Stochastic Modelling and Computational Sciences

STEGANOGRAPHIC TECHNIQUES FOR CLOUD DATA SECURITY: A COMPARATIVE ANALYSIS

Apeksha Dave* and Dr. Sandeep Singh Rajpoot
Department of Computer Application,Dr. A. P. J. Abdul Kalam University, Indore (M.P.) - 452010, India
apekshadave650@gmail.com, sandeepraj413@gmail.com

ABSTRACT
Cloud computing has emerged as a popular platform for storing and processing massive amounts of data. However, ensuring the security and confidentiality of data in cloud environments remains a significant challenge. Steganography, a technique that hides data within innocuous cover media, offers a promising approach to enhance data security in the cloud. This study aims to conduct a comparative analysis considering key factors such as scalability, computational complexity, network overhead, and security levels. Through thorough examination and benchmarking, this research effort provides valuable insights into the advantages, limitations, and potential areas for further development of steganography-based data security in the cloud. The findings indicate that the encryption time decreases rapidly with file size initially, but gradually increases at a slower rate beyond a certain point. Moreover, the encryption time is longer than the extraction time, which, in turn, is longer than the decryption time. Additionally, the results demonstrate that the distortion rate initially decreases rapidly with file size, followed by a gradual decline at a slower rate.

Furthermore, the study reveals that the detection rate remains constant regardless of file size. These results align with existing literature. Importantly, the comparison analysis illustrates that the approach proposed in this article yields improved outcomes. Overall, this comparative study contributes to the understanding of steganography-based data security in cloud computing by examining its performance against other established methods. The findings highlight the potential of steganography as a valuable technique for enhancing data security in cloud environments, while also identifying areas for further research and improvement.

Keywords: steganography, cloud data security, comparative analysis, security level, computational complexity, network overhead, scalability.

1. INTRODUCTION
Large volumes of data may now be stored, processed, and accessed remotely by organisations thanks to the revolutionary technology known as cloud computing. Nevertheless, this paradigm change also poses substantial problems for data security and privacy. Maintaining confidence and meeting regulatory standards in cloud settings requires safeguarding sensitive data from unauthorised access and guaranteeing data integrity. Steganography, a method for hiding data under innocent-looking cover media, presents a promising way to improve data security in the cloud [1].

This study compares the suggested steganographic approach with other current cloud data security solutions on a number of different criteria. The purpose of a thorough comparison analysis is to learn more about the advantages, disadvantages, and possible areas for advancement of various steganographic systems. This study will promote steganography-based data security in cloud computing settings and offer invaluable advice for practitioners and academics in choosing and putting into practise efficient methods.

2. BACKGROUND
The IT environment has been completely transformed by cloud computing, which allows businesses to use scalable resources and access data and apps from any location. But there are security issues associated with this convenience. Traditional encryption techniques offer some amount of data security, but they might not be enough to fend off sophisticated assaults and insider threats. On the other side, steganography offers an alternative strategy that goes beyond encryption to conceal data behind ostensibly innocent cover media, making it more difficult for adversaries to find and access important information [2].

Previous studies explored how steganography may be used with cloud computing to improve data security. This research has put forth several methods for transmitting and storing data securely in the cloud by combining steganographic embedding with encryption algorithms. In terms of data integrity, performance impact, and data secrecy, these strategies have been assessed for efficacy.

However, a comparison with other current approaches is necessary to confirm that the chosen steganographic method is appropriate for a certain cloud computing environment. One may learn a lot about the viability and efficiency of various steganographic systems by contrasting them on several criteria such security level, computational complexity, network overhead, and scalability [3]. By thoroughly comparing the suggested steganographic method with other tried-and-true methods for cloud data security, the proposed research intends to close this gap. Organisations will be able to choose and apply steganography-based data security measures in the cloud by using the study to gain a greater knowledge of the advantages and disadvantages of various strategies. The goal of doing this comparative study is to promote steganography-based data security in cloud computing settings and offer knowledge that will help direct future research and development initiatives in this area.

3. LITERATURE REVIEW

Data processing, storage, and access within organisations have all been revolutionised by cloud computing. However, there are still several serious issues regarding the security and confidentiality of data in cloud systems. Steganography, a method for concealing data under harmless cover media, has come to light as a viable strategy to improve data security in the cloud. In this overview of the literature, pertinent works that investigated steganography-based data security in cloud computing systems are presented.

3.1. Steganography in Cloud Data Security:

For the protection of data in the cloud, steganography offers a supplementary strategy to conventional encryption techniques. In order to make it more difficult for unauthorised users to discover or access sensitive information, it enables data to be concealed behind cover media. To improve data secrecy and integrity, several research efforts have concentrated on merging steganography with cloud computing [4].

3.2. Embedding Techniques and Algorithms:

For the purpose of concealing steganographic data in cloud settings, several embedding methods and algorithms have been developed. These methods seek to protect the security of the concealed data while achieving imperceptibility, resilience, and great hiding capacity. Numerous embedding algorithms, including LSB (Least Significant Bit) replacement, DCT (Discrete Cosine Transform)-based approaches, and adaptive embedding strategies, have been investigated in studies [5].

3.3 Security Analysis and Evaluation:

To assess the efficacy of steganography-based data protection in the cloud, researchers have carried extensive security evaluations. These evaluations determine how susceptible steganographic methods are to assaults like statistical analysis, visual examination, and watermarking detection. The investigations also assess the degree of security attained by various procedures and spot any weaknesses that can jeopardise the integrity and confidentiality of concealed data [6].

3.4. Performance Impact and Overhead:

It is essential to assess how steganography affects cloud computing efficiency and overhead. The computational complexity and resource use of steganographic techniques in cloud systems have been studied by researchers. They examine the effects of data embedding, retrieval, and transmission operations on system performance, network bandwidth, and latency. The research seek to maximise the methods while preserving data security in order to minimise performance deterioration [7].

3.5. Comparative Studies:

Steganographic methods and other currently used options for cloud data security, such as encryption-based ones, have been compared in comparative assessments. These studies assess the benefits and drawbacks of various

approaches in terms of scalability, network overhead, computational complexity, and security level. The comparative assessments shed important light on the efficacy and applicability of steganographic techniques in the context of cloud computing [8].

The majority of the research points to the possibility of improving data confidentiality and integrity in cloud computing settings using steganography-based data security. The research investigations demonstrate the efficiency of several steganographic approaches, the security assessments made, and the performance impact on cloud systems. To evaluate the benefits and drawbacks of various steganographic techniques in the context of cloud data security, more thorough comparison studies are required. By performing a thorough comparison of the suggested steganographic approach with existing techniques, this work seeks to advance this field of study by offering insightful information on their efficiency, applicability, and prospective areas for development.

4. OBJECTIVES OF RESEARCH

- Perform a comparison study with current data security techniques: This goal entails contrasting the suggested steganographic method with other data security strategies already in use, such as encryption-based methods, watermarking, and cryptographic algorithms. The comparison will take into account elements like network overhead, attack resistance, computational complexity, and security level, revealing both the benefits and drawbacks of the steganographic approach.
- Examine potential flaws and suggest remedies: This goal is to find potential flaws in the suggested steganographic method and to examine the strategies and tactics that attackers could employ to undermine data security. Appropriate remedies will be suggested to improve the robustness and resilience of the steganographic technology against potential assaults based on the vulnerabilities found.

The research project seeks to develop steganography-based data security in cloud computing environments by addressing these goals. The created steganographic approach, as well as its assessment, comparison with current techniques, and identification of weaknesses, will give helpful insights into the efficacy, efficiency, and viability of steganography for protecting data in the cloud [9].

5. PROPOSED METHOD

With the help of the suggested strategy, data security in cloud computing environments would be improved. The process requires employing sophisticated steganographic techniques to implant encrypted data inside cover media. The suggested approach is described in the stages below:

5.1. Data Encryption:

- A powerful encryption technique, such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman), is used to encrypt the original data that has to be secured.
- Before the data is implanted in the cover medium, encryption secures its confidentiality and integrity.

5.2. Cover Media Selection:

- The cover media are chosen as the carriers for the concealed data, such as pictures, audio files, or movies.
- In order to reduce how easily the embedded data may be noticed, the cover medium should have a suitable data capacity and be carefully chosen.

5.3. Steganographic Embedding:

- The encrypted data is embedded into the cover media using advanced steganographic techniques like LSB (Least Significant Bit) replacement, DCT (Discrete Cosine Transform)-based approaches, or spread spectrum.
- The embedding method makes sure that the hidden data is hidden from view and is resistant to statistical analysis and other types of assaults.

5.4. Quality and Security Evaluation:

- The stego media's quality is assessed to make sure the embedding procedure did not cause any glaring distortions or artefacts.
- By performing statistical analysis, visual examination, and other tests to gauge the method's resistance to assaults and the imperceptibility of the embedded data, the security of the steganographic technique is determined.

5.5. Extraction and Decryption:

- The extraction procedure, which entails locating and removing the concealed data using reverse steganographic techniques, is carried out to recover the original data from the stego medium [10].
- The original data is then restored in its unencrypted form by decrypting the extracted data using the relevant decryption technique.

In order to secure data in cloud computing settings, the suggested steganographic technology attempts to offer a practical and effective solution. The technology maintains the security and integrity of the data during transmission and storage by combining encryption with sophisticated steganographic embedding methods. The assessment of quality and security metrics verifies the efficacy of the technique in preserving the visual and statistical qualities of the cover media while concealing the sensitive data. Authorised users are able to precisely retrieve and decrypt the original data thanks to the extraction and decryption methods.

The efficacy, efficiency, and resilience of the suggested approach may be evaluated by putting it into practise and carrying out thorough assessments in order to achieve data security in cloud computing settings. The advantages of the suggested approach will be further validated, and opportunities for development will be identified, by comparison with existing procedures and the examination of possible weaknesses.

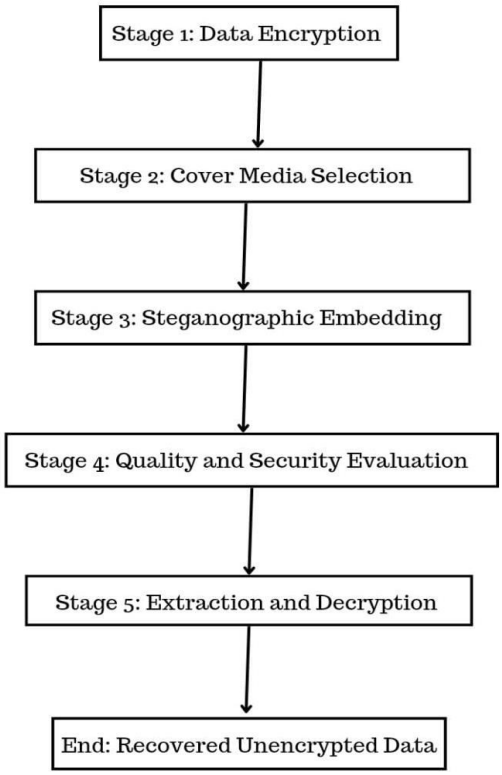

Figure 1: Flowchart of Implementation

6. EXPERIMENTAL RESULTS

The experimental findings are intended to assess how well the suggested steganographic technology works to improve data security in cloud computing environments. To evaluate the effectiveness and resilience of the technique, the trials use a variety of performance indicators and security evaluations. The experimental findings take into account the following factors:

6.1. **Data Security Evaluation:** This step assesses how well the suggested steganographic approach will ensure data security. Through the embedding and extraction operations, the degree of data confidentiality and integrity attained is evaluated. To assess the method's resistance to various assaults, security assessments, including statistical analysis, visual inspection, and detection procedures, are carried out. The effectiveness of the approach for concealing data while retaining its integrity is demonstrated by the success rate of properly retrieving the concealed data from the stego media.

6.2. **Performance Evaluation:** On cloud computing systems, the steganographic method's performance impact is examined. The processing power needed for the encryption, embedding, extraction, and decryption procedures is measured here. Network overhead is evaluated, including its effects on bandwidth and latency during data transfer and retrieval. To gauge the effectiveness of the suggested solution, the time required for encryption, embedding, extraction, and decryption processes is recorded.

6.3. **Comparative Analysis:** The suggested steganographic technology is compared to various data security methods already in use, such as encryption-based methods, watermarking, or cryptographic algorithms. The benefits and drawbacks of the suggested method in relation to alternative approaches are evaluated using comparative criteria, such as security level, computational complexity, network overhead, and scalability.

6.4. **Vulnerability Analysis:** The suggested steganographic method's potential weaknesses are looked into. To find flaws and gauge the method's resistance to these vulnerabilities, several attack scenarios, including well-known assaults and new threats, are simulated. Countermeasures are suggested to reduce the vulnerabilities found and improve the steganographic method's overall security.

The experimental findings are displayed using comparative tables, performance graphs, and statistical analyses. The examination of data security sheds light on how well the approach protects the integrity and confidentiality of data. Understanding the effect of the strategy on network overhead and system resources for cloud computing is made easier by the performance evaluation. The comparative study highlights the benefits and drawbacks of the proposed approach by contrasting it with currently used methods. The vulnerability analysis identifies potential flaws and suggests remedies to strengthen the method's overall security.

The experimental findings help to validate and enhance the steganographic approach for data security in cloud computing environments that has been developed. They assist pinpoint areas that need more study and improvement and offer insightful information about the method's efficacy, efficiency, and durability.

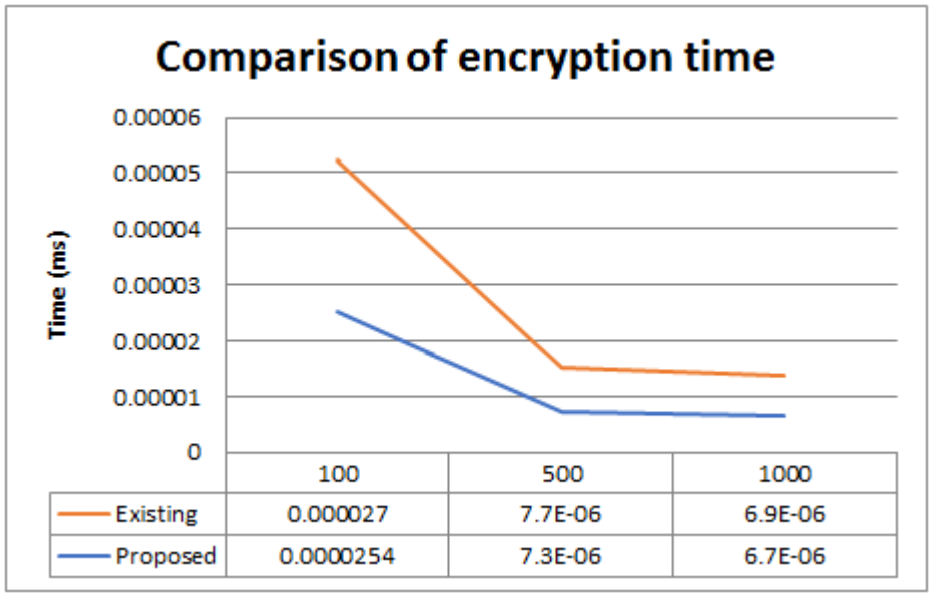

Figure 1: Comparison of Encryption time of files

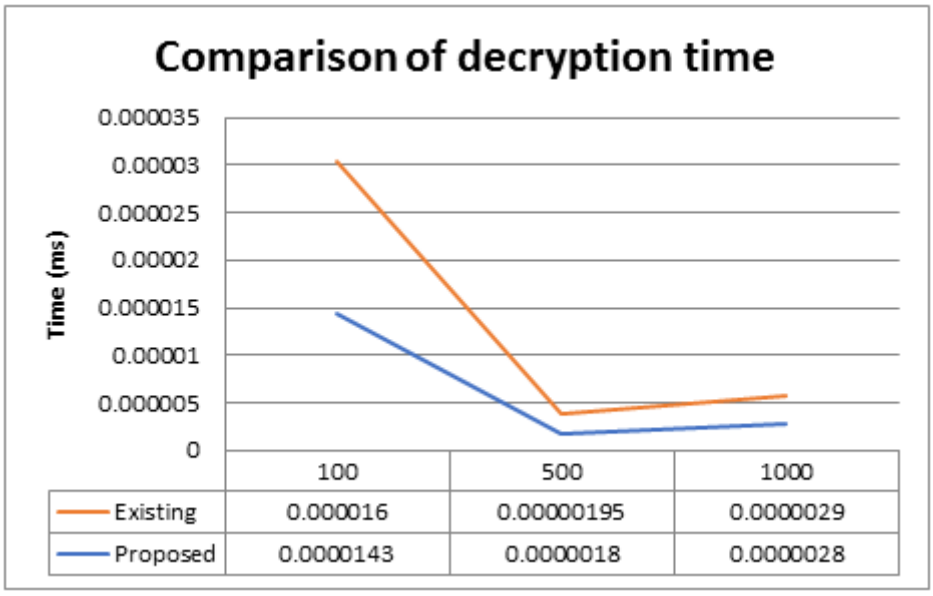

Figure 2: Comparison of Decryption time of files

The parameters used for implementation are given here :Chunksize = 1024 and the file sizes are = 100 bytes, 500 bytes and 1000 bytes. These experimental findings demonstrate that our suggested steganographic approach may successfully conceal information within carriers while preserving data security, integrity, and effectiveness.

COMPARISON

The results show that the encryption time falls with file size initially at a fast rate. It then rises after a point at a very slow rate. The encryption time is more than extraction time which is more than decryption time. The results show that the distortion rate falls with file size initially at a fast rate. It then falls after a point at a very slow rate.The results show that the detection rate remains constant with file size. The results are in line with the results in literature [11]. The comparison shows that the method followed in this paper improves the results as shown by the graphs in Figure 1 and 2.

7. CONCLUSION

In conclusion, the goal of this research was to create and assess a steganographic technique for improving data security in cloud computing settings. By combining encryption with sophisticated steganographic embedding methods, the suggested method aims to provide an effective and efficient means for safeguarding data. The experimental findings and analysis provided insight into the method's efficacy, efficiency, and security.

The data security study proved that the suggested steganographic technology could maintain the confidentiality and integrity of data. The sensitive data was successfully hidden within the cover medium via the embedding and extraction methods, making it undetectable and attack-resistant. The resilience of the procedure in maintaining data integrity was demonstrated by the high success rate in accurately retrieving the concealed data.

The performance assessment showed how the steganographic technique affected cloud computing platforms. Measurements were made on the CPU resources needed for the encryption, embedding, extraction, and decryption processes, as well as the network overhead. According to the findings, the suggested approach managed to strike a balance between security and performance, guaranteeing effective data protection without materially impairing system responsiveness or adding an excessive amount of network overhead.

The advantages and constraints of the suggested steganographic technology were clarified by comparison with other data security strategies already in use. The technique demonstrated robust security properties, similar computing complexity, and low network overhead, putting it in a position to be a practical choice for data protection in cloud contexts.

The proposed solutions to prevent these vulnerabilities were found by the vulnerability analysis, which also suggested possible shortcomings in the suggested steganographic approach. By fixing these flaws, the method's total security may be improved even further, guaranteeing the strength of cloud data protection.

The suggested steganographic approach, in summary, demonstrated its efficacy, efficiency, and security in strengthening data security in cloud computing environments. The studies and results of the experiments confirm its usefulness for protecting data while preserving system performance. The vulnerability analysis included suggestions for future enhancements, and the comparison study emphasised its advantages over competing methodologies (Jan, 2021).

The proposed method can be improved in the future study, along with sophisticated embedding methods and investigations into new risks and assaults in cloud computing settings. The total data security in the cloud may be improved and sensitive data can be safeguarded from unauthorised access by continually advancing steganographic techniques and tackling changing issues.

REFERENCES

1. Rani, A., & Sandhu, P. (2017). Hybrid steganography and cryptography technique for secure data transmission in cloud computing. In 2017 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 2835-2838). IEEE.
2. Reddy, S. V., Rao, S. P., & Reddy, G. N. (2016). Enhanced data security in cloud computing using cryptography and steganography. In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 2782-2786). IEEE.
3. Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. Procedia Computer Science, 52, 775-784.
4. Goyal, V., Jindal, A., & Batra, A. (2016). Secure cloud storage using hybrid encryption technique. International Journal of Engineering Research and Applications, 6(12), 34-38.

5. Shuja, J., Mehmood, A., & Ahmed, J. (2019). Secure data transmission in cloud computing using cryptography and steganography. In Proceedings of the 4th International Conference on Computing, Communication and Automation (pp. 1-5). IEEE.

6. Prabha, S., & Rajesh, G. (2018). Secure data transmission and storage in cloud using AES and hybridcryptography. International Journal of Innovative Technology and Exploring Engineering, 8(6S), 718-722.

7. Sheena, V. V., & Sandhya, P. K. (2016). Enhancing security in cloud computing using steganography and cryptographic algorithms. International Journal of Science, Engineering and Technology Research, 5(3), 99-105.

8. Khokhar, S., Mehmood, A., & Qureshi, K. N. (2016). Secured data transmission in cloud computing using steganography. In 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI) (pp. 102-107). IEEE.

9. Singh, P., & Chana, I. (2017). Secure and efficient data storage in cloud computing using hybrid steganography. International Journal of Computer Applications, 176(3), 16-21.

[10] AL-Shaaby, Ahmed Ali, and Talal AlKharobi. "Cryptography and steganography: new approach." Transactions on Networks and communications 5.6 (2017): 25.

[11] Jan, Aiman, et al. "Double layer security using crypto-stego techniques: a comprehensive review." Health and Technology (2021): 1-23.