Robust Encryption And Decryption Techniques For Multimedia Using AES And Triple DES

Kathi Yeshwanth, Kundrapu Vineetha, Md Jaffer Ali, N Prathima, Vishwas H N
Dept. of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, India,
bl.en.u4cse21096@bl.students.amrita.edu , bl.en.u4cse21106@bl.students.amrita.edu, bl.en.u4cse21124@bl.students.amrita.edu , bl.en.u4cse21132@bl.students.amrita.edu, hn_vishwas@blr.amrita.edu

***Abstract*—The multimedia Encryption and Decryption employing Triple DES and AES uses strong encryption methods to address the ongoing issue of illegal access to digital images, Audio and Video. Triple Data Encryption Standard, also known as Triple DES, is a safe symmetric-key encryption method that is used because it can offer increased security by using triple encryption and combining in both the encryption and decryption processes. When it comes to processing speed, Triple DES is slower than more efficient algorithms like Advanced Encryption Standard (AES), but it still provides strong protection for a variety of Multimedia types, including private medical photographs and financial information. The application of technologies like HTML, CSS, and Flask in the project allows for the development of a complete solution for protecting visual data on web platforms. Through the integration of Triple DES and AES into a web-based framework, the research not only addresses the crucial need for image security but also shows how encryption methods can be used in real-world situations to strengthen digital defenses against unwanted access and possible data breaches.**

Keywords— Confidentiality, Unauthorized Access, Symmetric-Key Encryption, Cryptographic Techniques, Digital Image Security, Data Encryption Standard, Advanced Encryption Standard.

I. INTRODUCTION

The security of multimedia data holds immense significance With the widespread utilization of digital media in communication, entertainment, and information exchange, it is crucial to ensure the protection of sensitive information against unauthorized access and cyber risks. Multimedia data, encompassing images, voice recordings, and video files, frequently contains confidential and personal details. Any compromise in its security could result in severe privacy breaches and substantial financial repercussions.

To address these security concerns, the research is cantered around the implementation of strong encryption and decryption methods tailored for multimedia content By utilizing the advantages of two well-known cryptographic algorithms - Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES) - the goal is to create a thorough security structure. AES is highly regarded for its effectiveness and robust encryption features, making it a popular option for safeguarding data in different scenarios. Conversely, Triple DES provides heightened security with its multiple encryption steps, adding an extra level of protection.

When it comes to data security, multimedia poses different issues than text-based data. Multimedia files come in a lot of different formats and sizes, thus encryption techniques that can process vast volumes of data effectively are needed. Multimedia data must also be safeguarded while transmission over networks, which are vulnerable to malevolent actors' interception and manipulation, as well as during storage.

The study focuses on building strong encryption and decryption techniques made especially for multimedia content in order to overcome these issues. To do this, cryptographic algorithms that offer strong security without sacrificing efficiency are used. The Triple Data Encryption Standard (Triple DES) and the Advanced Encryption Standard (AES) are two examples of these algorithms.

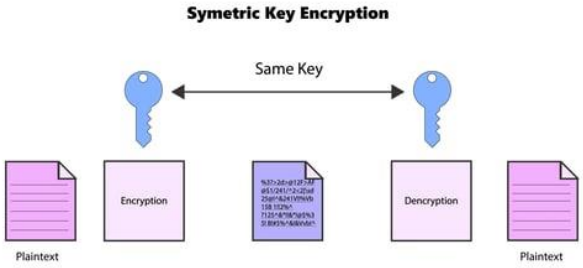

Fig. 1. symmetric key encryption.

The image above illustrates symmetric key encryption in action by showing how one key is used to encrypt and decrypt data. Data in plaintext is initially displayed on the image's left side. A symmetric key is used to encrypt this plaintext, producing a ciphertext—a format of the original data that is jumbled and unintelligible—that is placed in the middle. The information is secure and difficult for unauthorized parties to decipher thanks to the ciphertext. The same symmetric key is used throughout the decryption process to recover the original data, transforming the ciphertext back into plaintext as seen on the right side of the picture. This approach demonstrates the effectiveness and ease of use of symmetric key encryption, in which the same key confers security and accessibility. In order to preserve the integrity and confidentiality of the encrypted data, it is imperative to safeguard the key from unauthorized access.

By integrating AES and Triple DES, the research aims to develop a comprehensive security framework that addresses the diverse needs of multimedia data protection. AES's efficiency and strong encryption features make it ideal for general-purpose encryption, while Triple DES's multiple encryption steps provide an extra layer of security for highly sensitive applications. This dual approach ensures that multimedia data remains secure against a wide range of cyber threats, both during storage and transmission. Ensuring the confidentiality and integrity of sensitive information. By addressing the unique challenges of multimedia security, this research contributes to the development of secure digital media environments, ultimately protecting users' privacy and mitigating the risks associated with data breaches.

II. RELATED WORKS

[1] Chen Chen et.al. This paper presents a novel RSE algorithm for HEVC video bitstream encryption. In order to enhance security and performance of video encryption about a randomize-select sequence (RSS) proposed on the RC4 algorithm for AES – CTR encryption has been used. In particular, such aspects of available algorithms as flexibility, security measures, and efficiency can be viewed as the characteristics of RSE which are enhanced in comparisons with these algorithms. Measure of visual degradation, PSNR, SSIM, the flexibility of encryption location, Security enhancement are used for evaluation. The main objectives of this study will be to offer a nearly random encryption algorithm that can be practically applied in HEVC video bitstreams; it should also be able to guarantee that video compression and the above encryption algorithm are unrelated; additionally, it should be able to uphold low time complexity and higher security for cryptographic applications in compression of videos.

[2] Balajee Maram. The paper derives a framework that brings together encryption and steganography methods for safe communication through electronic photos, forecasts confidentiality and robustness of exposed message content, and discusses the relevance of the methods in securing information for functions such as military combat and financial trades. It includes inventing an image steganography plan safe and sound against lossy compaction and high-pass filtering: organizing an adjustable information covering formula, testing assorted compaction algorithms and ratios, estimating effectiveness using criteria such as PSNR and SSIM, testing the domain resistant to assaults, and comparing with related strategies. Outcomes measured are security and confidentiality of digital communication.

[3] Xin Huang et.al. This paper presents a Chaotic-based encryption method for video encryption in order to be used in the secure video streaming This method shows a high quality of encryption, sensitive to the keys, low correlation between pixels, and also find an effective correlation reduction among pixels. The methodology includes the designing and development of Chaotic-based encryption/decryption scheme for ACM and LM employing security analysis and calculations through histograms and pixel correlation. Results comprise of reduced dependence of corresponding pixels, a balanced histogram distribution for encrypted images, lossless decryption. They are: Designing an effective and secure cryptosystem for protecting the privacy of the VIP video streams; Outline and propose a Chaotic-based encryption scheme; Improve encryption quality; Ensure key sensitivity; Low correlation between the pixels; Comparison results between secured video frames; Statistical and correlation analysis.

[4] Sonali Guhe et.al. The paper proposes a method for the encryption of videos using chaotic functions Arnold's Cat Map and Logistic Map which are utilized for the pixel and frame permutations for security purposes. The techniques employed include the integration of chaotic functions and maps in the encryption/decryption setups, partitions of videos into frames, transforms on pixels, Arnold's Cat Map, logistic maps, and others for the manipulation of digital media. The primary or principal outcome of the study in the paper under consideration is the creation of an original technique for cryptography of video signals with the use of chaotic functions and maps. objective includes creating a distinct approach for performing video cryptography cantered on chaotic functions and focusing on video encryption in the context of digital media.

[5] Ahmed Maache et.al. It is related to hardware design of real-time video encryption/decryption system with AES-128 algorithm for Secure Online Communications based on low-cost FPGA board to reduce execution time for low-performance platform. It included the comparison of several HPS-based systems designs, the comparison of several HPS-based implementations of the AES-128 algorithm, designing the Qsys system for raw video input capture, as well as C programming of comparison hardware AES-128 algorithms with 128-bit keys – AES-128. Hence the faster implementation achieved over the software implementation, resources consumed by the design in LEs for-logic elements, Block Memory, and DSP blocks for the Cyclone-V FPGA.

[6] Christy Atika Sari et.al. Focusing on the topic the paper emphasizes that internet security is crucial; the need for 3DES cryptography and EOF steganography to secure the data results in effective image processing which is efficient in quality. The methodology includes designing and developing the computer algorithm for both encryption and decryption using the 3DES algorithm for secret key cryptography and substitution-permutation network, cryptography, image encryption, LSB in binary numbers, PSNR measurement as the comparison parameter, and image analysis comparison. PSNR values are expressed in dB. The main study goals are the use of the 3DES cryptography for digital image protection and application of the EOF steganography for the digital image security.

[7] S Sakthipriya et.al. The paper addresses issues like why data security is essential, image transfer through cryptography, and the link between an algorithm and data security wherein the paper concludes that TDES is the most suitable algorithm for ensuring data security. The methodology utilizes algorithms of Triple Data Encryption Standard (TDES) and Data Encryption Standard (DES) with specified key lengths for encryption and decryption of images. Performance of Triple Data Encryption Standard (TDES) and Data Encryption Standard (DES) in transferring images over a network.

[8] A.O Akinrotimi et.al. The paper under review emphasizes the significance of image encryption during secure information transmission, focuses on DES algorithm for encryption of iris images, and claims that the system presented in the paper, where the encryption and decryption of CASIA iris images were performed in MATLAB environment, shows slower encryption but faster decryption and concludes that DES algorithm may be used for providing strong security measures for iris images. In terms of the methodology, DES algorithm for encrypting iris images, implementing the system in MATLAB environment and decryption speed/encryption speed/memory usage etc.

[9] Divya Vadlamudi et.al. The Triple DES cryptographic method and steganography to hide encrypted data behind images are out as the key technical approaches mentioned in the paper that is mostly aimed at the problem of data security when speaking of cryptography. It also describes the Triple Data Encryption Algorithm (TDEA) as a block cipher and the use of this cipher to encrypt information. It includes the triple

DES method to encrypt images and can be integrated with reversible data hiding (RDH) for the transmission of information hidden in an image. Future works may include improving the security and reliability of encrypted techniques, possibly in proposing a more effective system for reverse encryption of images using the advanced encryption standard algorithm and triple DES algorithm. Further research in more sophisticated methods of information steganography and cryptography to be used in securing information in communication processes will also be another fruitful area of study.

[10] Junghwan Kim et.al. The paper aims to overcome this issue by providing a solution to improve data security in wireless communication by applying AES block cipher in CTR mode to encrypt Audio and Image files which proves successful encryption and decryption of the files. The methodology involves the use of AES counter mode in the process of encrypting the audio and image files to make sure that it is both fast and secure to encrypt. The study's goals are to improve information security and distribute data communication, integrate AES block cipher for audio and image encryption, and find out the practicality of CTR mode.

[11] Wangyi et.al. The paper presents a modified RSA encryption algorithm using meminductor chaos circuit in-depth information security and effective energy consumption and discusses the key issue that if the public key is encrypted, there are certain security risks due to the quantum computer. The methodology is entailing devising a meminductor chaos circuit and then suggesting alterations to the RSA encryption algorithm; Step by step procedure of the encryption algorithm has been explained briefly; Description of meminductor based chaotic circuit and its equations for numerical analysis has been provided. Possible future research could include studying meminductor based chaotic systems in secure communication and developing more secure encryption methods in relation to quantum computing. The development and possible implementation and testing of the improved encryption algorithm is another path that future research could take.

[12] Manohar N et.al. In this paper we try to define Video Steganography for secure communication, and we here propose a system that uses SLSB method, Fuzzy logic and Neural Network for better result, more efficiency and more security. The technique used in the study includes the use of Neural Networks, Secured LSB method, and Fuzzy logic for video steganography embedding of data by Secure base LSB method fuzzy logic functions and transport of logic and data Neural Networks for inputs and outputs. Assess the effectiveness of the proposed techniques based on PSNR/MSE information. Offer a comprehensive review on various steganography methods for steganography in Video Stream researchers.

[13] Divyashree. D et.al. The paper goes ahead to give reasons why information should be protected using cryptography and steganography then it gives an approach to use multimedia-based steganography, an evaluation on the performance of the approach using a mathematical model and lastly explains the process of embedding different types of files into video frames for steganography. The methodology used in the study is Multimedia based on steganography of information. Develop an extensive application of theory and techniques of Multimedia based steganography of information; discuss the technique/ methodology used for the proposed application; perform an evaluation/ analysis of the results with the help of a mathematical model and compare with other available methodologies.

[14] B. Vishnu et.al. The paper elaborates on the distinctive features of steganography, introduces the concept of PVD and Edge Detection in image steganography, and find out how secret data is embedded in image edges for security. It involves encrypting information using Image Steganography with PVD and Edge Detection techniques; converting secret text to decimal then binary; extracting the message and embedding it into edge regions using the PVD Method with a modulus function. The purpose of the research is to develop an improved image steganography mechanism based on the Edge Detection Algorithm (Canny Algorithm) and Pixel Value Differentiating (PVD) method to solve the problems caused by the LSB method, ensure the safety of the steganographic information, and provide double protection for the embedded text; take fixed image size into consideration; avoid quality loss in the resulting image; and improve security and robustness.

[15] Mohak Kataria et.al. The paper focuses on investigating the advancements in steganography and encryption algorithms to strengthen image transmission; the paper shows that using various kinds of techniques can enhance data security and stability. The approach included cryptography in which plaintext was encoded utilizing various encryption algorithms together with random color images; steganography in which the resultant ciphertext was hidden in cover images using LSB and Spread Spectrum techniques; and finally, performance evaluation of the derived stego-images by means of metrics including peak signal-to-noise ratio, mean square error, information entropy, and histograms. The specific aims of the study are to: Explore the use of modern Steganography applications for safe image transmission; Develop advanced Steganography applications to digital images for safe transmission of information; and to ascertain the better approach in integrating Steganography and Encryption in safe data transmission through pictures. The conducted study has proven the efficiency of steganography as a reliable means of communication which ensures the confidentiality of the provided information from the potentially numerous unlawful users' attempts to get access to the data; furthermore, it underlines the necessity for steganography to be implemented together with some encryption tool for the successful data transfer.

III. PROPOSED METHODOLOGY

A. Triple DES

Encryption : Triple DES (3DES) is a symmetric-key block cipher, enhancing the security of DES by applying it three times to data blocks. Three 56-bit keys (K1, K2, K3) are generated, and the plaintext undergoes an initial permutation (IP) before sequential encryption with these keys. The process involves encrypting with K1, decrypting with K2, and re-encrypting with K3. This triple-layer encryption fortifies security against certain attacks. The encrypted data undergoes a final permutation (FP) to yield the ciphertext. 3DES is widely employed for heightened security, offering backward compatibility with DES.

Algorithm:

```
def triple_des_encrypt(filebytes, key):

cipher = DES3.new(key, DES3.MODE_ECB)

ciphertext = cipher.encrypt(filebytes)
 return ciphertext
```

Decryption : Triple DES decryption involves reversing the encryption process by applying the inverse operations in three stages. First, the ciphertext undergoes a Final Permutation (FP) to counter the Initial Permutation (IP) performed during encryption. Subsequently, the ciphertext is decrypted using the third key (K3), followed by encryption with the second key (K2) to revert the double encryption applied during encryption. Finally, the result is decrypted with the first key (K1). The use of three keys and the reversal of encryption operations enhance security, providing backward compatibility with the original DES while offering significantly improved resistance against various cryptographic attacks.

Algorithm:

```
def triple_des_decrypt(filebytes, key):

cipher = DES3.new(key, DES3.MODE_ECB)

filebytes = cipher.decrypt(cipher)

return filebytes
```

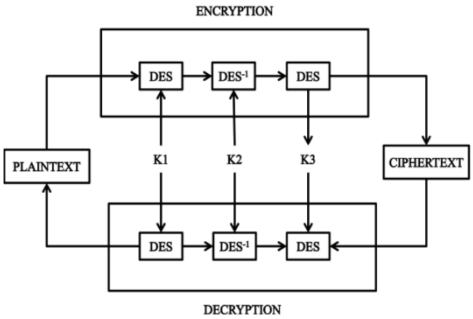

Fig. 2. Architecture diagram of Triple DES.

This Architecture Diagram of Triple DEs illustrates the encryption and decryption process, which uses the DES algorithm three times to increase security. The plaintext is initially encrypted using DES using key K1, then decrypted using key K2 and then encrypted again using key K3 to produce the ciphertext during the encryption phase. The ciphertext goes through the following reverse procedure during decryption: in order to recover the original plaintext, it is first encrypted using DES using key K2, then decrypted with DES using key K1. The original DES algorithm's security is greatly increased by this triple-layered method.

B. AES

Encryption:The Advanced Encryption Standard (AES) is a widely adopted symmetric encryption algorithm designed to secure sensitive data. It operates on fixed-size blocks of data and supports key lengths of 128, 192, or 256 bits. AES employs a substitution-permutation network (SPN) structure, involving key expansion, substitution (using a substitution box), permutation, and multiple rounds of mixing operations. The number of rounds depends on the key size (10 rounds for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys). AES is known for its efficiency, security, and versatility, making it the encryption standard for various applications, including secure communications and data protection.

Algorithm:

```
def aes_encrypt(plain_text, key):

padder = padding.PKCS7(algorithms.AES.block_size).padder()

padded_data = padder.update(plain_text) + padder.finalize()

# Create an AES cipher object

cipher = Cipher(algorithms.AES(key), modes.ECB(), backend=default_backend())

# Encrypt the data

encryptor = cipher.encryptor()

 cipher_text = encryptor.update(padded_data) + encryptor.finalize()

return cipher_tex
```

Decryption:AES(Advanced Encryption Standard) decryption involves the reverse process of encryption. The ciphered text, obtained after encryption, undergoes an inverse series of transformations in multiple rounds. These rounds consist of operations like SubBytes (substitution of bytes using a predefined S-box), ShiftRows (shifting rows of the state matrix), MixColumns (mixing columns within the matrix), and AddRoundKey (XORing the state matrix with a round key derived from the original key). The process iterates for a specified number of rounds determined by the key size. Ultimately, the decrypted text is obtained by reversing the

initial KeyExpansion process and applying the inverse Initial Round operation.

Algorithm:

```
def aes_decrypt(cipher_text, key):

    # Create an AES cipher object

    cipher = Cipher(algorithms.AES(key), modes.ECB(), backend=default_backend())

    # Decrypt the data

    decryptor = cipher.decryptor()

    padded_data = decryptor.update(cipher_text) + decryptor.finalize()

    # Unpad the decrypted data

    unpadder = padding.PKCS7(algorithms.AES.block_size).unpadder()

    plain_text = unpadder.update(padded_data) + unpadder.finalize()

    return plain_text
```

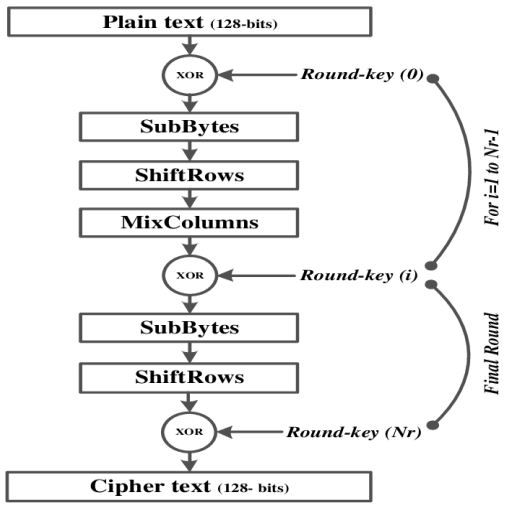

Fig. 3. Architecture of AES

The architecture diagram demonstrates how 128-bit plaintext is transformed into 128-bit ciphertext using the Advanced Encryption Standard (AES) encryption method. First, an XOR operation is performed on plaintext using the first-round key (Round-key 0). It then goes through a sequence of rounds (from i = 1 to Nr-1) with four operations in each round: SubBytes (using an S-box to substitute bytes), ShiftRows (permuting by row), MixColumns (mixing by column to produce diffusion), and an XOR with a round-specific key (Round-key i). There is no MixColumns step in the last round. The decrypted data is processed in reverse, using each round's inverse operations on the ciphertext as a starting point. By use of these organized modifications, the AES algorithm guarantees effective and safe data encryption.

IV. RESULTS

The most secure method for protecting private data is through the encryption and decryption of audio, video, and image data. A ciphered version of the data is created in those processes by transforming it using cryptographic techniques. Unable to decrypt with the same algorithm and key after encryption, the original content cannot be accessed. This system secures against unwanted access by guaranteeing the privacy of image content, voice recordings, and video footage. Assuring that only authorized parties can access the content, encryption protects the integrity of the data during transmission or storage. On the other hand, decryption returns the data to its original state. Finding the right balance between encryption and decryption is essential to protecting sensitive information's confidentiality and integrity and preserving data security without restricting authorized access.

The protection of both audio and visual data is equally important in multimedia material, where voice and video encryption expands on these ideas. Conversations are encrypted with voice technology such that they are only decryptable and understandable after they have been encrypted. Keeping private discussions secret requires this for secure communications. Visual media is also protected by video encryption, which makes it unreadable and requires the right decryption in order to see. This is crucial in domains where it's necessary to protect sensitive visual and audio data, such as telemedicine, remote conferencing, and secure video communications. Due to their ability to risk security and computing performance, the encryption algorithms and key management techniques used are critical to the effectiveness of securing audio, video, and image data. In the digital age, securing sensitive information fundamentally involves encrypting and decrypting audio, video, and image data. Organizations may guarantee the confidentiality, integrity, and security of multimedia content by utilizing powerful encryption algorithms and effective key management procedures. Maintaining privacy and safeguarding sensitive information across a range of applications and sectors requires a comprehensive approach to data security.

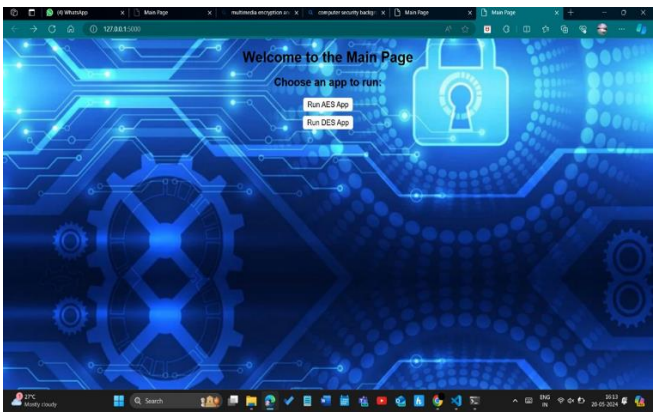

Fig. 4. The user interface components and basic functionalities to Implement AES or DES encryption and decryption applications.

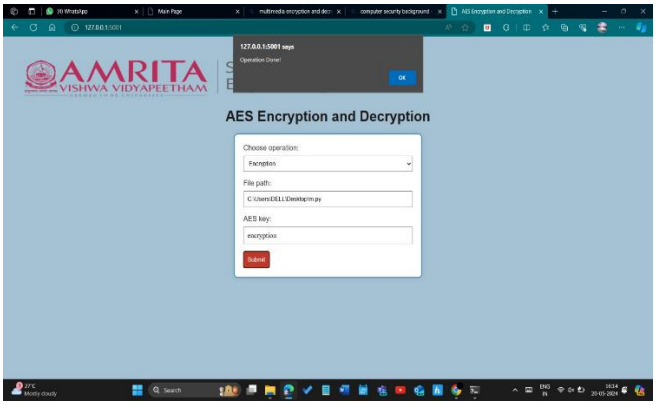

Fig. 5. The user interface components and basic functionalities to Implement AES encryption and decryption applications.

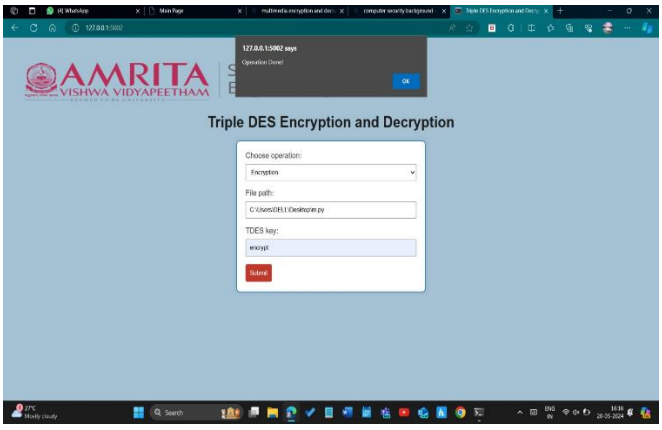

Fig. 6. The user interface components and basic functionalities to Implement DES encryption and decryption applications.

V. CONCLUSION

Implementing AES or Triple DES for voice, video, and image encryption and decryption offers strong protection against unwanted access. The security and integrity of sensitive data are guaranteed by these symmetric-key block ciphers, which provide efficient encryption techniques. Images, audio files, and video footage are protected from possible attacks by the complex key management and encryption procedures, which help to create a secure environment. AES is typically advised due to its better strength and efficiency in modern cryptographic applications, while Triple DES should be chosen based on specific security requirements. Triple DES is vulnerable to several cryptographic attacks since it uses a fixed key length of 168 bits, essentially using just 112 bits, even though it is still secure. AES is more ideal for protecting a variety of multimedia content since it has a faster encryption/decryption time and is optimized for modern technology and resource-constrained applications.

VI. REFERENCES

[1] Yasser, I., Mohamed, M.A., Samra, A.S. and Khalifa, F., 2020. A chaotic-based encryption/decryption framework for secure multimedia communications. Entropy, 22(11), p.1253.

[2] Hosny, K.M., Zaki, M.A., Lashin, N.A., Fouda, M.M. and Hamza, H.M., 2023. Multimedia security using encryption: A survey. IEEE Access.

[3] Al-Hazaimeh, O.M., Abu-Ein, A.A., Al-Nawashi, M.M. and Gharaibeh, N.Y., 2022. Chaotic based multimedia encryption: a survey for network and internet security. Bulletin of Electrical Engineering and Informatics, 11(4), pp.2151-2159.

[4] Kalabhavan, P.K. and Bodheswaran, B., 2021. A Novel Approach for Encryption and Decryption by RSA Algorithm in Secure Multimedia Communication. International Journal of Research in Engineering, Science and Management, 4(6), pp.254-256.

[5] Chowdhary, C.L., Patel, P.V., Kathrotia, K.J., Attique, M., Perumal, K. and Ijaz, M.F., 2020. Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), p.5162.

[6] Gafsi, M., Abbassi, N., Hajjaji, M.A., Malek, J. and Mtibaa, A., 2020. Improved chaos-based cryptosystem for medical image encryption and decryption. Scientific Programming, 2020, pp.1-22

[7] Dua, M., Makhija, D., Manasa, P.Y.L. and Mishra, P., 2022. 3D chaotic map-cosine transformation-based approach to video encryption and decryption. Open Computer Science, 12(1), pp.37-56.

[8] Manohar, N. and Kumar, P.V., 2020, May. Data encryption & decryption using steganography. In 2020 4th international conference on intelligent computing and control systems (ICICCS) (pp. 697-702). IEEE.

[9] Dinkar, A. and Sahana, B., 2021. AES-based android video encryption and decryption app. In Proceeding of Fifth International Conference on Microelectronics, Computing and Communication Systems: MCCS 2020 (pp. 327-339). Springer Singapore.

[10] Cheng, S., Wang, L., Ao, N. and Han, Q., 2020. A selective video encryption scheme based on coding characteristics. Symmetry, 12(3), p.332.

[11]Vinodhini, R.E., Vimalkumar, K., Malathi, P. and Gireeshkumar, T., 2018. A Highly Secured Image Steganography using Bernoulli's Chaotic Map and Binary Hamming Code. International Journal of Pure and Applied Mathematics, 118(7), pp.159-164.

[12] Jnana Ramakrishna, C., Bharath Kalyan Reddy, D., Amritha, P.P., Lakshmy, K.V. and Sachnev, V., 2024. A secure authenticated image encryption scheme based on elliptic curve cryptography. International Journal of Computers and Applications, 46(3), pp.184-193.

[13] Sravani, S. and Raniith, R., 2021, July. Image steganography for confidential data communication. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 01-05). IEEE.

[14] Vinod, M., Pallavi, M., Ajith, S. and Sriram, P., 2020. Reversible data hiding in encrypted video using reversible image transformation. Journal of Computational and Theoretical Nanoscience, 17(1), pp.136-140.

[15] Sajitha, A.S. and Priya, S.S.S., 2023. Analysis of Various Visual Cryptographic Techniques and Their Issues Based on Optimization Algorithms. International Journal of Image and Graphics, 23(06), p.2350059.