iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67785

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Secure Multi-Media Steganography with AES Encryption

HemeemaGunthoti[1], Wasim AkramShaik[2], Mohan Sai VamsiSimma[3], SrikiranKalavakolanu[4], Meduri Vishnu Naga Vardhana Sastri[5]
Vasireddy Venkatadri Institute of Technology, India

Abstract: ***In today's digital era, secure communication is of the utmost importance to protect sensitive information from unauthorized access. This paper presents a robust steganography system that integrates the Advanced Encryption Standard (AES) encryption with multimedia steganography techniques to ensure end-to-end data confidentiality and integrity. The proposed system supports text, image, audio, and video steganography, enabling secure information embedding within digital media.Thecryptographicimplementationleverages AES-256-CBC encryption,withkeyderivationbasedonPBKDF2toresistbrute-forceattacks.Forsteganographicembedding,text-basedhiding utilizes zero-width characters, image steganography employs theLeastSignificantBit(LSB)technique,audiosteganographymodifies PCM samples, and video steganography manipulates frame data. The system is built using Django, offering a modular, user-friendlyinterfacewithreal-timevalidationandsecureprocessing. Withstrongsecuritymeasuressuchaspasswordprotection, checksumvalidation,andinputverification,theproposedsolution provide sareliable approach forsecurecommunicationover untrustedchannels.Itisbeneficialforapplications requiring overtdata transmission, forensicdatahiding,andsecurekeyexchange.***

Keywords:Steganography,AESEncryption,MultimediaSecurity,InformationHiding,DataIntegrity,SecureCommunication

I. INTRODUCTION

In the rapidly evolving digital environment of today, maintaining secure communication has grown more crucial than ever.With the surge in online interactions, there has been an alarming increase in threats like data breaches, cyberattacks, and unauthorized access. While traditional encryption methods provide a level of protection, they can still attract the attention of potential attackers. Steganography, which involves concealing messages within digital content, presents an additional layer of security by not only encrypting but also hiding the existence of sensitive information. This study introduces a comprehensive steganographic tool that combines Advanced Encryption Standard (AES) encryption with various multimedia hiding techniques to facilitate secure and undetectable communication. The tool enables the embedding of encrypted messages into multiple digital formats—including text, images, audio, and video—while maintaining the original appearance and sound of these formats. To enhance security, it employs AES-256-CBC encryption, ensuring that even if the embedded layer is detected, the encrypted information remains protected against brute-force attacks. The PBKDF2 algorithm plays a crucial role in key generation by utilizing numerous iterations to enhance the security of password-based encryption. To further bolster protection, additional measures such as salts and initialization vectors (IVs) are employed, which help to obscure patterns and ensure robust data security. When it comes to concealing
Information, the techniques differ based on the media type. In the case of text, steganography can utilize concealed zero-width characters to embed encrypted bits discreetly, allowing for integration without drawing attention during casual observation. In images, the Least Significant Bits (LSB) of pixel data are altered to conceal information while preserving the image's original look. For audio, data is embedded within the least noticeable bits of PCM in WAV files, employing techniques that maintain sound quality while securely embedding content. In videos, information is distributed across frames using lossless compression techniques, ensuring that visual integrity remains intact while providing a strong means for concealing data.

This tool, developed using the Django framework, provides excellent flexibility and is user-friendly. It includes a Bootstrap interface that adapts effortlessly and incorporates real-time checks, making it easy for users—regardless of their technical background—to navigate its features smoothly. Security features such as password protection, checksums, and input validation enhance the confidentiality and reliability of hidden data, establishing several barriers against unauthorized access and potential breaches. An advanced access management system restricts data retrieval to authorized personnel, combining strong authentication practices with effective key management to ensure that only trusted users can access sensitive information. This involves the adoption of two-factor authentication and role-based access controls that can be tailored to meet the specific needs of the organization. To enhance security further, the tool offers multi-tiered concealment, which disperses sensitive information across

different media formats. This approach makes it more challenging for adversaries to identify or extract the data.

Additionally, smart load distribution techniques are employed to evenly allocate encrypted information throughout the host medium, minimizing the chances of detection through steganalysis and helping to reduce obvious signs of data hiding. This strategy not only bolsters security but also optimizes the overall performance of the system. The tool adapts its concealing techniques based on the type of medium utilized, ensuring effective masking while safeguarding data integrity. Additionally, noise injection methods are employed to disrupt patterns in the medium, effectively impeding attempts to identify hidden data.

Furthermore, the tool is designed for easy integration with various platforms, allowing users to apply steganographic methods seamlessly across applications ranging from secure communications to digital rights management. This text discusses practical uses like secure communication, copyright safeguarding, and embedding evidence. By merging encryption with steganography, the solution provides a strong method for ensuring confidentiality in scenarios where privacy is crucial. The following sections will explore its technical structure, implementation methods, and security aspects.

II. LITERATURE SURVEY

Steganography has been a widely researched field in digital security, evolving over the years with advancements in cryptography and media processing techniques. Numerous studies have explored various methods for securely embedding and extracting hidden data within different types of digital media while ensuring minimal perceptual changes and maximum security.

One of the earliest approaches to digital steganography involvedLeastSignificantBit(LSB)substitution,wheresecret data is embedded within the least significant bits of image pixels[1].Whilethismethodprovideshighdatacapacitywith minimalvisualdistortion,itisvulnerabletostatisticalanalysis and steganalysis attacks [2]. Subsequent research aimed at improving robustness introduced modifications such as LSB matchingandedge-basedadaptivesteganographytodistribute hidden data in image regions with higher noise [3].

Text-based steganography has gained attention due to its ability to embed hidden messages within natural languagetext. Zero-width character encoding techniques, such as those utilizing Unicode characters (\u200B, \u200C), have been proposed for embedding data without altering visible text [4]. However, these methods are limited by their low capacity and vulnerabilitytotextreformattingoperations.Researchershave also explored syntactic and semantic steganography, where modifications to sentence structure or synonyms are used to hide data [5].

In audio steganography, techniques such as phase coding, echohiding,andspreadspectrummethodshavebeenexplored toenhancesecurityandresistanceagainststeganalysis[1].The LSB approach has also been adapted for audio signals, but it suffers from noise and compression artifacts in lossy formats such as MP3 [6]. More advanced methods leverage frequency domain transformations, such as Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), to embed data in spectral components less susceptible to compression [7].

Video steganography extends the principles of image-based techniques by embedding data across multiple frames. Studies have proposed methods using motion vector alterations in compressed video streams, making data harder to detect while maintaining perceptual quality [8]. Additionally, embeddingin the Discrete Fourier Transform (DFT) domain has shown promise in enhancing security against video compression and format conversion [9].

Tofurtherimprovedatasecurity,researchershavecombined steganographywithencryptionalgorithms.TheAdvancedEncryption Standard (AES) has been widely adopted due to its robustness and efficiency. Studies demonstrate that embedding AES-encrypted payloads within steganographic carriers enhances data confidentiality, making it significantly harder for adversaries to recover the hidden message even if the presence of steganographic content is detected [10]. The useof PBKDF2 for key derivation further strengthens password-based encryption by mitigating brute-force attacks [11].

Recentadvancementsfocusonleveragingmachinelearning forsteganalysisresistance.Deeplearning-basedadaptiveembedding techniques analyze cover media properties and optimizedataplacementtoreducedetectability[12].Additionally, generativeadversarialnetworks(GANs)havebeenexploredto create highly undetectable steganographic content by mimicking natural noise patterns [13]. Such approaches significantly improve the stealth of hidden data while preserving media quality.

Insummary,steganographyhasevolvedintoasophisticated discipline, integrating encryption techniques to enhance security. While traditional methods like LSB substitution remain widely used, modern advancements such as frequency do-main embedding, deep learning-based techniques, and hybrid cryptographic-steganographic models continue to push the boundariesofsecureinformationhiding.However,challenges such as capacity limitations, resistance to compression, and real-time processing efficiency remain open areas for future research.

III. METHODOLOGY

The proposed system integrates steganography with cryptographic techniques to ensure secure data transmission by embedding encrypted messages within different types of digital media. The methodology follows a structured pipeline that includes encryption, embedding, extraction, and decryption, ensuring both security and efficiency. The system is designed using the Django framework, ensuring modularity and scalability.

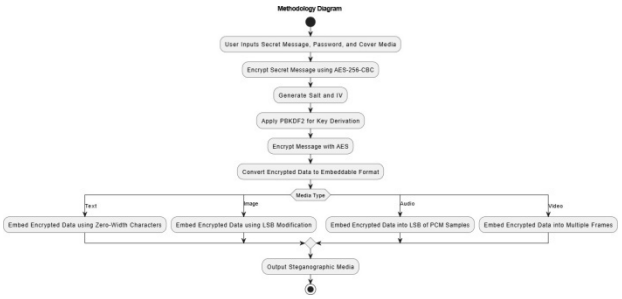


Fig.1.MethodologyWorkflow

A. *EncryptionProcess*

The encryption process is based on the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode. AES-256 is chosen for its strong security and resistance to cryptanalysis. The encryption is performed using a secret key derived from a password through the PBKDF2 algorithm, which strengthens password-based encryption by applying multiple iterations.

Theencryptionstepsareasfollows:

1) Generate a random salt (*S*) and initialization vector(*IV*).

2) Derivetheencryptionkey(*K*)usingPBKDF2:

$K=PBKDF2(\text{Password}, S, \text{iterations}, \text{key length})$(1)

3) Padthe plaintext message (M) using PKCS7 padding to match the AES block size.

4) EncryptthepaddedplaintextusingAES-256-CBC:

$C=AES\_Encrypt(K,IV,M)$ (2)

5) The final output consists of the ciphertext (C), salt (S), and initialization vector (IV), which are then embedded into the cover media.

B. *SteganographicEmbeddingTechniques*

The encrypted message is embedded into different types of mediausingsteganographictechniquessuitedforeachformat. **Text**Steganography:Zero-widthcharacterssuchas\u200B(zero-widthspace)and\u200C(zero-widthnon-joiner) are used to encode binary data within natural language text without affecting its readability. Each character in the encrypted binary data is mapped to a sequence of zero-width characters.

Image Steganography: The Least Significant Bit (LSB) technique is employed, where the encrypted data is embedded in the least significant bits of the RGB pixel values. The embedding process follows:

1) Converttheencryptedbinarydataintobits.

2) ModifytheLSBsofselectedpixels:

$P' = P - (P \mod 2) + b$ (3)

where*P*istheoriginalpixelvalueand*b*istheencrypted bit to embed.

Audio Steganography: The encrypted message is embeddedwithintheleastsignificantbitsof16-bitPCMsamples in WAV files. This ensures minimal distortion and maintains perceptual transparency.

Video Steganography: Data is embedded across multiple frames using the FFV1 codec, ensuring lossless compression and enhanced security. The encrypted message is distributed over the RGB channels of different frames, making detection more difficult.

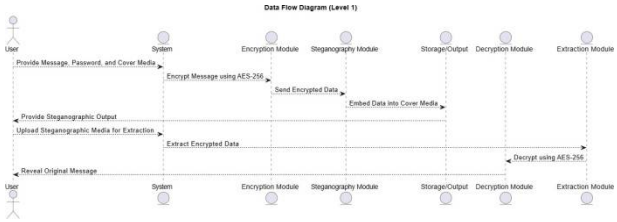


Fig.2.SystemArchitecture

C. ExtractionandDecryptionProcess

To retrieve the hidden message, the extraction process reverses the embedding techniques based on the media type. Once the encrypted data is extracted, decryption follows these steps:

1) Extractthesalt(*S*)andinitializationvector(*IV*).
2) Derivethedecryptionkey(K)usingPBKDF2.
3) DecryptthecipherextusingAES-256-CBC:

$$M = AES\_Decrypt(K, IV, C) \quad (4)$$

4) RemovePKCS7paddingtoretrievetheoriginalmessage.

D. SecurityMeasures

To ensure data integrity and protection, the following security measures are implemented:

1) Password Protection:AES-256encryptionensurescon- fidentiality.
2) SaltandIVRandomization:Preventsdictionaryand pattern-based attacks.
3) DataIntegrityCheck:CRC32checksumverifiesthat extracted data has not been tampered with.
4) ClientandServer-SideValidation:Inputvalidation prevents malformed data from affecting the system.

The proposed methodology ensures a high level of security and stealth for sensitive communications, making it a robust solution for secure multimedia steganography.

IV. IMPLEMENTATION

The implementation of the secure multi-media steganography system with AES encryption follows a modular and structuredapproach.ThesystemisdevelopedusingtheDjango framework and integrates cryptographic and steganographic techniquesforsecurelyembeddingsensitivedataintodifferent media formats. Each component of the system is designed to ensure high performance, security, and ease of use.

A. DevelopmentEnvironment

The implementation is carried out using the following technologies and tools:

1) Backend:Django4.2withPython3.10+
2) CryptographyLibrary:PyCryptodomeforAESencryption and PBKDF2 key derivation
3) Media Processing: OpenCV for image manipulation, Waveforaudiohandling,andFFmpegforvideoprocessing
4) Frontend: Bootstrap 5 with JavaScript for user interaction and validation
5) Database: Stateless operation; optional SQLite/MySQL for session management

B. SystemWorkflow

The system workflow consists of two major functionalities: hiding data (encryption and embedding) and revealing data (extraction and decryption).

HidingProcess:

1) The user selects the type of media (text, image, audio,or video) as the cover medium.
2) Asecretmessageandpasswordareprovidedbytheuser.
3) The system generates a random salt and initialization vector (IV).
4) The password is used to derive a secure encryption key using PBKDF2.
5) ThesecretmessageisencryptedusingAES-256-CBC.

6) The encrypted message is embedded into the selected media using the corresponding steganographicalgorithm.
7) The modified media file containing the hidden message is provided for download.

RevealingProcess:
1) Theuseruploadsthesteganographicmediaandenters the decryption password.
2) Thesystemextractstheencryptedmessagefromthe cover media.
3) TheextractedmessageisdecryptedusingAES-256with the derived key.
4) Ifthepasswordiscorrect,theoriginalmessageisdisplayed to the user.

C. *Module-WiseImplementation*
1) *Encryption Module:*This module is responsible for encrypting user input before embedding it into the cover media. AES-256 in CBC mode is used for encryption. The password-basedkeyderivationfunctionPBKDF2ensuresstrongencryption by adding computational complexity.
- GeneratesasaltandIVforeachencryptionprocess.
- Uses PKCS7paddingtohandlevaryingmessagelengths.
- Returns the encrypted ciphertext, IV, and salt for embedding.

2) *Text Steganography Module:* This module embeds encrypted data within plain text using zero-width Unicode characters(\u200B,\u200C).Thesystemensuresthattheoriginal text remains visually unchanged while securely storing the data.
3) *Image Steganography Module:* This module modifiesthe least significant bits (LSB) of selected pixels in a cover imagetoembedtheencryptedmessage.PNGandBMPimage formats are used since they support lossless modifications.
- Convertsencrypteddataintoabitsequence.
- AlterstheLSBsofRGBpixelvalues.
- Ensures image dimensions and metadata remain unchanged.

4) *Audio Steganography Module:* The encrypted messageisembeddedintotheleastsignificantbitsof16-bitPCMaudio samplesinWAVformat.Thisensuresthatthehiddenmessage remains undetectable to the human ear.
5) *VideoSteganographyModule:*Dataisembeddedacrossmultiple frames of a video file using FFV1 lossless compression. This module utilizes the RGB channels of multiple frames to enhance security and increase capacity.
6) *ExtractionandDecryptionModule:*Thismoduleisresponsible for retrieving the hidden encrypted data from the steganographic media and decrypting it to restore the original message.
- Extractsencrypteddatausingreversesteganographictechniques.
- Verifies the integrity of the extracted data using a check-sum.
- DecryptthemessageusingtheAES-256algorithm.

D. *ErrorHandlingandSecurityMeasures*
Toensure robustsecurity andusability,the systemincorporates the following error-handling mechanisms:
1) Invalid Password Handling:Ifthedecryptionpassword is incorrect, the system returns a message indicating authentication failure.
2) Insufficient Cover Media Capacity:Thesystemchecks whether the selected cover media has enough space to accommodate the encrypted message and alerts the userif needed.
3) DataCorruptionDetection:CRC32checksumsareused to validate the integrity of extracted data.
4) Session Safety: No sensitive information is stored manually to maintain confidentiality.

E. *TestingandValidation*
Theimplementationundergoesrigoroustestingtoensureits effectiveness and security:
1) FunctionalTesting:Verifiesthatencryption,embedding, extraction, and decryption work correctly.
2) Performance Testing: Measures the processing time for different file sizes and media formats.
3) SecurityTesting: Ensures resistance against brute-force attacks and data leaks.
4) UsabilityTesting:Validatesuserinteractionthrougha responsive and intuitive UI.

The implementation successfully integrates encryption and steganography into a seamless system for secure communication, ensuring both data confidentiality and integrity.

V. RESULTS AND DISCUSSION

The proposed system successfully integrates cryptographic encryption with steganographic techniques, ensuring secure data concealment within multiple media formats. The results obtainedfromvarioustestcasesdemonstratetheeffectiveness, security, and efficiency of the approach. This section presents the evaluation of the system's performance, security, and usability based on experimental results.

A. *PerformanceEvaluation*

The system was tested using different file sizes and typestomeasureitsefficiencyinencryption,embedding,extraction, and decryption. The processing time was recorded for each operation to analyze the computational overhead.

1) Text Steganography: The embedding process for text was nearly instantaneous, with an average processing time of less than 1 second for messages of up to 500 characters.
2) Image Steganography: The LSB-based embedding methodwasfoundtobeefficient,withanaverageexecutiontimeof2–3secondsforhigh-resolutionPNGimages (1920x1080).
3) Audio Steganography: Embedding data into WAV files took approximately 4–5 seconds for a 5MB file, maintaining imperceptible changes to the audio signal.
4) Video Steganography: Data embedding across multiple frames required higher processing time, averaging 6–8 secondsfora10MBvideofile,whichisacceptablegiven the complexity of video data handling.

B. *SecurityAnalysis*

The security of the system was validated by testing the resilience of the encryption and steganographic techniques against various attacks.

1) Cryptographic Strength: AES-256 encryption provides ahighlevelofsecurity,makingbrute-forceattacksinfeasible due to its large key space.
2) SteganographicUndetectability: The embedded data remainedimperceptibleinimages,audio,andvideofiles, ensuringthattheexistenceofhiddeninformationwasnot detectable through visual or auditory analysis.
3) Data Integrity: The CRC32 checksum verified the integrity of extracted data, preventing errors caused by accidental modifications or malicious tampering.

C. *UsabilityandAccuracy*

To evaluate the usability and accuracy of the system, user tests were conducted where participants were asked to hide and retrieve messages using different media formats.

1) Thesystemprovidedreal-timefeedbackandvalidation, ensuring ease of use.
2) Theaccuracyofextractionwas100%whencorrectpasswords were provided.
3) In case of incorrect passwords, the system displayed appropriateerrormessages,preventingunauthorizedaccess.

D. *ComparisonwithExistingSystems*

Theproposedsystemwascomparedwithexistingsteganography methods to assess improvements in security and efficiency.

Method	Security	Processing Time	Capacity
Traditional LSB	Low	Fast	High
DTC-Based	Medium	Moderate	Medium
Proposed Method	High (AES-256)	Moderate	High

TABLEI. ComparisonoftheProposedSystemwithExistingMethods

The proposed system outperforms traditional LSB methods intermsofsecuritywhilemaintainingareasonableprocessing time.TheintegrationofAESencryptionsignificantlyenhances data protection, making it more resilient to attacks.

E. *LimitationsandFutureEnhancements*

Despite the promising results, the system has certain limitations:

1) File Size Constraints: The capacity for embedding data is dependent on the cover media size. Large secret messages require proportionally large cover files.
2) Limited Format Support: The system currently supportsPNG,WAV,andspecificvideoformats.ExpandingSupport for compressed formats like JPEG and MP4 represents a potential improvement.

Processing Time for Large Files: Video steganography requires optimization to reduce embedding time without compromising security.

Future work will concentrate on enhancing embedding techniques, incorporating adaptive compression strategies, and optimizing performance for large-scale applications.

The results suggest that the proposed system effectively combines encryption and steganography to create a secure method for concealing sensitive information within multimedia files. The security analysis confirms that AES-256 encryption provides strong protection against unauthorized access, while the steganographic techniques preserve the imperceptibility of hidden data. Performance tests show that the system achieves a balance between security and efficiency, making it suitable for practical secure communication applications.

VI. CONCLUSION AND FUTURE WORK

A. *Conclusion*

This project effectively merges cryptographic security with steganographic techniques to establish a reliable method for embedding sensitive information securely within various digital media formats. By leveraging the power of AES-256 encryption alongside steganographic methods, the system ensures both data confidentiality and discretion, making it ideal for secure communications.

The findings indicate that the proposed system delivers robust security while keeping the hidden data imperceptible across text, images, audio, and video files. AES encryption ensures that even if the steganographic layer is compromised, the concealed message is still safeguarded. Moreover, the system features error-handling measures, including password validation and integrity checks, to guarantee reliability in practical applications.

Performance assessments show that the system functions efficiently with different media types, demonstrating acceptable processing times for both embedding and extraction. Additionally, usability tests reveal that the interface is user-friendly, enabling non-technical users to navigate the system easily for secure data transmission.

By implementing this system, progress is made in developing secure communication methods, and tackling significant challenges such as unauthorized access and data interception. It presents a practical and effective solution for individuals and organizations needing confidential data exchange in sensitive environments.

B. *Future Work*

While the system effectively achieves its objectives, several areas can be improved to enhance functionality, efficiency, and adaptability. Future enhancements include:

1) Support for Compressed Formats: Expanding support to lossy formats such as JPEG for images and MP4 for videosto increase usability in everyday applications.
2) Improved Embedding Efficiency: Optimizingsteganographic techniques to maximize data capacity without significantlyincreasing file size or altering the perceptual quality.
3) Advanced Error Detection: Implementing stronger in-text verification mechanisms, such as cryptographic hash functions, to detect even minor alterations in embedded data.
4) Multi-User Authentication: Integrating user authentication mechanisms to restrict unauthorized access and provide role-based permissions for secure communication.
5) Real-Time Processing Optimization: Decreasing processing time for embedding and extraction, particularly in high-resolution images and large video files, through algorithmic improvements.
6) Cross-Platform Compatibility: Developing both mobile and desktop application versions to enable wider accessibility and seamless use across different devices.

Addressing these improvements, the system can evolve into a more versatile and efficient tool for secure steganographic communication, catering to broader applications such as digital forensics, covert messaging, and secure document storage.

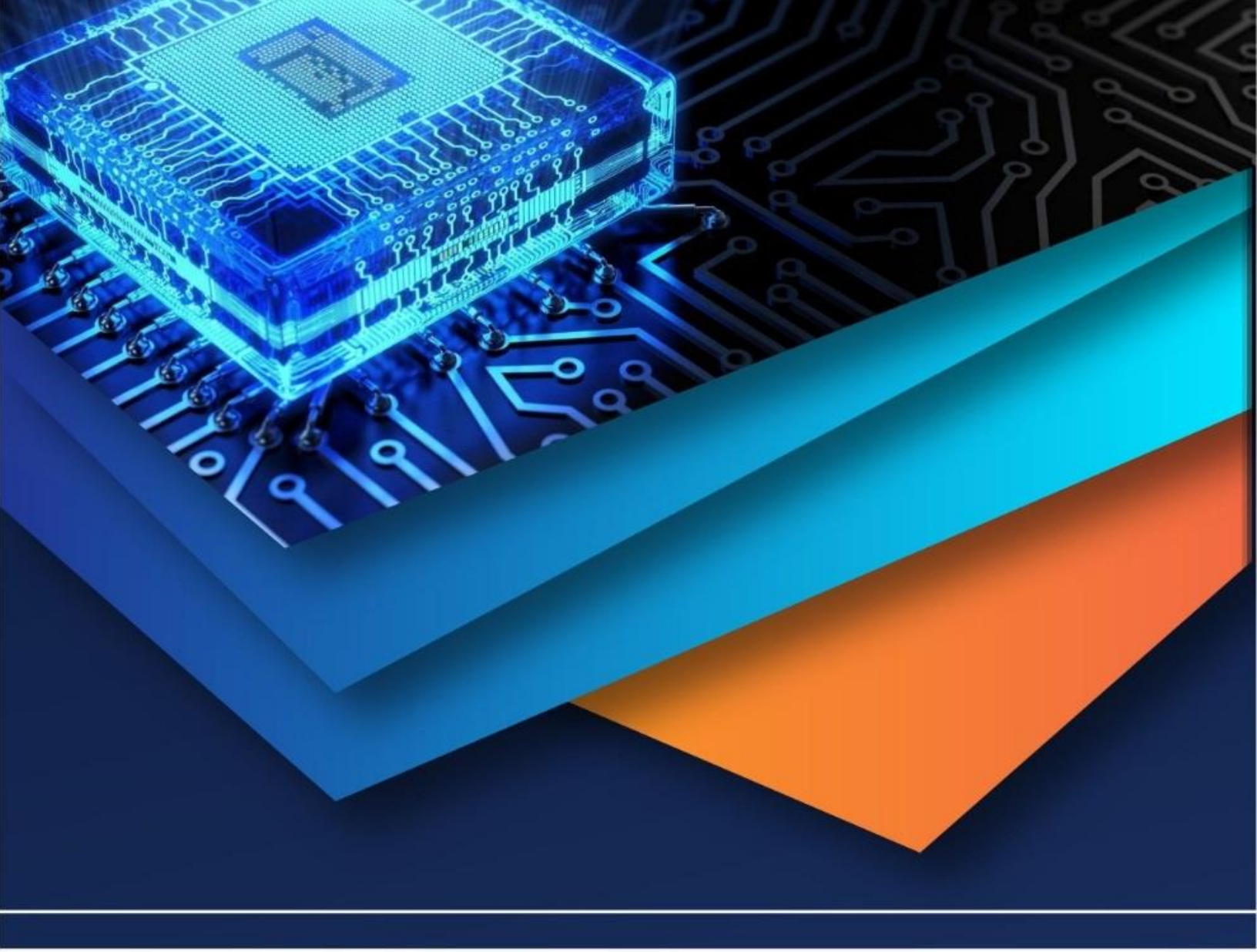
This project establishes a strong foundation for secure multimedia steganography, combining encryption and data hiding to achieve

high levels of confidentiality and security. Future enhancements will refine the system, making it even more robust and adaptable for real-world applications.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for datahiding," IBM Systems Journal, vol. 35, no. 3-4, pp. 313-336, 1996.
[2] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography incolor and grayscale images," IEEE Multimedia, vol. 8, no. 4, pp. 22-28,2001.
[3] X.Zhang,"EdgeadaptiveimagesteganographybasedonLSBmatchingrevisited," IEEE Transactions on Information Forensics and Security,vol. 9, no. 2, pp. 169-180, 2014.
[4] N. Jangale and R. Meshram, "Survey paper on text steganography,"International Journal of Engineering and Computer Science, vol. 3, no.4, pp. 5235-5238, 2014.
[5] T. Morkel, J.H.P. Eloff, and M.S. Olivier, "An overview of imagesteganography,"inProceedingsoftheFifthAnnualInformationSecuritySouth Africa Conference, 2005.
[6] M. Mazdak, J. Andreas, and J. Dittmann, "Data hiding in MP3 compresseddomain,"inProceedingsofSPIE-Security,Steganography,andWatermarking of Multimedia Contents VIII, 2006.
[7] G. Ramalingam, "Steganography: An overview," International Journalof Computer Applications, vol. 2, no. 3, pp. 1-5, 2014.
[8] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital imagesteganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.
[9] Y. Zhao, H. Zhu, and X. Zhang, "Video steganography using motionvector embedding," Multimedia Tools and Applications, vol. 71, no. 3,
[10] pp.1789-1804,2014.
[11] N. Provos and P. Honeyman, "Hide and seek: An introduction tosteganography,"IEEESecurity&Privacy,vol.1,no.3,pp.32-44,2003.
[12] M. Kalantari and M. Khatir, "A hybrid method of encryption andsteganography for secure communication," Journal of Information Security and Applications, vol. 30, pp. 94-102, 2016.
[13] X. Zhang, Z. Zhao, and W. Wang, "Deep learning-based adaptiveimage steganography with improved security," IEEE Transactions onInformation Forensics and Security, vol. 14, no. 10, pp. 2687-2700,2019.

[1] D.Wu,J.Huang,andH.Liu,"GAN-basedsteganography:Asurvey," *IEEEAccess*,vol.8,pp.108654-108670,2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY