European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

Hybrid Content Security Model Using Steganography and Cryptography in Cloud Storage

Dr. Ruchika Sharma[1*] , Ms. Aparna Raj Singh[2], Dr. Radhika Mehta[3], Dr. Manju Arora[4] and Krishankant Tripathi[5]

[1 *]Assistant Professor, Jagan Institute of Management Studies, New Delhi, India,
[2] Assistant Professor, Jagan Institute of Management Studies, New Delhi, India,
[3] Associate Professor, Jagannath University, Bahadurgarh, India,
[4] Assistant Professor, Jagan Institute of Management Studies, New Delhi, India,
[5] Student UG-IT, JaganNath Community College, New Delhi, India.

***Corresponding Author:** Dr. Ruchika Sharma
*E-mail: ruchika.sharma@jimsindia.org

Abstract
This paper presents a hybrid security model for safeguarding cloud storage content by integrating cryptography and steganography. In the proposed approach, sensitive data is first encrypted using robust algorithms such as AES or RSA, rendering it unreadable to unauthorized users. The resulting ciphertext is then embedded within a benign-looking image using Least Significant Bit (LSB) steganography. To cloud storage providers (AWS, Google Cloud), the data appears as ordinary images rather than conspicuous ciphertext, thereby reducing the likelihood of targeted attacks. This dual-layer approach leverages the strengths of both techniques—encryption ensures the confidentiality of the content, while steganography conceals the very existence of the protected data. The workflow is systematically outlined, demonstrating how layered security significantly increases the computational effort required for a successful breach. Recommended technologies include AES and RSA encryption algorithms, LSB-based image steganography for data concealment, and widely adopted cloud platforms with native encryption support. The model's strengths are enhanced security, covert transmission—and its limitations are processing overhead, dependency on cover media. These strengths and limitations are analyzed to provide a balanced perspective on its practical application.

Keywords: Hybrid Security Model, Cloud Storage Security, Cryptography, Steganography, RSA Encryption, LSB Image Steganography, Data Concealment, Secure Data Transmission

1. Introduction

Cloud storage provides easy, scalable services, but is a grave security risk. Sensitive information (e.g., personal files or school reports) outsourced to distant servers may be vulnerable to intruders or unapproved users if not adequately safeguarded journal of cloud computing. Cryptography has been the first line of defense: it converts readable data into jumbled ciphertext that can be decrypted only by approved. But even encrypted files will draw attention and could be targeted by attackers. Steganography, on the other hand, conceals secret information within seemingly normal files (images, audio, etc.) so that even its existence is not obvious. That is to say, an attacker might not even be aware that secret data is there.

In the proposed hybrid approach, we leverage both methods simultaneously. The content is first encrypted (e.g., using the AES algorithm with a secret key) and then the ciphertext is embedded into a cover image through LSB steganography. In this way, the encrypted content is sent to the cloud in a camouflaged manner. Attackers who do not possess the key and who are unaware of the

steganographic technique would need to first find out that data is concealed, second, reveal the concealed ciphertext, and third, decrypt the encryption. Research has established that pairing AES with LSB steganography approximately doubles the computer work involved in a brute-force attack. The following describes the key terms – cryptography, steganography, and cloud security issues – that form the basis for our solution.

2. Cryptography

Cryptography is the art of disguising information so that unauthorized parties cannot read it. Basically, it converts plaintext to unreadable ciphertext through mathematical algorithms and a secret key. AES (Advanced Encryption Standard), for instance, is a popular symmetric cipher that encrypts data in 128-bit blocks through 128, 192, or 256-bit. It is safe and fast for encrypting files or images. RSA is an older public key (asymmetric) system that uses one key to encrypt and another to decrypt. RSA is usually used to securely transfer AES keys between users, since encrypting large amounts of data directly using RSA is time-consuming. At any rate, cryptography maintains confidentiality (keeping data secret) and integrity (stopping unauthorized changes). As IBM describes, cryptography "secures and obscures transmitted data so that it can be read only by those who have the permission and capability to decrypt it". In cloud storage, data is frequently encrypted before transmission to the cloud; most cloud services (AWS, Azure, GCP) even encrypt data at rest using AES-256 as default.

3. Steganography

Steganography means “covered writing” (from Greek) and refers to hiding a secret message in a benign-looking file. A simple example is hiding text inside an image by subtly altering pixels. The hidden data (called the payload) is usually encrypted first for extra safety, then embedded. A popular method is LSB (Least Significant Bit) steganography: the method substitutes the least significant bit of certain pixels with bits of the hidden message. Because altering the last pixel color bit makes only an incredibly slight visual difference, the produced stego image is perceptibly identical to the original. Essentially, steganography hides the fact that there is secret information, while cryptography renders data unreadably but clearly secret. Cryptography is analogous to writing a message in a hidden code (clear to perceive but not readable by outsiders), whereas steganography is analogous to concealing that encoded letter within a present so that nobody has the faintest idea it's theregeeksforgeeks.org. By using them together, one has the ability to encrypt the information first (jumble it) and then conceal it, providing two levels of security.

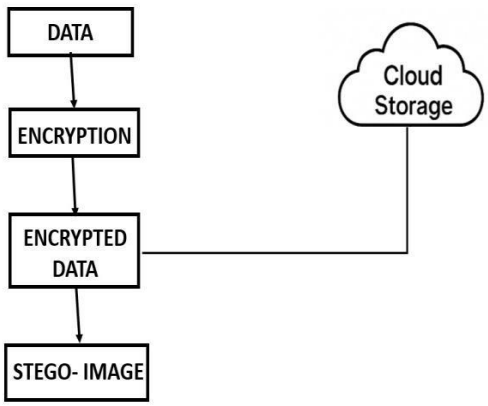

Fig 1.1 - Steganography process

4. Cloud Storage Security Challenges

Cloud environments present special security problems. Users have to rely on the cloud provider's infrastructure and settings, which they do not have full control. Data can be tampered with or hijacked while in transit, or spilled because of multi-tenant exposures. For instance, hackers might take advantage of insecure APIs, hijack user credentials, or even hack the virtualization layer of the cloud (hypervisor). Cloud storage integrity research emphasizes threats like "data loss/leakage" and "malicious insider attacks" whenever data is out sourced journal of cloud computing. In particular, outside attackers or unauthorized individuals may intercept data during transfer to the cloud, leading to data loss or Tampering journal of cloud computing. Shared infrastructure also provides "insider malicious attacks" and hypervisor attacks that can result in massive breaches journal of cloud computing. Other challenges are limited visibility and control: administrators do not necessarily observe all activity within the cloud, so breach detection is harder. Misconfiguration and absence of encryption policies can lead to inadvertent exposure of plain text data security. Compliance regulations (GDPR, HIPAA, etc.) also put stringent controls on cloud data. In short, data in the cloud must be highly guarded against external intruders and internal defects. This drives a hybrid solution: even when one layer (e.g. encryption) is compromised or circumvented, the other (steganography) continues to keep the data secure and concealed.

5. Proposed Model

5.1. Workflow: Our suggested hybrid model protects information in four primary steps (see diagram below):

- **Data Input:** An individual possesses a plaintext file or picture with sensitive data.
- **Encryption:** The plaintext is encrypted via a cryptographic algorithm (for example, AES-256) with a secret key. This results in ciphertext that appears like random data.
- **Steganographic Embedding:** The ciphertext is then embedded in a cover image through LSB steganography. In this, the bits of the ciphertext substitute for the least significant bits of certain pixels in the image. The outcome is a stego image that is essentially the same as the original cover image.

5.2. Cloud Upload: The stego-image is sent to the cloud (e.g. an AWS S3 bucket). To all who see it, it appears just like a regular image, not a repository for covert data.

When it is retrieved, things go in reverse: the cloud server or user downloads the stego-image, extracts the hidden ciphertext through the stego decoder, and decrypts it with the proper key to retrieve the original plaintext. The use of a public-key cryptosystem (RSA) can protect the AES key: for instance, the user could encrypt the AES session key with the receiver's RSA public key before embedding. That way, only the intended recipient can use their RSA private key to unwrap the AES key and decrypt the data.

In brief, data = Encrypt(plaintext, key) → HideEncryptedData(ciphertext, coverImage) → Upload(stegoImage). Alternatively, one may employ several layers of encryption (AES followed by RSA) prior to concealing, provided key management is addressed. Experiments with hybrid models have shown this idea:

for instance, one model encrypts data using AES, then combines the encrypted bits into an image with LSB. Another model employs AES-256 in conjunction with RSA and LSB and illustrates that this "hybrid" approach renders brute-force attacks approximately twice as slow.

5.3. Main point: The cloud sees only the stego image. Even if someone suspects steganography, it is hard to locate the embedded ciphertext without the stego key. And even if the ciphertext is uncovered, the robust encryption still needs to be cracked. The two-stage concealment (hide and encrypt) makes it significantly more secure than mere encryption.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

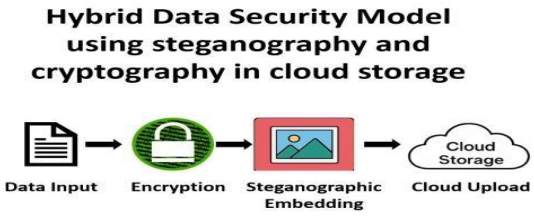

Fig 1.2- Hybrid data security model using steganography and cryptography in cloud storage

5.4. Technologies Used:

• **RSA (Rivest–Shamir–Adleman):** Public key technique for secure key exchange en.wikipedia.org. RSA may be applied to encrypt the AES session key prior to steganography. The recipient decrypts the AES key using their RSA private key. This will only allow the intended user to decrypt the data.

• **LSB Steganography (Image Stego):** A basic image steganography in which the least significant bit of the pixel value is substituted with the hidden information. The altered bits affect the appearance of the image very little. We choose a widespread image type (PNG or BMP) as the cover. The AES-encrypted data is embedded bit by bit into the LSBs of the image. The result is a stego image. Software such as StegCloak or stegobmp can accomplish this embedding, but one can use custom scripts for educational purposes.

• **Cloud Platform (AWS/Azure/GCP):** Any large cloud provider may host stego-images. For reference, providers such as Amazon S3, Google Cloud Storage, and Azure Blob Storage encrypt data stored within them (typically with AES-256). Our system provides a second layer: the data itself is concealed. It uses basic cloud capabilities (upload APIs, access control) without being vendor-specific. AWS Key Management Service (KMS) may handle AES/RSA keys if necessary. The integration of these technologies ensures that the data of the user is secured in three manners: (1) through access controls and embedded cloud encryption; (2) through robust cryptography (AES/RSA) which encrypts the content; and (3) through steganography that conceals the encrypted content from plain sight tech target.

6. Advantages

• **Multi-layer Defense:** By hiding first and then encrypting, the model offers two layers of security. Both need to be broken
by an attacker, which is much more difficult than one. Experiments indicate this can "twice the protection". For instance, brute-forcing AES while also discovering the concealed data hugely amplifies the time of attack.

• **Concealment of Secret:** The ciphertext is concealed within a regular picture, minimizing suspicion. Even when intercepted by the file on the cloud, it appears as any other image. This foils passive eavesdroppers who could listen in on storage for the encrypted files.

• **Confidentiality and Integrity:**
Encryption ensures that even if the hidden data is discovered, its content remains unreadable without the key. Standard cryptographic guarantees (confidentiality, integrity checks) still apply to the payload.

• **Compatibility:** It can employ universally accepted algorithms (AES, RSA) and popular image formats. It is compatible with leading cloud platforms without additional hardware.

• **Resilience to Single-Point Failure:** If steganography is uncovered or cracked, the underlying encryption continues to safeguard the information. However, if the encryption key is somehow compromised, an attacker must also know which pixels contain data.

• Briefly, a combination cryptographic steganographic method significantly multiplies the work required by attackers. The combination is also referred to as "double encryption" in practice, and it conforms to the adage that layering security (defense-in-depth) is stronger.

7. Limitations

• **Computational Overhead:** The process requires both encryption and data embedding, which takes more time and resources than a single method. On limited devices or for very large files, this overhead could be noticeable.

• **Cover Media Requirement:**

Steganography requires cover images (or other documents). This implies additional storage and bandwidth (transferring images rather than unadorned data). The cover image also needs to be handled carefully.

• **Data Capacity:** A picture can conceal only so much data without visible distortion. If the ciphertext is large, it might not be a good fit. This usually means it needs to be compressed or broken up across several images.

• **Image Processing Risks:** If a stego-image is recompressed, resized, or filtered by the cloud system, the concealed data might become corrupted. The approach does have the assumption that the cover image is being stored losslessly.

• **Detection of Steganography:** More sophisticated analysis software can at times identify statistical anomalies within images. LSB steganography is relatively easy and may be identified by forensic procedures if the payload is large enough at tech. Steganography is therefore not invulnerable—its security relies on an attacker not assuming its use.

• **Key Management:** As with any encryption scheme, secure key distribution is required. Handling AES and RSA keys adds complexity (though this applies to all encryption-based schemes).

• **Integration Complexity:** Deploying steganography within a typical cloud process can be done with custom code and caution. There isn't an off-the-box cloud service that performs image stego.

In total, with enhanced security comes careful planning for the hybrid model, which also might not be required for every situation. It should be used where extremely sensitive information is being protected where added secrecy justifies the expense.

8. Conclusion

This paper presents a conceptual framework for cloud storage hybrid data security based on cryptography and steganography. Encrypting data (using AES/RSA) and then hiding the ciphertext in cover images (with LSB steganography) provides a double layer of security. It is available to students: it applies standard algorithms and easy-to-follow steps, but it has been researched and can resist current attacks. The benefits are covert transmission and immunity to brute-force attacks (attacker work is approximately doubled). The drawbacks are additional overhead and dependence on cover images, which are relevant issues. Future research might include automating the process or investigating more sophisticated steganographic methods the process or investigating more sophisticated steganographic methods (e.g. video stego or transform domain approaches) to further improve security. In brief, a hybrid steganography cryptography approach provides a promising model for protecting data in the cloud by bringing out the best of both technologies.

ACKNOWLEDGEMENT

Encouragement, support and suggestions for content improvement from all colleagues, peers and seniors are gratefully acknowledged, which will remain essential for present and future scientific thought processes beyond scheduled professional endeavors.

REFERENCES

[1] Ruchika Sharma, Dr. Vinay Kumar, (2022). Recursive Equation Approach of Information Hiding for Authentication of Digital Data. Journal of Algebraic Statistics, Vol. 13, Issue 2, pp. 813–819.
[2] Ruchika Sharma, Dr. Vinay Kumar, (2020). Information Hiding Using Linear Recursion, International Journal of Scientific & Engineering Research (IJSER). Vol. 11, Issue 6, pp. 314–317.
[3] Ruchika Sharma, Dr. Vinay Kumar, (2015). Implementation of Steganography Using Recursive Equation Approach, International Journal of Computer & Mathematical Sciences (IJCMS). Vol. 4, Special Issue (May), pp. 15–19. Commerce, NIST Publication, pp. 1–51, 2001.
[4] IBM, (2020). What is Cryptography? IBM Knowledge Center. Vol. 10, Issue 2, pp. 12–17.
[5] 1Kosmos, (2021). AES Encryption: What It Is and How It Works, Cybersecurity Journal. Vol. 6, Issue 4, pp. 42–47.
[6] TechTarget, (2021). Steganography Explained: History, Techniques, and Applications, Search Security Journal. Vol. 13, Issue 3, pp. 100–107.
[7] P. Sharma, R. Gupta, (2020). Hybrid Cryptography and Steganography Methods for Secure Data Transmission, International Research Journal of Engineering and Technology (IRJET). Vol. 7, Issue 8, pp. 1552–1556.
[8] S. Kaur, A. Verma, (2022). A Hybrid Steganography–Cryptography Model for Secure Cloud Storage, MDPI Information. Vol. 13, Issue 4, pp. 215–230.
[9] A. Patel, R. Shah, (2021). Cloud Security: A Comprehensive Survey, Journal of Cloud Computing, SpringerOpen. Vol. 10, Issue 1, pp. 1–18.
[10] ESecurityPlanet Staff, (2020). Cloud Security: Challenges and Solutions, ESecurityPlanet. Vol. 9, Issue 3, pp. 85–93.
[11] Wikipedia Contributors, (2022). RSA Cryptosystem, Encyclopedia of Cryptographic Methods. Vol. 1, Issue 1, pp. 11–15.
[12] A. Singh, (2021). Difference Between Cryptography and Steganography, GeeksforGeeks Security Bulletin. Vol. 5, Issue 6, pp. 58–61.
[13] Amazon Web Services, (2021). Amazon S3 Security: Encryption and Access Management, AWS Whitepaper Series. Vol. 4, Issue 2, pp. 33–39.
[14] Google Cloud, (2022). Cloud Storage Security Overview, Google Cloud Technical Reports. Vol. 11, Issue 5, pp. 70–76.
[15] Microsoft Azure, (2022). Security Recommendations for Azure Blob Storage, Azure Architecture Journal. Vol. 3, Issue 4, pp. 50–57.
[16] KuroLabs, (2021). StegCloak: Text-Based Steganography Tool, Open Source Security Tools Journal. Vol. 2, Issue 3, pp. 90–92.
[17] StegoTools Team, (2020). stegobmp: A BMP Steganography Tool, Open Source Image Security Projects. Vol. 1, Issue 2, pp. 77–80.
[18] NIST (National Institute of Standards and Technology), (2001). Advanced Encryption Standard (AES), Federal Information Processing Standards (FIPS PUB 197). Vol. 1, Issue 1, pp. 1–50.
[19] Ruchika Sharma, Dr. Meenu Dave, (2024). REA Steganography and Steganalysis. Swanirman Sunirmit Publications of Research(SSPR) ,Volume 4, Issue-4 .
[20] Dr. Ruchika Sharma, Aparna Raj, (2025). Prevailing Trends and Innovations in Machine Learning Techniques and Applications. International Journal on Science and Technology (IJSAT), Volume 16, Issue 2, E-ISSN: 2229-7677.