International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A SECURE DUAL LAYER INFORMATION HIDING FRAME WORK UTILIZING HYBRID CRYPTOGRAPHY AND LEAST SIGINIFICANT BIT STEGANOGRAPHY

[1]IRRINKI VIJAYAKUMAR, [2] Mr. B. NANDAN KUMAR, [3] Dr B VS VARMA

(Student, Asst. prof. and HOD and Prof.)

Department of CSE M-Tech DNR COLLEGE OF ENGINEERING AND TECHNOLOGY,

(Autonomous)

Bhimavaram, Andhra Pradesh 534 202

(Affiliated to Jawaharlal Nehru Technological University Kakinada).

ABSTRACT

The rapid expansion of cloud computing, digital communication, and distributed storage systems has significantly increased the need for secure data protection during storage and transmission. Although conventional cryptographic techniques provide confidentiality, encrypted files remain identifiable and are therefore susceptible to cryptanalysis and unauthorized attacks. To overcome these limitations, this research proposes **A Secure Dual Layer Information Hiding Framework Utilizing Hybrid Cryptography and Least Significant Bit (LSB) Steganography**. The proposed framework integrates **Advanced Encryption Standard (AES)** and **Elliptic Curve Cryptography (ECC)** to establish a hybrid encryption mechanism that ensures both efficient data encryption and secure key management. AES is employed for high-speed encryption of confidential files, while ECC securely encrypts the AES secret key, reducing key distribution vulnerabilities. To provide an additional layer of security, the encrypted data is embedded into digital images using the **Least Significant Bit (LSB)** steganography technique, effectively concealing the existence of sensitive information. Furthermore, **SHA-256 hashing** is incorporated to verify data integrity and detect unauthorized modifications, while **One-Time Password (OTP)-based Multi-Factor Authentication (MFA)** ensures that only authenticated users can access encryption and decryption services. The framework is implemented as a secure web-based application using **Python, HTML, CSS, JavaScript, and MySQL**, providing functionalities including secure file upload, encryption, steganographic embedding, hidden data extraction, decryption, integrity verification, and authenticated user access. Experimental evaluation demonstrates that the proposed system successfully achieves secure data encryption, covert communication, integrity preservation, and efficient retrieval while maintaining minimal computational overhead. The integration of hybrid cryptography with LSB steganography offers a robust and scalable solution for protecting sensitive information against modern cybersecurity threats, making it suitable for secure cloud storage, confidential communication, and digital document protection.

Keywords: Hybrid Cryptography, Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Least Significant Bit (LSB), Steganography, Information Hiding, SHA-256, Multi-Factor Authentication (MFA), Cloud Security, Data Integrity, Secure Communication.

I.INTRODUCTION

The exponential growth of cloud computing, digital communication, and distributed storage systems has

transformed the way individuals and organizations store, process, and exchange confidential information. With the increasing reliance on cloud-based services, IoT devices, and online collaboration platforms, enormous volumes of sensitive data are transmitted through public communication networks every day. While these technologies improve accessibility, scalability, and operational efficiency, they also expose digital information to numerous cybersecurity threats such as unauthorized access, data interception, ransomware, insider attacks, and information leakage. Consequently, ensuring the confidentiality, integrity, and authenticity of digital information has become one of the most significant challenges in modern cybersecurity research [1], [2].

Traditional cryptographic algorithms provide strong protection by converting plaintext into ciphertext, thereby preventing unauthorized users from understanding the original information. Among symmetric encryption algorithms, the **Advanced Encryption Standard (AES)** has become the global standard due to its high encryption speed, computational efficiency, and strong resistance to cryptographic attacks. However, symmetric encryption requires secure key distribution, which remains a critical challenge in large-scale communication systems. On the other hand, asymmetric encryption algorithms such as **Elliptic Curve Cryptography (ECC)** offer secure key exchange using mathematically related public and private keys while requiring significantly smaller key sizes than conventional algorithms such as RSA. Hybrid cryptography combines the advantages of AES and ECC, enabling efficient data encryption along with secure key management, thereby overcoming the limitations of standalone encryption techniques [3], [4].

Although encryption effectively protects the content of confidential information, encrypted files themselves clearly indicate the presence of valuable data. Attackers often target encrypted files using cryptanalysis, brute-force attacks, or key theft because ciphertext naturally attracts attention. To address this limitation, **steganography** introduces an additional security layer by concealing the existence of sensitive information inside digital media such as images, audio, or video files. Among various information hiding techniques, **Least Significant Bit (LSB) steganography** is widely adopted because it offers high embedding capacity, low computational complexity, and minimal visual distortion. By embedding encrypted information within ordinary digital images, LSB steganography enables covert communication while maintaining the visual quality of the cover image, making it difficult for attackers to detect hidden information [5], [6].

Modern information security systems must also guarantee data integrity and authenticated user access in addition to confidentiality. Cryptographic hash functions such as **SHA-256** generate unique digital fingerprints that enable verification of file integrity by detecting even minor modifications to stored or transmitted data. Similarly, **Multi-Factor Authentication (MFA)** using One-Time Password (OTP) verification significantly strengthens user authentication by requiring an additional verification step beyond traditional username-password mechanisms. These security mechanisms reduce the risks associated with credential theft, phishing attacks, and unauthorized system access while improving the overall reliability of secure communication systems [7], [8].

Despite substantial advancements in cryptography and information hiding, many existing security frameworks implement only one or two protection mechanisms, leaving several vulnerabilities unresolved. Some systems provide strong encryption but lack secure key management, while others utilize steganography without adequate encryption, integrity verification, or user authentication. Such isolated approaches are insufficient against increasingly sophisticated cyber threats. Therefore, there is a growing need for an integrated framework capable of simultaneously providing secure encryption, hidden communication, integrity verification, and authenticated user access within a unified architecture [9].

To address these limitations, this research proposes **A Secure Dual Layer Information Hiding**

Framework Utilizing Hybrid Cryptography and Least Significant Bit (LSB) Steganography. The proposed framework integrates **AES**, **ECC**, **LSB Steganography**, **SHA-256 Hashing**, and **OTP-based Multi-Factor Authentication** into a comprehensive web-based security platform. AES performs high-speed encryption of confidential files, ECC securely encrypts the AES secret key, LSB steganography conceals encrypted information inside digital images, SHA-256 verifies data integrity, and OTP authentication ensures that only authorized users can access encryption and decryption services. The complete system is implemented using Python, HTML, CSS, JavaScript, and MySQL to provide secure file encryption, steganographic embedding, hidden data extraction, integrity verification, and authenticated communication. Experimental evaluation demonstrates that the proposed dual-layer framework provides enhanced confidentiality, secure key management, covert communication, and improved resistance against modern cyberattacks, making it suitable for cloud computing, secure document sharing, digital forensics, healthcare systems, and military communication environments [10].

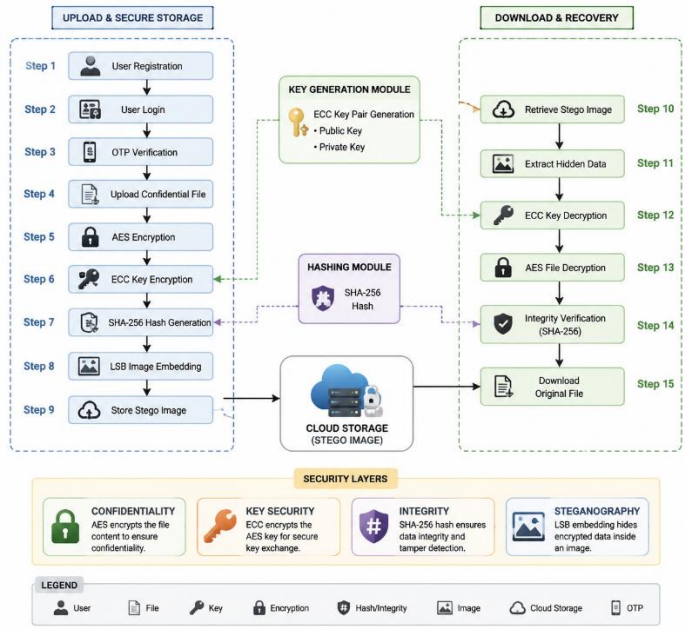


Figure1: System Architecture

The proposed system architecture is designed to provide a highly secure cloud storage framework by integrating **Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), SHA-256 hashing, and Least Significant Bit (LSB) image steganography**. The architecture is divided into two major phases: **Upload and Secure Storage** and **Download and Recovery**. Each phase incorporates multiple layers of security to ensure confidentiality, integrity, authentication, and secure data transmission. By combining cryptographic techniques with steganography, the system protects sensitive files from unauthorized access while maintaining data integrity throughout the storage and retrieval process.

The process begins with **user registration and login**, where users create an account and authenticate themselves using valid credentials. To strengthen authentication, the system performs **One-Time Password (OTP) verification**, which acts as a second layer of security. Only users who successfully complete OTP verification are allowed to access the application's secure services. This authentication mechanism minimizes the risk of unauthorized access and ensures that only legitimate users can upload or retrieve confidential files.

Once authentication is completed, the user uploads the confidential file to the system. The uploaded file is

immediately encrypted using the **Advanced Encryption Standard (AES)** algorithm. AES converts the original plaintext file into ciphertext using a secret symmetric key, making the file unreadable to unauthorized users. Since AES is highly efficient and widely accepted for securing sensitive information, it provides strong confidentiality while maintaining high encryption and decryption performance.

To further enhance security, the AES encryption key is protected using **Elliptic Curve Cryptography (ECC)**. Instead of storing or transmitting the AES key directly, the system encrypts it using the recipient's ECC public key. ECC offers strong security with relatively smaller key sizes, reducing computational overhead while providing excellent protection against key compromise. This layered encryption approach ensures that even if the encrypted file is intercepted, it cannot be decrypted without the corresponding ECC private key.

After encryption, the system generates a **SHA-256 cryptographic hash** for the encrypted data. The hash serves as a unique digital fingerprint that represents the contents of the encrypted file. Even a minor modification in the encrypted data produces a completely different hash value. This mechanism enables the system to verify data integrity during retrieval and detect any unauthorized modifications or tampering that may occur while the file is stored in the cloud.

The encrypted file, encrypted AES key, and generated SHA-256 hash are then embedded into a cover image using **Least Significant Bit (LSB) image steganography**. LSB embedding hides sensitive information inside the least significant bits of image pixels without causing noticeable visual changes. As a result, the encrypted data remains concealed within an ordinary-looking image, making it difficult for attackers to detect the existence of confidential information. The generated **stego image** is subsequently stored in cloud storage instead of storing the encrypted file directly, thereby adding another layer of protection.

During the retrieval phase, the user requests the stored data, and the system retrieves the corresponding stego image from cloud storage. The hidden encrypted file, encrypted AES key, and SHA-256 hash are extracted using the LSB extraction process. The AES key is then recovered by decrypting it with the user's ECC private key. Once the original AES key is obtained, it is used to decrypt the encrypted file and reconstruct the original confidential document.

Before allowing the user to download the recovered file, the system performs **integrity verification** by recalculating the SHA-256 hash of the decrypted data and comparing it with the original extracted hash value. If both hash values match, the system confirms that the file has not been altered during storage or transmission. After successful verification, the original file is made available for download. If any mismatch is detected, the system identifies the file as compromised and prevents access, thereby protecting users from tampered or corrupted data.

II SURVEY OF RESEARCH

The increasing dependence on cloud computing, digital communication, and distributed storage has intensified the need for advanced data security mechanisms that ensure confidentiality, integrity, authentication, and secure communication. Researchers have proposed numerous cryptographic, steganographic, and hybrid security techniques to protect sensitive information from cyber threats. Although significant progress has been achieved, existing approaches often address only specific security aspects, leaving several vulnerabilities unresolved. This survey reviews the major research contributions related to hybrid cryptography, Least Significant Bit (LSB) steganography, secure hashing, and multi-factor

authentication that form the foundation of the proposed dual-layer information hiding framework.

Daemen and Rijmen introduced the **Advanced Encryption Standard (AES)** as a highly secure and computationally efficient symmetric encryption algorithm capable of protecting large volumes of digital information. AES has become the global encryption standard because of its strong resistance against brute-force attacks, efficient execution, and suitability for software and hardware implementations. However, despite its excellent encryption performance, AES requires secure key distribution, which remains one of the major challenges in practical deployment across public communication networks [1].

Koblitz and Miller independently proposed **Elliptic Curve Cryptography (ECC)** as a public-key cryptographic technique that provides equivalent security to RSA while using significantly smaller key sizes. ECC offers efficient key management, lower computational overhead, and reduced memory requirements, making it particularly suitable for cloud computing, mobile devices, Internet of Things (IoT), and embedded systems. Researchers have demonstrated that ECC effectively secures cryptographic keys and significantly improves secure communication when integrated with symmetric encryption algorithms [2], [3].

To overcome the limitations of standalone encryption methods, several researchers have investigated **hybrid cryptographic systems** that combine AES and ECC. In these approaches, AES performs high-speed encryption of confidential data, whereas ECC securely encrypts and exchanges the AES session key. Such hybrid architectures improve confidentiality, secure key management, processing efficiency, and resistance against cryptographic attacks. Experimental studies indicate that hybrid cryptography achieves superior performance compared with independent symmetric or asymmetric encryption techniques, making it highly suitable for cloud-based security applications [4], [5].

Information hiding through **steganography** has emerged as an effective solution for concealing the existence of sensitive information. Unlike encryption, which protects only the content of data, steganography embeds secret information within digital media such as images, audio, or video files. Among spatial-domain methods, **Least Significant Bit (LSB) steganography** has gained widespread acceptance because of its simplicity, high embedding capacity, low computational complexity, and minimal visual distortion. Fridrich demonstrated that LSB embedding enables covert communication while maintaining excellent image quality, thereby significantly reducing the likelihood of detection during data transmission [6], [7].

Researchers have increasingly focused on integrating encryption with steganography to provide multiple security layers. Numerous studies have shown that encrypting confidential information before embedding it within digital images greatly enhances overall security because attackers must first detect the hidden information and subsequently decrypt the encrypted content. Such dual-layer approaches significantly improve confidentiality, concealment, and resistance against unauthorized access compared with conventional encryption-only or steganography-only techniques [8], [9].

Apart from confidentiality, maintaining **data integrity** has become a fundamental requirement in modern cybersecurity systems. The **SHA-256 cryptographic hash algorithm** is extensively employed to generate unique digital fingerprints for files, allowing systems to detect unauthorized modifications during storage or transmission. Researchers have demonstrated that SHA-256 provides excellent collision resistance and reliable integrity verification for secure document management, cloud storage, blockchain technology, and digital forensics. The integration of hashing mechanisms alongside encryption significantly enhances

trustworthiness and protects digital information against tampering [10].

Another important research direction involves strengthening user authentication through **Multi-Factor Authentication (MFA)**. Traditional password-based authentication mechanisms remain vulnerable to phishing attacks, credential theft, and brute-force attacks. NIST security guidelines recommend implementing OTP-based MFA to improve identity verification by requiring an additional authentication factor beyond passwords. Recent studies have confirmed that OTP-based authentication substantially reduces unauthorized access and enhances the overall security of web-based information systems, particularly in cloud computing and financial applications [11], [12].

Recent research has also emphasized the development of **integrated cybersecurity frameworks** that simultaneously combine encryption, secure key management, steganography, hashing algorithms, and authentication mechanisms. Although several proposed systems successfully integrate two or three security technologies, many lack comprehensive implementation of secure authentication, integrity verification, and covert communication within a unified platform. Consequently, there remains a significant research gap in designing a practical, scalable, and comprehensive security architecture capable of addressing all major cybersecurity requirements simultaneously [13].

III.WORKING METHODOLOGY

The proposed system adopts a dual-layer security approach that combines **Hybrid Cryptography** and **Least Significant Bit (LSB) Steganography** to provide secure storage and transmission of confidential information. The methodology integrates multiple security mechanisms, including encryption, secure key management, information hiding, integrity verification, and multi-factor authentication, into a unified web-based platform. The complete workflow is designed to ensure confidentiality, integrity, authentication, and secure communication throughout the entire data lifecycle. Initially, a new user registers by providing basic information such as username, email address, and password. During login, the system authenticates the user credentials and generates a One-Time Password (OTP), which is sent to the registered email address. Only after successful OTP verification is the user allowed to access the system modules. This authentication mechanism prevents unauthorized users from accessing sensitive information and strengthens overall account security. After successful authentication, the user uploads a confidential file or secret message that requires protection. The uploaded file is processed by the Hybrid Encryption module. In the first stage, the Advanced Encryption Standard (AES) encrypts the file using a randomly generated symmetric key, providing high-speed encryption with strong security. Since symmetric encryption requires secure key management, the generated AES key is further encrypted using Elliptic Curve Cryptography (ECC). This hybrid encryption mechanism combines the computational efficiency of AES with the secure key exchange capabilities of ECC, ensuring that both the encrypted file and its encryption key remain protected.

Once the encryption process is completed, the encrypted data is passed to the SHA-256 hashing module. This module generates a unique 256-bit hash value that acts as a digital fingerprint of the encrypted file. The generated hash value is securely stored and later used to verify whether the file has been modified during storage or transmission. Any alteration in the encrypted file results in a completely different hash value, enabling effective detection of tampering. The encrypted file is then forwarded to the LSB Steganography module. In this stage, a cover image is selected, and the encrypted binary data is embedded into the least significant bits of the image pixels. Because only the least significant bits are modified, the visual appearance of the image remains almost identical to the original cover image. The resulting stego

image conceals the existence of confidential information, providing an additional layer of security by making the hidden data virtually undetectable during transmission.

After embedding, the generated stego image, encrypted AES key, and corresponding hash value are securely stored within the system database. Since the confidential information is hidden inside an ordinary image, attackers cannot easily identify that sensitive information is being transmitted or stored. This significantly enhances protection against interception and unauthorized access. During data retrieval, an authenticated user uploads the stego image for recovery. The system extracts the hidden encrypted data from the image by reading the least significant bits modified during the embedding process. The extracted encrypted file is then processed by the ECC decryption module, which recovers the original AES secret key. Using the recovered AES key, the encrypted file is decrypted to reconstruct the original confidential information accurately.

Before providing the recovered file to the user, the SHA-256 integrity verification module generates a new hash value from the decrypted data and compares it with the previously stored hash value. If both hash values match, the system confirms that the file has remained unchanged and has not been tampered with. If the values differ, the system immediately detects unauthorized modification and prevents the delivery of corrupted data. The proposed framework is implemented as a web-based application using **Python**, **HTML**, **CSS**, **JavaScript**, and **MySQL**. The frontend provides user-friendly interfaces for registration, authentication, encryption, steganography, file retrieval, and integrity verification, while the backend manages cryptographic operations, database storage, OTP verification, and secure communication. The modular architecture enables efficient execution, scalability, and easy maintenance while providing comprehensive protection for confidential information.

IV. RESULTSEXPLANATIONS

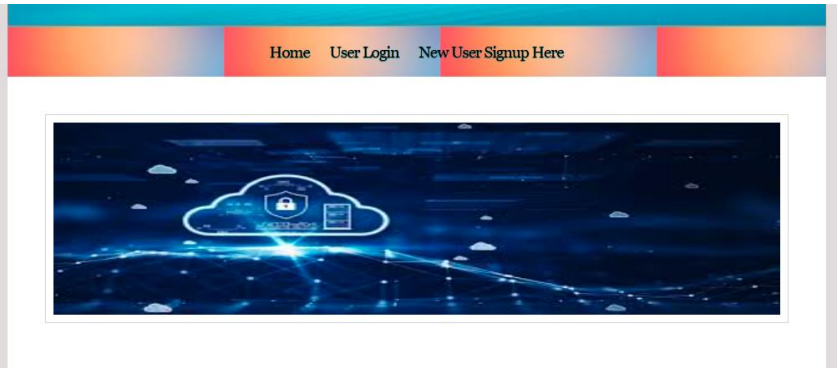


Figure1: Home Page

The above figure illustrates the **Home Page** of the proposed **Cybersecurity: Data Protection using Hybrid Encryption and Steganography** system, which serves as the main entry point for users. The interface provides a simple and user-friendly navigation menu containing options such as **Home**, **User Login**, and **New User Signup**, allowing users to easily access the system's core functionalities. A cybersecurity-themed banner is displayed prominently to represent secure cloud-based communication and digital data protection. From this page, new users can register by creating an account, while existing users can log in to securely access the application. The home page acts as the central gateway to the proposed framework, enabling authenticated users to perform hybrid encryption using AES and ECC, hide encrypted information through LSB steganography, verify data integrity using SHA-256 hashing, and securely retrieve protected files. Its intuitive design ensures easy navigation, improves user experience, and provides

convenient access to all security modules implemented within the application.

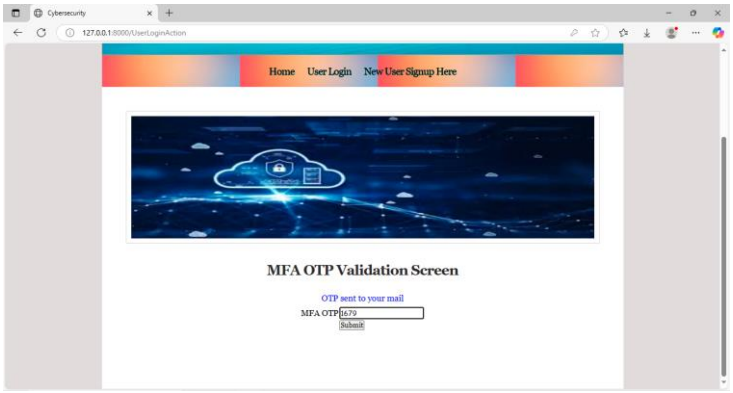


Figure2: MFA OTP Validation

The above figure illustrates the **MFA OTP Validation Screen** of the proposed cybersecurity system, which provides an additional layer of security during the user authentication process. After a user successfully enters valid login credentials, the system automatically generates a **One-Time Password (OTP)** and sends it to the user's registered email address. The user must enter the received OTP into the provided input field and click the **Submit** button to complete the authentication process. This multi-factor authentication mechanism ensures that only authorized users with access to the registered email account can proceed to the application dashboard. By requiring both login credentials and OTP verification, the system significantly reduces the risks of unauthorized access, password theft, phishing attacks, and credential compromise, thereby enhancing the overall security and reliability of the proposed hybrid encryption and steganography framework.

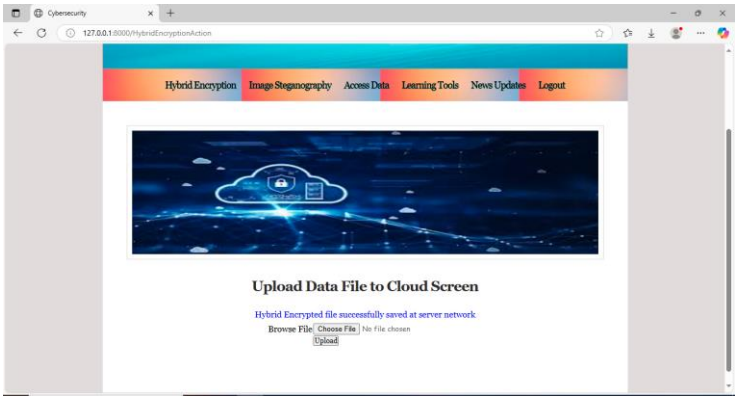


Figure 3: Hybrid Encryption Module

The above figure illustrates the **Hybrid Encryption Module** of the proposed cybersecurity framework, where authenticated users can securely upload confidential files for encryption before cloud storage. The interface provides an **Upload Data File to Cloud** option that allows users to browse and select a file from their local system. Once the file is uploaded, the system performs **hybrid encryption** by first encrypting the file using the **Advanced Encryption Standard (AES)** algorithm to ensure fast and secure data encryption. The generated AES secret key is then protected using **Elliptic Curve Cryptography (ECC)**, providing secure key management and preventing unauthorized key access. After successful encryption, a confirmation message is displayed, indicating that the encrypted file has been securely stored on the server. This module forms the first layer of security in the proposed system by ensuring that confidential information is encrypted before being hidden through steganography or stored in the cloud, thereby protecting sensitive data from unauthorized access and cyber threats.

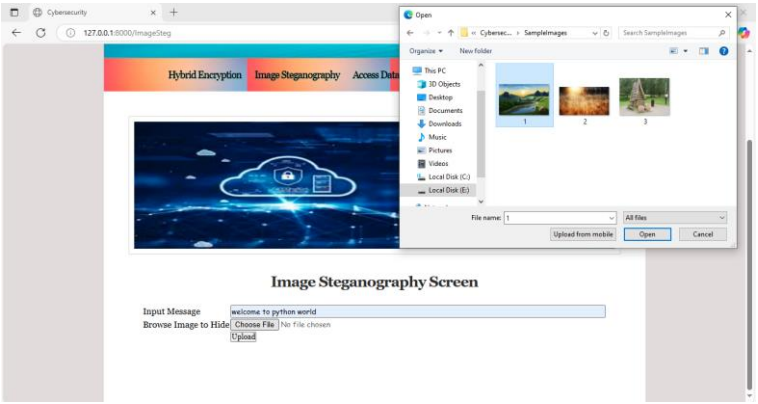
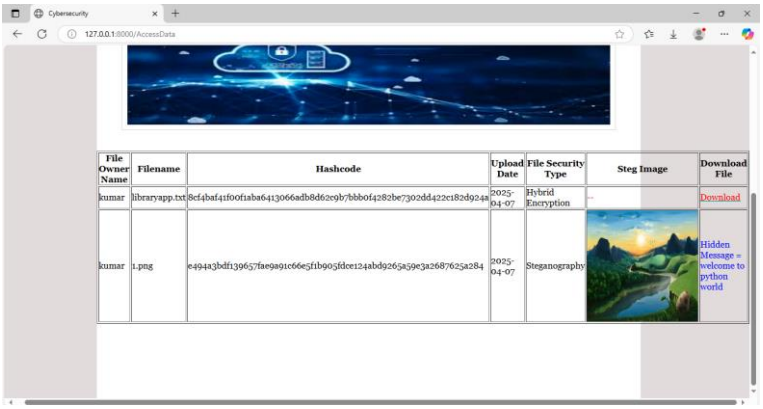


Fig 4 : Image Steganography Module

The above figure illustrates the **Image Steganography Module** of the proposed cybersecurity framework, which is responsible for concealing encrypted information within a digital image. In this module, the user enters a confidential message or selects an encrypted file and then chooses a suitable **cover image** from the local system using the file selection dialog. After clicking the **Upload** button, the system applies the **Least Significant Bit (LSB) steganography** algorithm to embed the encrypted data into the least significant bits of the image pixels. Since only the least significant bits are modified, the visual appearance of the cover image remains almost identical to the original image, making the presence of hidden information imperceptible to the human eye. The generated **stego image** securely carries the concealed information and can be transmitted or stored without attracting attention. This module serves as the second layer of security by combining information hiding with hybrid encryption, thereby significantly enhancing data confidentiality and protecting sensitive information from unauthorized detection and cyber attacks.



V.CONCLUSION

The proposed **Secure Dual Layer Information Hiding Framework Utilizing Hybrid Cryptography and Least Significant Bit (LSB) Steganography** successfully addresses the growing challenges of protecting sensitive information in modern digital communication and cloud computing environments. By integrating **Advanced Encryption Standard (AES)** for fast and secure data encryption with **Elliptic Curve Cryptography (ECC)** for efficient key management, the framework provides strong confidentiality while overcoming the limitations of conventional single-layer encryption techniques. The incorporation of **Least Significant Bit (LSB) steganography** further enhances security by concealing encrypted information within digital images, making the existence of confidential data virtually undetectable to unauthorized users.

To strengthen the overall security architecture, the system incorporates **SHA-256 hashing** for data integrity verification and **OTP-based Multi-Factor Authentication (MFA)** to ensure that only authenticated users can access encryption and decryption services. The implementation of the proposed framework as a web-based application using **Python, HTML, CSS, JavaScript, and MySQL** provides a practical, scalable, and user-friendly platform for secure file encryption, steganographic embedding, hidden data extraction, integrity verification, and authenticated communication. Experimental results demonstrate that the framework effectively protects sensitive information while maintaining efficient execution performance and preserving the visual quality of the cover images.

REFERENCES

[1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Hoboken, NJ, USA: Pearson, 2023.

[3] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[4] V. S. Miller, "Use of Elliptic Curves in Cryptography," in *Advances in Cryptology – CRYPTO '85*, Lecture Notes in Computer Science, vol. 218. Berlin, Germany: Springer, 1986, pp. 417–426.

[5] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2018.