SECURE MULTIMEDIA CONTENT SHARING USING HYBRID ECC-AES ENCRYPTION WITH REAL-TIME ACCESS CONTROL

[1]Sathiyapriya P, [2]Muthusamy P, [3]Kavya M, [4]Priyadharshini S, [5]Rohini M

[1] Assistant Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[2]Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[3,4,5]Student, Department of CSE(Cyber Security), Muthayammal Engineering College.

[1]sathiyapriya18mec@gmail.com, [2]mpmmuthu6@gmail.com, [3]kavyamurugesan7@gmail.com,

[4]priyadharshinisellamuthu2004@gmail.com, [5]rohinimaham1721@gmail.com

ABSTRACT

In the modern digital era, secure sharing of multimedia content such as audio, images, and videos has become a critical requirement in communication and information exchange. Traditional image-based steganographic techniques limit scalability and are inefficient for handling large multimedia files. To address these challenges, this project presents a robust and scalable secure multimedia content- sharing framework that integrates advanced steganography with hybrid cryptographic techniques. The proposed system embeds audio data within video files instead of static images, enabling enhanced flexibility and improved capacity for large-scale multimedia protection. The video is first decomposed into frames, and selected frames undergo Discrete Wavelet Transform (DWT)-based audio embedding. To further strengthen security, a hybrid encryption approach is employed, where Elliptic Curve Cryptography (ECC) ensures secure key generation and the Advanced Encryption Standard (AES) provides efficient data encryption. This dual-layer security mechanism guarantees confidentiality, integrity, and resistance to unauthorized access while preserving the visual quality of the video.

KEYWORDS – Secure Multimedia Communication, Video Steganography, Audio Embedding, Discrete Wavelet Transform (DWT), Hybrid Cryptography, Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), Multimedia Data Security, Confidential Content Sharing.

1. INTRODUCTION

In today's digitally connected world, multimedia data such as audio, images, and videos plays a vital role in communication and information exchange. With the rapid growth of online sharing platforms and cloud services, ensuring the security and privacy of sensitive multimedia content has become a major concern. Unauthorized access, data tampering, and misuse of confidential media highlight the need for stronger protection mechanisms. Conventional security methods, including basic encryption and image-based data hiding

techniques, are limited in capacity and scalability. Existing systems commonly embed audio within images using Discrete Wavelet Transform (DWT) and apply hybrid encryption with Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). Although effective, these approaches are unsuitable for large or high-resolution multimedia content.

To address these challenges, the proposed system introduces a video-based audio embedding framework integrated with hybrid ECC–AES encryption. By embedding audio into selected video frames using DWT, the system enhances security, scalability, and data-handling capability while preserving multimedia quality. This approach offers an efficient and robust solution for secure multimedia sharing in applications such as digital communication, medical data transmission, and confidential media distribution.

1.1 SCOPE OF THIS PROJECT

This project aims to:

- To develop a secure multimedia sharing system using video-based steganography and hybrid encryption.
- To embed audio data into video frames using Discrete Wavelet Transform (DWT).
- To apply hybrid ECC–AES encryption to ensure data confidentiality and integrity.
- To support secure transmission and accurate retrieval of multimedia content.
- To maintain multimedia quality while enhancing security and scalability.

The framework is intended for secure multimedia communication over digital and cloud platforms, providing efficient protection for sensitive audio-video content.

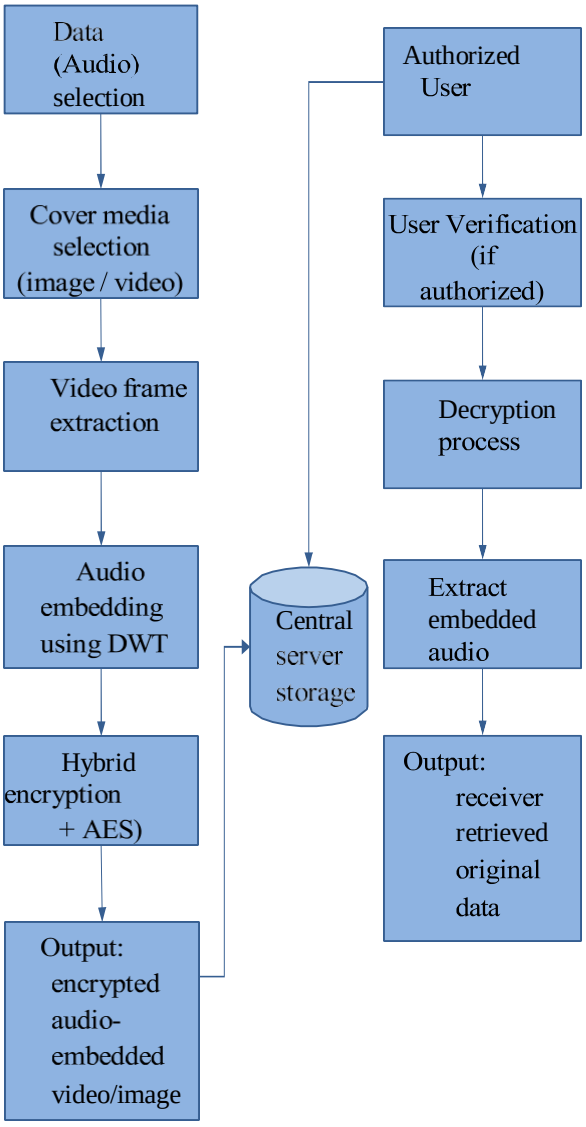
2. PROPOSED WORK

This project proposes the development of a secure multimedia sharing framework that embeds audio data within video files to achieve scalable and flexible content protection.

The system converts video data into individual frames and applies Discrete Wavelet Transform (DWT)-based steganography to imperceptibly embed audio content while preserving multimedia quality. By integrating a hybrid cryptographic approach, the framework utilizes Elliptic Curve Cryptography (ECC) for secure key generation and Advanced Encryption Standard (AES) for efficient data encryption. This dual-layer security mechanism ensures confidentiality, integrity, and resistance against unauthorized access or tampering during multimedia transmission.

The proposed system aims to provide a robust, efficient, and scalable solution for secure multimedia sharing in applications such as digital communication, cloud storage, and confidential media distribution.

2.1 System Architecture



3.1 Data Processing & Preprocessing

To ensure secure multimedia transmission and controlled access, the proposed system employs a structured data processing and preprocessing pipeline based on the following processes:

- **Data (Audio) Selection:** The system begins by selecting sensitive audio data intended for secure transmission.
- **Cover Media Selection (Image/Video):** A suitable cover image or video is selected to hide the audio data while ensuring minimal perceptual distortion after embedding.
- **Video Frame Extraction:** When a video is used as the cover medium, individual frames are extracted to enable efficient data embedding.
- **Output – Receiver Retrieved Original Data:** Finally, the authorized receiver securely retrieves the original audio data with ensured confidentiality and access control.

3.2 Secure Multimedia Processing and Access Control

3.2.1 Hybrid Encryption-Based Multimedia Security:

This module uses a hybrid ECC–AES encryption approach to secure audio- embedded multimedia content, where ECC handles secure key generation and AES performs efficient data encryption, ensuring confidentiality and protection against unauthorized access.

3.2.2 Real-Time Access Control and Secure Data Retrieval:

The real-time access control module authenticates authorized users before permitting decryption and extraction of embedded audio, ensuring secure access, data protection, and accurate retrieval without quality loss.

3.3 TOOLS AND LIBRARIES

The Secure Multimedia Content Sharing framework employs the following technologies:

- Python: Used for steganography, hybrid ECC–AES encryption, and multimedia processing.
- OpenCV: Used for video processing, frame extraction, and frame reconstruction during audio embedding and retrieval.
- Cryptography Library (ECC & AES): Hybrid encryption using ECC for key generation and AES for data encryption/decryption.
- NumPy: Supports numerical computations and efficient manipulation of audio and video data arrays.
- FFmpeg: Handles multimedia format conversion, audio extraction, and video encoding/decoding operations.
- MySQL: Manages secure storage of user credentials, access control data, and encryption-related metadata.
- PyCharm IDE: Used as the development environment for coding, testing, and debugging the system modules.

4. PROGRAM

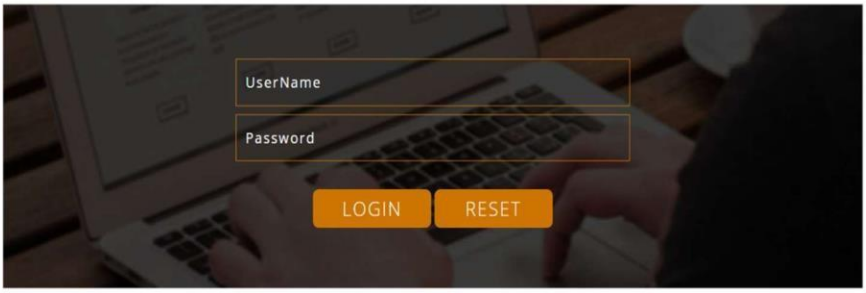
```
from flask import Flask, render_template, request, session, send_file, flash
import mysql.connector
import os

app = Flask(__name__)
app.config['SECRET_KEY'] =
'aaa'

2. Database
Connection def
db_connection():
    return
        mysql.connector.connect
        ( host='localhost',
        user='root',
        password='',
        database='1imageaudiovideoendb'
    )

3. User Authentication (Sender Login)
@app.route("/senderlogin",
methods=['POST']) def senderlogin():
    username = request.form['uname']
    password = request.form['password']
    session['sname'] = username

    conn            =
```

```
        (username, password)
    )
    data = cursor.fetchone()

    if data:
        flash("Login Successful")
        return render_template('SenderHome.html')
    else:
        flash("Invalid Username or Password")
        return render_template('SenderLogin.html')

4. Encryption and Decryption Module (ECC +
AES) from ecies.utils import generate_key
import pyAesCrypt
def encrypt(key, source, destination):
    pyAesCrypt.encryptFile(source, destination, key)

def decrypt(key, source, destination):
    pyAesCrypt.decryptFile(source, destination, key)

5. Image    Upload    and    Encryption
@app.route("/imupload",
methods=['POST']) def imupload():
    file = request.files['file']
    receiver =
    request.form['rname']

    filename = file.filename
    upload_path = "static/upload/" + filename
    encrypt_path = "static/Encrypt/" + filename

    file.save(upload_path)

    keypair = generate_key()
    public_key = keypair.public_key.format(True).hex()
    encrypt(public_key, upload_path, encrypt_path)

    conn                =
    db_connection()
    cursor              =
    conn.cursor()
    cursor.execute(
        "INSERT INTO msgtb VALUES ('','%s','%s','%s','%s','image')" %
        (session['sname'], receiver, filename, public_key)
    )
    conn.commit()

    flash("Image Encrypted Successfully")
    return render_template('SendMessage.html', prikey=public_key)
```

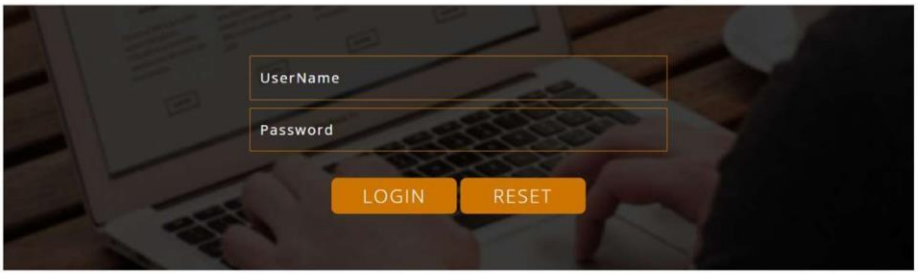
```
6. Decryption Process (Receiver
     Side) @app.route("/fdecrypt",
     methods=['POST']) def
     fdecrypt():
     key = request.form['hkey']
     filename = request.form['filename']
    encrypted_file = "static/Encrypt/" +
    filename decrypted_file =
    "static/Decrypt/" + filename

    decrypt(key, encrypted_file, decrypted_file)
    return send_file(decrypted_file, as_attachment=True)

7. Email Notification
Module def
sendmail(to_mail, message):
    import smtplib
    from email.mime.text import MIMEText

    sender = "projectmailm@gmail.com"
    password = "xxxxxxxxxxxx"

    msg = MIMEText(message)
    msg['Subject'] = "Secure Message
    Alert" msg['From'] = sender
    msg['To'] = to_mail

    server = smtplib.SMTP('smtp.gmail.com', 587)
    server.starttls()
```

5. RESULTS AND OUTPUT

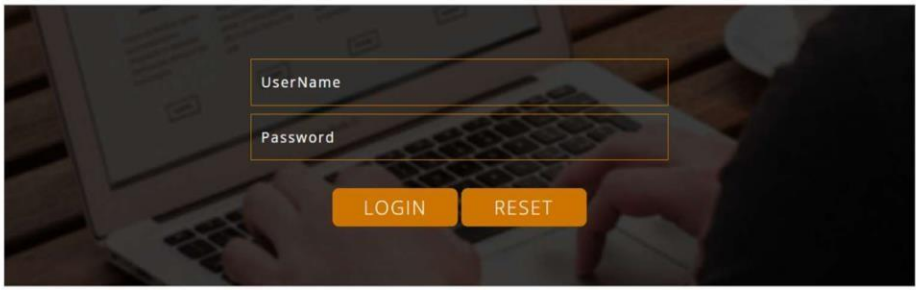
Admin Login



Sender Login



Receiver Login



6. CONCLUSION

The proposed project effectively integrates video-based steganography with hybrid ECC–AES encryption to ensure secure multimedia content sharing. By embedding audio data within video frames using Discrete Wavelet Transform (DWT), the system enhances scalability while preserving multimedia quality. The hybrid encryption mechanism safeguards the embedded content against unauthorized access and tampering. Overall, the system addresses the limitations of traditional image-based approaches and provides a robust, efficient, and secure solution for modern multimedia communication.

REFERENCES

[1] K. M. Hosny et al., "Multimedia security using encryption: A survey," IEEE Access, vol. 11, pp. 63027–63056, 2023.

[2] I. Yasser et al., "A chaotic-based encryption/decryption framework for secure multimedia communications," Entropy, vol. 22, no. 11, p. 1253, 2020.

[3] E. A. Albahrani, T. K. Alshekly, and S. H. Lafta, "A review on audio encryption algorithms using chaos maps-based techniques," Journal of Cyber Security and Mobility, pp. 53–82, 2022.

[4] M. Dua et al., "3D chaotic map–cosine transformation-based approach to video encryption and decryption," Open Computer Science, vol. 12, no. 1, pp. 37–56, 2022.

[5] U. Zia et al., "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," International Journal of Information Security.

[6] E. J. De Aguiar et al., "A blockchain- based protocol for tracking user access to shared medical imaging," Future Generation Computer Systems, vol. 134,
pp. 348–360, 2022.

[7] E. Goceri, "Medical image data augmentation: techniques, comparisons and interpretations," Artificial Intelligence Review, vol. 56, no. 11, pp. 12561–12605,
2023.

[8] Singh, Ajay, and Rakesh Kumar. "Hybrid AES–ECC based secure multimedia transmission with enhanced key management." International Journal of Information Security.

[9] Al-Husainy, Mahmoud A., et al. "Secure video steganography using discrete wavelet transform and encryption techniques." Multimedia Tools and Applications.

[10] Kumar, Sanjeev, and Pradeep Kumar Singh. "An efficient video steganography approach using DWT and AES encryption." Journal of Information Security and Applications, vol. 58, pp. 102735, 2021.