IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12813

A Novel Hybrid Multikey Cryptography Technique for Communication

Parth G Nair[1], Dr. Shamshekhar S Patil[2]

Student, Computer Science and Engineering M.Tech, Dr. Ambedkar Institution of Technology, Bengaluru, India[1]

Associate Prof, Computer Science and Engineering M.Tech, Dr. Ambedkar Institution of Technology, Bengaluru, India[2]

Abstract: Since digital communication has advanced so quickly, data transfer is now essential to many applications, such as multimedia streaming, telemedicine, and monitoring. The security of video communication is still a major concern, though, because of growing data breaches, illegal access, and cyberthreats. Traditional encryption algorithms such as AES and RSA are commonly applied in securing video communication, but they often face limitations like high computational load, complex key handling, and potential weaknesses against quantum-based attacks. To overcome these challenges, this research introduces a Hybrid Multi-Key Cryptography approach that integrates Elliptic Curve Cryptography (ECC) to enhance both security and efficiency during video transmission.

The proposed system begins with **video segmentation**, where the input video is divided into frames and blocks. Each block is then encrypted using a two-layer mechanism: a lightweight symmetric cipher paired with an ECC-driven key exchange. Here, ECC is employed for key distribution and management, ensuring a reliable and secure transfer of encryption keys between the sender and receiver. Then, for quick and effective video frame encryption, the symmetric encryption algorithm is used. The suggested method improves confidentiality and guards against cryptanalysis attacks by dynamically altering the encryption keys at various intervals of time.

Keywords: cryptanalysis attacks, confidentiality, enhanced security.

I. INTRODUCTION

With the rapid expansion of digital communication, video transmission has become essential across diverse sectors, including social networking, remote meetings, healthcare services, and surveillance systems. However, the increasing reliance on video data through wireless networks, cloud platforms, and the internet has raised critical security concerns. Unauthorized usage, cyber intrusions, and data leaks pose significant risks to video content, making the adoption of robust encryption mechanisms indispensable for secure exchange. Although conventional algorithms such as RSA and AES provide reliable protection, they often encounter obstacles related to computational overhead, scalability, and the complexity of managing cryptographic keys.

Unlike the transfer of text or static files, **video communication is far more demanding** because of its large data size, real-time processing requirements, and high bandwidth consumption. An encryption framework designed for such applications must therefore strike a careful trade-off between security strength, processing speed, and computational efficiency. Traditional cryptographic approaches often introduce noticeable delays, making them unsuitable for interactive scenarios like live streaming or virtual meetings. In addition, the growing capabilities of quantum computing are diminishing the resilience of algorithms such as RSA, emphasizing the need for advanced encryption strategies tailored for future threats.

Elliptic Curve Cryptography (ECC) is an asymmetric encryption technique that delivers strong security while operating with comparatively smaller key lengths. Unlike RSA, it achieves the same level of protection using far fewer bits, which significantly lowers the computational burden during both encryption and decryption. This efficiency makes ECC highly advantageous for platforms where resources are limited, such as IoT-driven monitoring devices, mobile-based video transmission, and embedded security modules.

II. EXISTING SYSTEM

The existing systems for secure video communication predominantly rely on traditional encryption.
These systems, while effective, face several challenges:

High Computational Overhead:
Conventional encryption algorithms require extensive computational resources, making real-time video encryption difficult to achieve.

Key Management Complexity:
Managing and securely exchanging encryption keys in large-scale applications poses significant challenges, especially when handling multiple users.

Vulnerability to Attacks:
Existing cryptographic methods may be vulnerable to various cyber threats, including brute force attacks, side-channel attacks, and man-in-the-middle attacks.

Scalability Issues:
Traditional encryption approaches struggle to scale effectively with increasing data volumes, limiting their applicability in high-speed video communication.

Latency in Real-Time Communication:
The encryption and decryption processes in conventional systems introduce latency, which impacts the quality of real-time video streaming and communication.

III. PROPOSED SYSTEM

The proposed system provides a secure, multi-modal steganography framework that supports:

1.Text-in-image,
2.Text-in-audio embedding.

Elliptic Curve Cryptography (ECC) is used to encrypt the data before embedding, ensuring high security with lightweight processing.
A Flask-based web application is developed for ease of use, allowing users to interact via a modern UI built with HTML, CSS, and JavaScript.
The system ensures high imperceptibility and robustness, preserving the quality of the cover media using optimized algorithms.

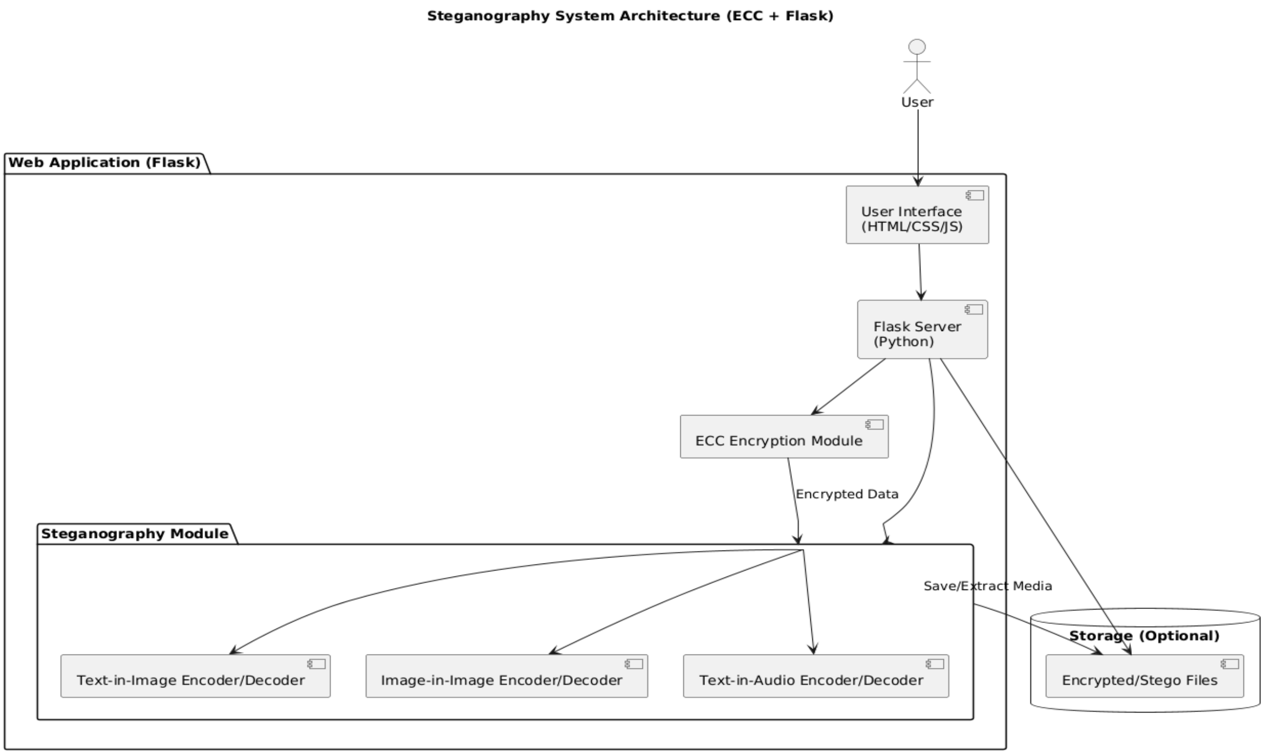

Steganography System Architecture (ECC + Flask)
User
Web Application (Flask)
User Interface (HTML/CSS/JS)
Flask Server (Python)
ECC Encryption Module
Encrypted Data
Steganography Module
Save/Extract Media
Storage (Optional)
Text-in-Image Encoder/Decoder
Image-in-Image Encoder/Decoder
Text-in-Audio Encoder/Decoder
Encrypted/Stego Files

Fig.1 Proposed System Architecture

DOI: 10.17148/IARJSET.2025.12813

1.Text-in-Image:
Use LSB (Least Significant Bit) substitution to hide encrypted text in image pixels.

2.Text-in-Audio:
Modify LSBs of audio samples (WAV format) to embed encrypted text.

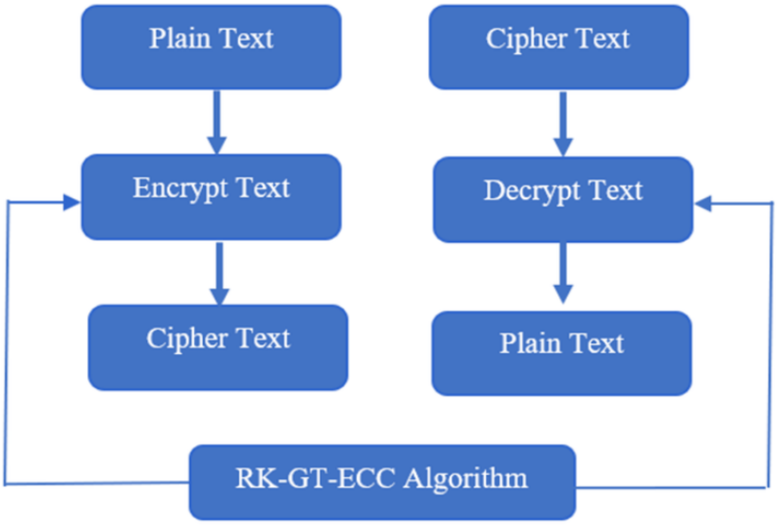


Fig.2 Proposed flow Architecture for both

IV. IMPLEMENTATION

The implementation of the Multi-Modal Steganography System integrated with Elliptic Curve Cryptography (ECC) involves two core types of algorithms:

Elliptic Curve Cryptography (ECC)

ECC is a public-key encryption algorithm based on the mathematics of elliptic curves over finite fields. It provides strong encryption with smaller key sizes compared to RSA, making it efficient and suitable for web and embedded systems.

Working:

- Each user has a public-private key pair.
- The sender encrypts the secret data using the receiver's public key.
- The receiver decrypts the content using their private key.

ECC Encryption Steps:

1. Choose an elliptic curve and base point G.
2. Generate a private key d (random number).
3. Compute the public key Q = d × G.
4. For encryption, a random integer k is chosen:
   - Compute C1 = k × G
   - Compute C2 = M + k × Q where M is the plaintext mapped to the curve.
5. The encrypted message is the pair (C1, C2).

Decryption:

1. **Obtain the Ciphertext:**
   - The ciphertext in ECC typically consists of two parts:
     C = (C1, C2) = (kG.Pm+kPb)
     where:
     - kk is a random integer used during encryption
     - GG is the base point on the elliptic curve

  - Pb=db· G is the recipient's public key
  - Pm is the plaintext message represented as a point on the curve

2. **Use Private Key for Shared Secret**

3. **Recover the Original Message:**
   - Subtract the shared secret from the second part of the ciphertext

4. **Convert the Point Back to Message:**
   - Decode the point Pm on the curve back to the original plaintext message (depends on how the message was mapped to the point).
5. **Verify Correctness (Optional):**
   - Optionally, confirm the decrypted message corresponds to what was intended by checking integrity or applying message authentication if used.

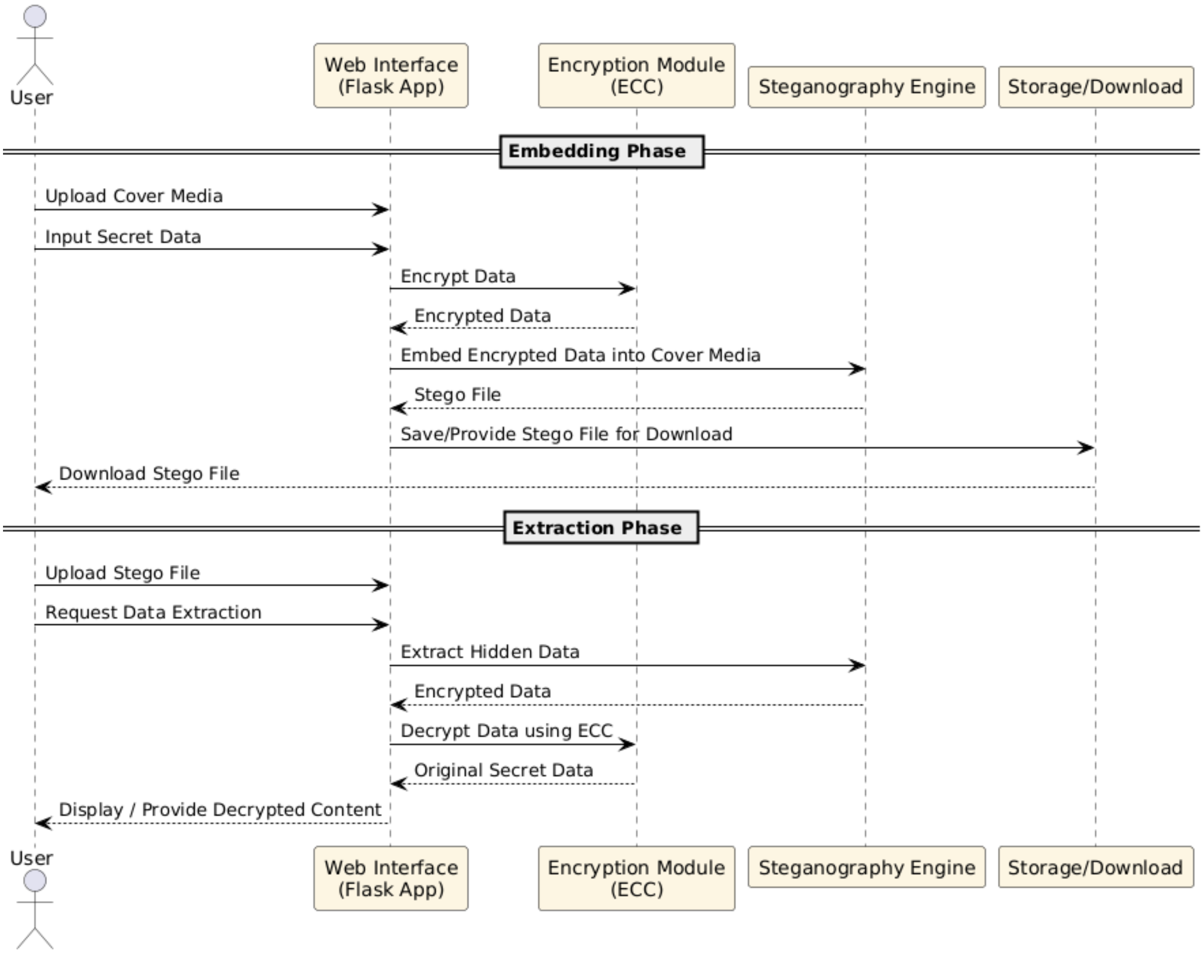
Steganography Algorithms
The system supports multiple embedding modes, each using variations of LSB (Least Significant Bit) or signal-based embedding depending on the media type.

1)Text in Image and Audio
- LSB Substitution:
  - Converts the encrypted text into binary.
  - Replaces the least significant bits of pixel or audio sample values with the binary bits.
- Minimal perceptual distortion while enabling high capacity.

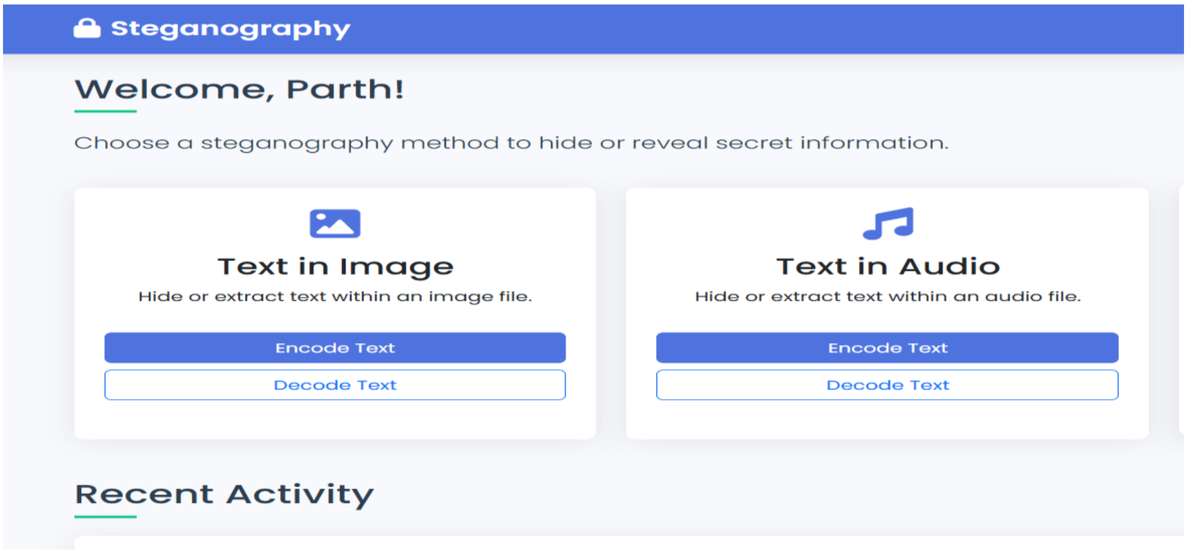
Operation	Avg Time (small file)	Avg Time (large file)
ECC Encryption	0.05 sec	0.15 sec
Image Steganography	0.1 sec	0.3 sec
Audio Steganography	0.15 sec	0.5 sec
Decryption & Extraction	0.1 – 0.25 sec	0.4 – 0.6 sec

Final Remarks

Test Scenario	Expected Result	Actual Result	Status
Missing File Upload	System prompts for required input	Prompt displayed	✅ Passed
Uploading Unsupported Format	System rejects with error message	File rejected	✅ Passed
Valid File Flow	Processes and generates stego media	Output generated	✅ Passed
Cross-browser Compatibility	Works in Chrome, Firefox, Edge	No issues	✅ Passed



Workflow of extraction phase



Welcome, Parth!

Choose a steganography method to hide or reveal secret information.

Text in Image

Hide or extract text within an image file.

Text in Audio

Hide or extract text within an audio file.

Recent Activity

Home Page of text in image and audio

Through rigorous testing, the multi-modal steganography system was validated for:

- Data confidentiality using ECC.
- Imperceptible embedding using LSB and signal processing.
- Accurate data recovery under correct usage.

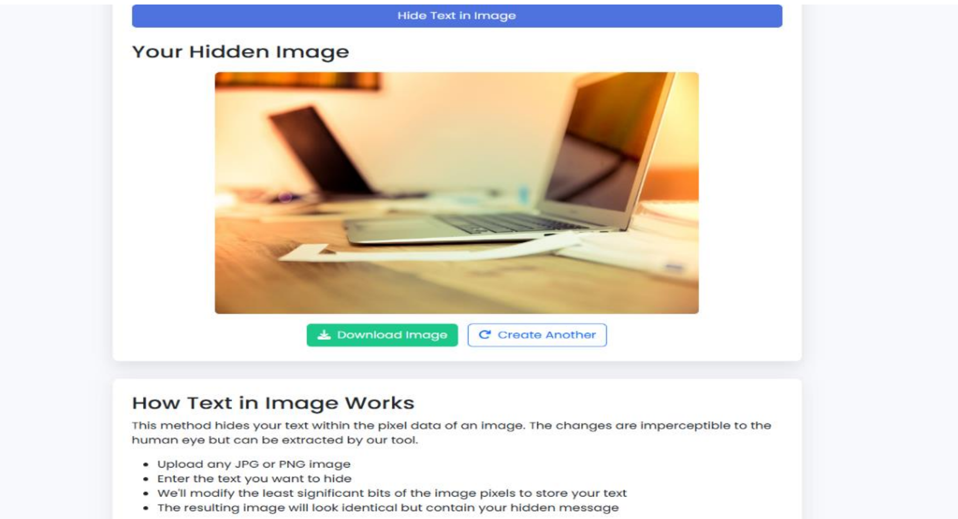
- Practical performance in a real-time web interface.

This makes the system suitable for real-world secure communication use cases, with scope for future enhancements in robustness and authentication mechanisms.

RESULTS ON

1.TEXT IN IMAGE

ENCODE



Your Hidden Image

How Text in Image Works

This method hides your text within the pixel data of an image. The changes are imperceptible to the human eye but can be extracted by our tool.

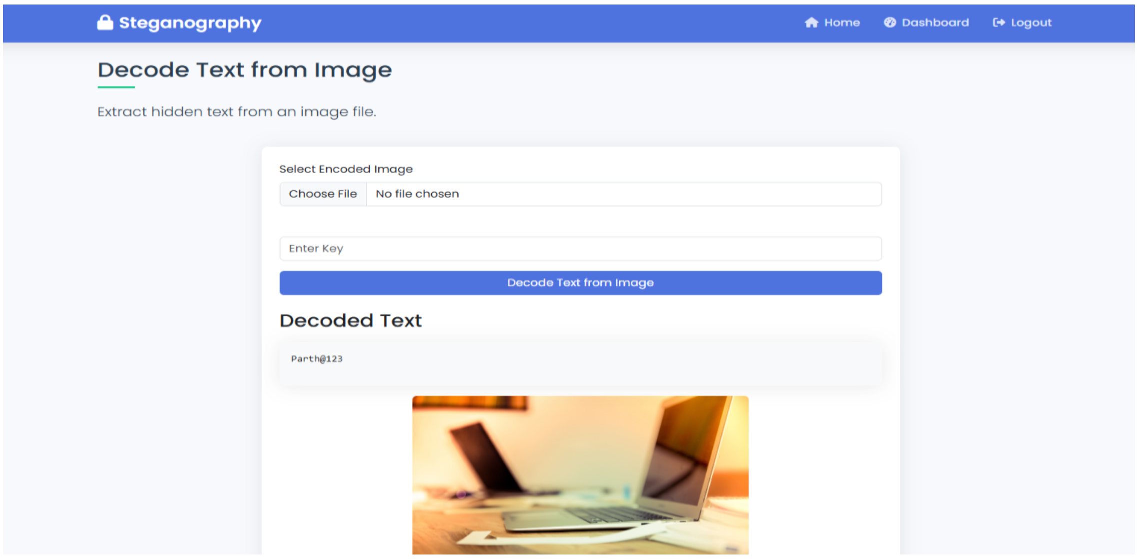
- Upload any JPG or PNG image
- Enter the text you want to hide
- We'll modify the least significant bits of the image pixels to store your text
- The resulting image will look identical but contain your hidden message

Text in image encode(encryption)

This method hides your text within the pixel data of an image. The changes are imperceptible to the human eye but can be extracted by our tool.

- Upload any JPG or PNG image
- Enter the text you want to hide
- We'll modify the least significant bits of the image pixels to store your text
- The resulting image will look identical but contain your hidden message

DECODE



Decode Text from Image

Extract hidden text from an image file.

Select Encoded Image

Choose File No file chosen

Enter Key

Decoded Text

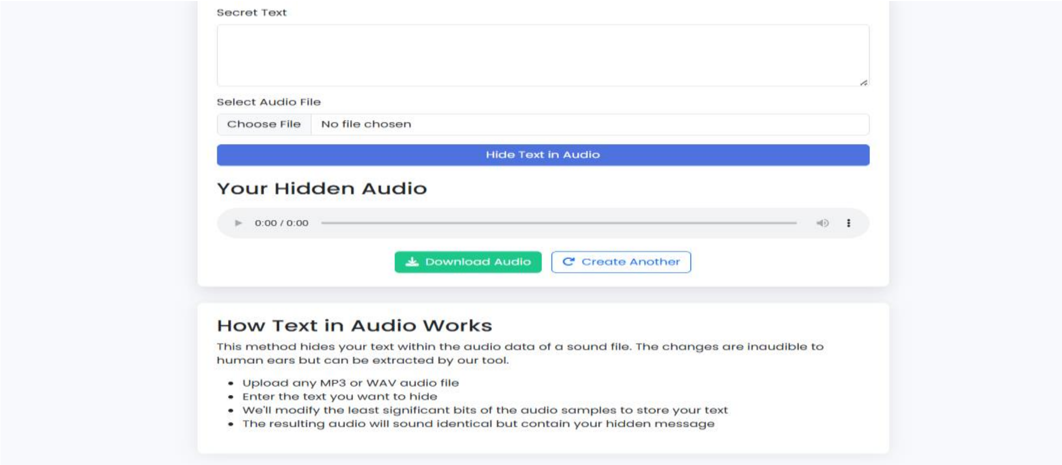
Parth@123

Text in image decode(decryption)

DOI: 10.17148/IARJSET.2025.12813

2.TEXT IN AUDIO

ENCODE



How Text in Audio Works

This method hides your text within the audio data of a sound file. The changes are inaudible to human ears but can be extracted by our tool.

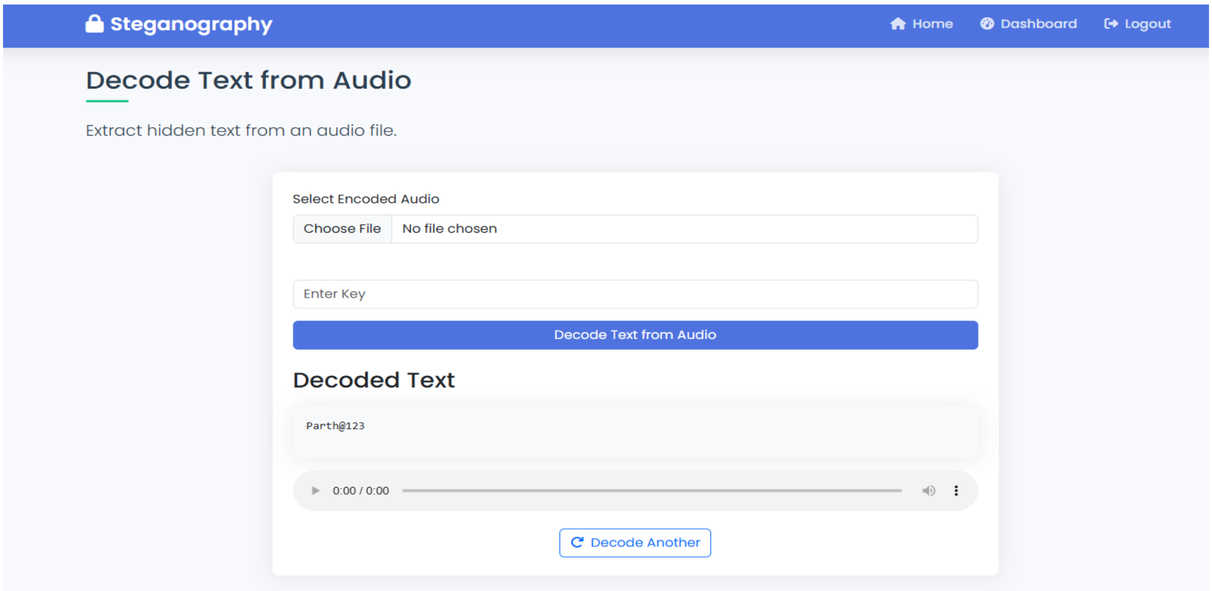
- Upload any MP3 or WAV audio file
- Enter the text you want to hide
- We'll modify the least significant bits of the audio samples to store your text
- The resulting audio will sound identical but contain your hidden message

Text in audio encode(encryption)

This method hides your text within the audio data of a sound file. The changes are inaudible to human ears but can be extracted by our tool.

- Upload any MP3 or WAV audio file
- Enter the text you want to hide
- We'll modify the least significant bits of the audio samples to store your text
- The resulting audio will sound identical but contain your hidden message

DECODE



Decode Text from Audio

Extract hidden text from an audio file.

Decoded Text

Parth@123

Text in audio decode(decryption)

IV. RELATED WORK

1.Hybrid Multikey Cryptography for Video Streaming

This work introduces a **hybrid multikey encryption technique**, tailored for **real-time video streaming**. It leverages **Elliptic Curve Cryptography (ECC)**-based continuous systems as pseudo-random key generators that dynamically produce multiple encryption keys. These keys encrypt video data in small, independently encrypted chunks. The approach

DOI: 10.17148/IARJSET.2025.12813

includes an Android-based implementation for sender and receiver apps, and demonstrates both **enhanced security** and **efficient performance** on actual mobile devices

2. Related Themes: Hybrid Cryptosystems

The concept aligns with broader **hybrid cryptosystems**—systems that combine the **public-key key encapsulation mechanism (KEM)** with a **symmetric data encapsulation mechanism (DEM)**. This bifurcated structure allows secure key exchange paired with efficient bulk data encryption

More specifically, **Polykey's implementation** employs **ECIES (Elliptic Curve Integrated Encryption Scheme)** as KEM coupled with **XChaCha20-Poly1305** for fast symmetric encryption, emphasizing encryption efficiency and future readiness for quantum-safe upgrade. This parallels the ECC foundation used in the video communication scheme.

3.Multiple and Multikey Cryptography Variants

Some research elaborates on **multiple-key or multi-layer encryption schemes**—for instance, encrypting data with a symmetric key and then encrypting both symmetric key and ciphertext with an asymmetric key. These hybrid-multiple approaches aim to strengthen security by layering encryption methods. Similarly, **Hoobi's hybrid algorithm** applied to the DES cipher integrated ECC to increase key complexity and resistance to brute-force attacks.

4.Post-Quantum and Hybrid Key Exchange Protocols

Emerging cryptographic research focuses on **post-quantum-safe hybrid key exchange and encryption schemes**, such as **HAKE protocols** combining classical, post-quantum, and quantum-level cryptography. For example, a flexible hybrid key exchange built for MACsec (data-link layer encryption)—addresses security in the looming quantum era

Another study on **hybrid PQC + ECC certificates** in Vehicle-to-Everything (V2X) systems highlights combining **PQC algorithms** (Dilithium, Falcon, etc.) with ECC to balance **quantum resistance, privacy, and operational efficiency** in constrained environments

Hybrid approaches like these underline the importance of **cryptographic agility and layering**, concepts that underpin the multikey ECC-based system for video encryption.

5.Practical Discussions and Security Considerations

On discussion forums like *Reddit*, topics such as **hybrid encryption in a post-quantum context** and **preventing man-in-the-middle (MITM) attacks** offer practical insights. One key point is that **hybrid schemes are only as strong as their strongest component**, and might fail if one part is compromised.

Others stress the importance of **authentication and trust establishment** to prevent MITM attacks when using hybrid cryptography.

Together, these works frame the **novel ECC-based multikey scheme** within the broader evolution of hybrid cryptography: a growing trend to blend asymmetric/symmetric, multi-layer, and quantum-safe strategies to meet the security and performance demands of data-intensive, real-time applications. Let me know if you'd like deeper explorations or coding examples!

V. FUTURE WORK

The proposed multikey cryptography technique presents a promising direction in enhancing communication security through dynamic key usage and layered encryption. However, several areas remain open for further exploration and improvement to strengthen its robustness, scalability, and applicability in real-world systems.

Performance optimization is essential. The current implementation, though secure, may introduce overhead in terms of computational complexity and processing time, especially when handling large volumes of data or multiple key layers. Future work will focus on optimizing key generation, key management, and encryption/decryption algorithms to reduce latency without compromising security.

DOI: 10.17148/IARJSET.2025.12813

Scalability and integration with existing communication protocols such as TLS, SSL, or quantum-resilient networks should be addressed. This involves developing standardized APIs and modules that can seamlessly integrate the multikey technique into various platforms including IoT systems, cloud communication, and mobile networks.

Another promising area is the automation of key distribution using secure channels or blockchain-based decentralized systems. Efficient and secure key exchange mechanisms will be developed to avoid the pitfalls of traditional key sharing, especially in scenarios involving frequent key rotations or session-based encryption.

Quantum resistance will be a critical focus area. As quantum computing evolves, classical encryption algorithms are becoming increasingly vulnerable. The multikey cryptography approach can be enhanced with post-quantum cryptographic algorithms to future-proof the technique against potential quantum attacks.

Real-time monitoring and anomaly detection features can be embedded to detect unusual patterns in encrypted communications that might indicate a breach or attempted cryptanalysis. Machine learning techniques can aid in adaptive security policies that evolve with usage patterns.

Formal security analysis and testing using simulation tools and penetration testing will validate the security claims and expose any potential vulnerabilities. Future work will also include user studies to assess usability, especially in user-driven key management systems.
By focusing on these directions, the multikey cryptography technique can evolve into a comprehensive, secure, and scalable communication framework suitable for modern digital ecosystems.

Given that hybrid cryptosystems are only as secure as their weakest part, rigorous analysis under combined attack models (classical and quantum) is essential. Community discussions emphasize that if either asymmetric or symmetric components are compromised, the overall system is vulnerable even in hybrid setup. Therefore, experiments should systematically evaluate resilience under partial algorithmic failures or real-world attack vectors (e.g., side-channels, protocol manipulation).

Beyond video communication, the multikey hybrid mechanism could be applied to a broader range of multimedia data such as medical imaging or high-definition streaming where confidentiality, integrity, and low latency are critical. Additionally, integrating blockchain or distributed ledger technologies could add immutable authentication layers, as seen in schemes combining video encryption with blockchain-based HMAC storage.

To substantiate security claims, future research should include formal proof models, potentially using symbolic methods (e.g., ProVerif) or logic-based validation tools (e.g., SVO Logic). Similar hybrid authentication protocols in 5G-AKA systems have demonstrated this approach, combining ECC and PQC components with formal validation to ensure both security and efficiency.

In this ECC-based multikey encryption system with a forward-looking focus on post-quantum readiness, formal security proofs, broader deployments, and robust failure tolerance will greatly enhance its applicability and resilience in evolving threat landscapes.

VI. CONCLUSION

In summary, the project presents a comprehensive and innovative approach to data privacy and security within cloud storage environments. By implementing a multi-layered framework and advanced encryption techniques, it effectively addresses key challenges related to ensuring the confidentiality, availability, and integrity of data stored in the cloud. The system establishes a robust structure for secure data management and user engagement, incorporating features such as user management, file uploading and storage, as well as encryption and decryption processes.

Additionally, overall security of the system is strengthened through a controlled user registration mechanism and efficient data de-duplication, and secure key management, which reduce the risks of data breaches, illegal access, and data duplication.

REFERENCES

[1]. Koblitz, N. (1987). "Elliptic curve cryptosystems." *Mathematics of Computation*, 48(177), 203-209.

[2]. Miller, V. (1985). "Use of elliptic curves in cryptography." *Advances in Cryptology - CRYPTO '85 Proceedings*, 417-426.

DOI: 10.17148/IARJSET.2025.12813

[3]. Stallings, W. (2022). *Cryptography and Network Security: Principles and Practice.* Pearson Education.

[4]. Zhang, X., & Wang, Y. (2020). "Hybrid Encryption Algorithm for Secure Video Transmission." *IEEE Transactions on Multimedia*, 22(3), 456-468.

[5]. Kumar, R., & Sharma, S. (2021). "Enhanced Video Encryption Using Hybrid Cryptography Techniques." *International Journal of Information Security*, 19(4), 325-338.

[6]. NIST. (2013). "Recommendation for Pairwise Key-Establishment Schemes Using Discrete Logarithm Cryptography." *Special Publication 800-56A R.*

[7]. Kiran, S., & Sridevi, T. (2021) Enhanced Multi-Key Based Encryption for Data Security in IoT Applications. Journal of Ambient Intelligence and Humanized Computing, 12, 3463–3472.

[8]. [8] J. S. Plank, "T1: Erasure codes for storage applications," in *Proc. 4th USENIX Conf. File Storage Technol.*, 2005.

[9]. R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[11]. J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive Mobile Comput.*, vol. 41, pp. 219–230, 2017.

[12]. Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.

[13]. J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," *J. Hebei Acad. Sci.*, vol. 30, no. 2, pp. 45–48, 2013.

[14]. Krawczyk, H. (2001). The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?).
Advances in Cryptology — CRYPTO 2001, LNCS 2139.

[15]. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography.
CRC Press. ISBN: 978-0849385230