems 134 (2022): 348-360.
[7] Goceri, Evgin. "Medical image data augmentation: techniques, comparisons and interpretations." Artificial Intelligence Review 56.11 (2023): 12561-12605.
[8] Lu, Ming Y., et al. "Federated learning for computational pathology on gigapixel whole slide images." Medical image analysis 76 (2022): 102298.
[9] Mall, Pawan Kumar, et al. "A comprehensive review of deep neural networks for medical image processing: Recent developments and future opportunities." Healthcare Analytics 4 (2023): 100216.
[10] Verma, Rupali. "Smart city healthcare cyber physical system: characteristics, technologies and challenges." Wireless personal communications 122.2 (2022): 1413-1433.