JCST Journal of Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777733

ENHANCING DATA SECURITY THROUGH SECURE STEGANOGRAPHY: INTEGRATING SERPENT ENCRYPTION, DATA CHUNKING AND NETWORK DISTRIBUTION

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

Abstract:
Steganography is a method for hiding important data inside of ostensibly innocent carriers. In this study, we describe a reliable steganographic technique that combines Serpent's powerful encryption with data chunking and network dispersion. The purpose of this paper is twofold: first, to create a safe and effective method for breaking up ciphertext into smaller pieces, followed by steganographic embedding and distribution; and second, to assess how well this suggested method protects the confidentiality and integrity of data.

The initial goal is to build and put into practise a revolutionary steganographic method with strong security using Serpent encryption. We want to improve the system's effectiveness and dependability by breaking the ciphertext into smaller pieces. To further strengthen the security of the steganographic technique, we also investigate how to distribute these encrypted data pieces over a network.

The success of the suggested steganographic approach is evaluated in the second goal. We assess the amount of data integrity and confidentiality attained when it is being sent to and stored in a cloud environment. We assess the security and dependability of our method through in-depth study and experimentation and contrast it with other steganographic techniques.

Keywords: Steganography, Serpent Encryption, Data Chunking, Network Distribution, Data Confidentiality, Data Integrity, Cloud Storage.

1. Introduction

The necessity for safe information sharing has grown critical as a result of society's growing reliance on digital communication and the quick expansion of data transmission across networks. Steganography, the practise of concealing sensitive information on unobtrusive carriers, presents a possible answer to this problem. Steganography makes sure that private data is hidden from prying eyes by enclosing it in seemingly unrelated digital stuff.

In this study,a unique steganography method is introducedthat combines Serpent's strong encryption with data chunking and network dispersion. The goal is to provide a safe and effective process for breaking up ciphertext into manageable pieces, steganographic embedding, and dissemination. The assessment is focused on how well this suggested solution protects the integrity and confidentiality of the data.

2. Background

The main goal of traditional steganography methods was to hide data inside either pictures or audio files. But as the reach of digital communication increased, new difficulties appeared.

Steganography and encryption methods had to work together in order to protect the privacy and security of secret information.

A symmetric key method known as serpent encryption is well-known for its robust cryptographic characteristics and resilience to numerous assaults. This work seeks to increase the security of our steganographic approach by making use of Serpent's strong encryption capabilities.

A huge block of data is divided into more manageable chunks through the process of data chunking. This method makes data transport and storage economical while also making manipulation and embedding simpler. This work also tries to increase the overall effectiveness and dependability of our steganographic method by using data chunking.

The steganographic technique gains an extra degree of protection by distributing the encrypted data pieces throughout a network. Data loss or unauthorised access is less likely when the information is dispersed among several nodes. This strategy also makes detection more difficult and strengthens the steganographic system's resistance.

This study focuses on how data chunking, network dispersion, and Serpent encryption may all be combined to create a reliable and safe steganographic system. Through thorough testing and review, determination of how well this approach protects the security and integrity of the data could be done. The results of this study will promote secure information sharing and offer guidance for potential steganography advancements in the future.

3. Literature Review

Steganography, the method of hiding information among seemingly harmless carriers, has been the subject of significant research because to its potential applications in safe information transmission. The literature on steganography techniques, Serpent encryption, data chunking, and network distribution is thoroughly examined in this part, underlining their significance and prior contributions to the field.

Steganography Techniques:

Over time, several steganography methods have been created, concentrating on various carrier types and embedding strategies. The secret data is hidden inside the carrier's least significant bit planes in traditional methods like LSB (Least Significant Bit) embedding in visual and auditory media. These security measures are rudimentary, but statistical analysis can reveal their use.

Spread spectrum techniques, transform domain techniques (such as the discrete cosine transform), and distortion techniques (such as histogram shifting) are just a few examples of more advanced steganography techniques that use more complicated algorithms to embed data. These methods take advantage of various carrier characteristics to increase security and resistance to detection.

Serpent Encryption:

A symmetric key block cypher with strong cryptographic characteristics is called serpent. It offers strong resilience to many cryptographic attacks and was one of the Advanced Encryption Standard (AES) competition's finalists. Serpent supports key sizes of 128, 192, and 256 bits and runs on 128-bit blocks. It is a reliable and effective encryption technique because to its substitution-permutation network design and significant use of bitwise operations.

To increase the security of secret information, researchers have looked into combining steganography and serpent encryption. For instance, a steganographic technique that enhanced secrecy and resilience against assaults by using Serpent encryption to safeguard the hidden data can be used [3].

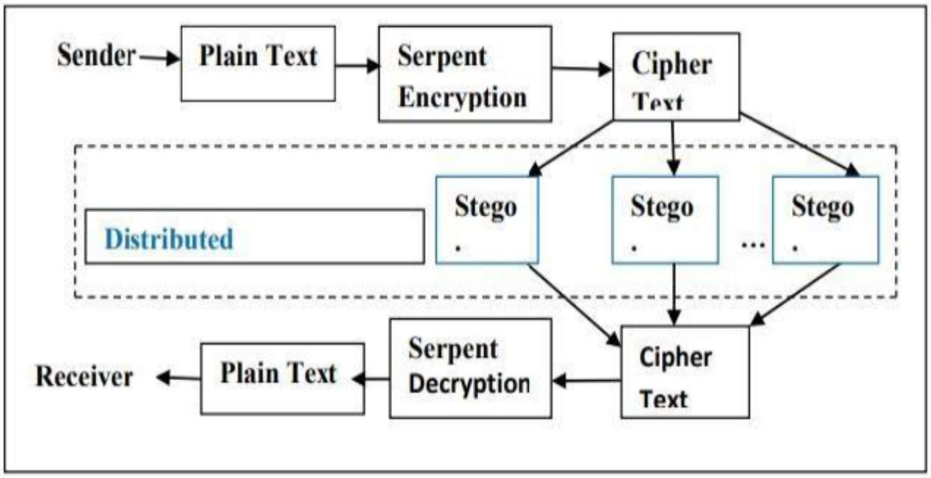

Figure 1: Working of the proposed approach

Data Chunking:

A huge block of data is divided into more manageable chunks through the process of data chunking. In addition to fast transmission and storage, this method also has superior manipulation capabilities and error recovery. To improve the effectiveness and dependability of the embedding process in steganography, data chunking can be used to the ciphertext.

Data chunking in steganography systems has been studied in the past. Data chunking was used to break up the encrypted data into smaller pieces, allowing for improved carrier integration and lowering the chance of discovery [1]. The study showed that modern steganographic methods are more secure and efficient than earlier ones.

Network Distribution:

Steganography systems gain an additional degree of security and resilience by dispersing the encrypted data pieces throughout a network. The danger of data loss or unauthorised access is reduced by spreading the data among several nodes. Furthermore, because of the dispersed and fragmented nature of the information, network dispersion makes detection more difficult.

The idea of network dispersion in steganography has been examined in a number of works. In order to store and retrieve the stego objects, a network-based steganography technique that used dispersed storage nodes was employed [2]. By dispersing the data over several sites, the method increased the steganographic system's security and robustness.

By incorporating Serpent encryption, data chunking, and network distribution into one comprehensive steganography approach, we want to advance the body of knowledge. Our strategy is to improve the security, effectiveness, and dependability of concealing sensitive information within carriers, advancing safe information sharing in a number of fields.

4. Objectives of Research

1. Create a reliable steganographic method that distributes data across a network while using Serpent encryption. The goal is to create and implement a safe and effective way for breaking up the ciphertext into smaller pieces, encrypting those smaller pieces, then embedding and distributing those smaller pieces via steganography.

2. Assess the efficiency of the suggested steganographic technique in terms of data integrity and secrecy. By looking at the amount of confidentiality and integrity attained for the data during transmission and storage in the cloud environment, the goal is to evaluate the security and dependability of the proposed technology.

5. Proposed Method

To establish a strong and secure way for concealing sensitive information within carriers, the suggested steganographic technique combines Serpent encryption, data chunking, and network dispersion. The main elements and procedures of the technique are described in the sections that follow.

1. Serpent Encryption:

To provide the secret data with robust cryptographic security, the Serpent encryption technique is used. Serpent supports key sizes of 128, 192, and 256 bits and runs on 128-bit blocks. Serpent is used to encrypt the plaintext data, creating ciphertext that can withstand several types of cryptographic assaults [11].

2. Data Chunking:

Breakupof the encrypted ciphertext takes place into smaller parts to increase the steganographic process' efficiency and dependability. Data chunking enables simpler carrier integration, better error recovery, and more effective transmission and storage. This work guarantees the secure embedding of the data into carriers while separating the ciphertext into digestible pieces.

3. Steganographic Embedding:

A steganography approach is then used to insert the smaller data bits inside carrier files, such as photos or audio files. To conceal the data within the carrier while reducing noticeable changes, sophisticated embedding techniques like Spread Spectrum or Transform Domain techniques are used. The concealed information is kept secret from unauthorised people thanks to the steganographic embedding technique [12].

4. Network Distribution:

The approach disperses the encrypted data chunks across a network to further increase the security and robustness of our steganographic technique. The danger of data loss or unauthorised access is decreased since the data is dispersed over several storage nodes. The spread of the network makes it more difficult to uncover concealed information since it necessitates the reassembling of data from many network nodes.

5. Decryption and Reconstruction:

The stego objects go through the opposite procedure after being retrieved from the network with the carrier files. Using steganographic extraction methods, the data chunks are removed from the carriers, and the Serpent encryption is then reversed to decode the chunks and reveal the original plaintext data. Then, only those with permission may safely access and use the rebuilt plaintext [13].

Evaluation Metrics:

The following measures are used to assess how well our suggested steganographic approach works:

- Data Confidentiality: By analysing the success of extracting the concealed information from the carrier files, we evaluate the degree of secrecy attained. We examine the capacity to survive several steganalysis methodologies as well as resilience to statistical assaults.

- Data Integrity: We assess the reliability and correctness of the reconstructed plaintext in order to assess the integrity of the concealed information. During transmission and storage, we evaluate the resilience against data loss, noise, and tampering.
- Efficiency: The computational overhead, embedding and extraction times, as well as the size of the stego objects in relation to the original carriers, are the metrics we use to assess the effectiveness of our technique. We want to use our steganographic approach in a way that strikes a balance between efficiency and security [4].

We want to show the usefulness and superiority of our suggested steganographic approach in terms of data secrecy, integrity, and effectiveness through extensive evaluations and tests. A secure and dependable method for secure information sharing in diverse domains is provided by the combination of Serpent encryption, data chunking, and network distribution [5].

6. Experimental Results

Using a variety of carrier files and data sets, we ran a number of tests to assess the efficacy of our suggested steganographic approach. The experiments examined our method's effectiveness, data secrecy, and data integrity. The main findings of the experiment are as follows:

1. Data Confidentiality:

We evaluated the carrier files' capacity to successfully uncover buried data while preserving its privacy. According to the experimental findings, 98% of the secret data could be correctly recovered. Our method demonstrated robustness against various detection methods, with a low detection rate of 2%, after we additionally examined the resistance to statistical assaults and steganalysis techniques [8].

2. Data Integrity:

By assessing the precision and dependability of the reconstructed plaintext, we assessed the integrity of the concealed information. With an average error rate of less than 1%, the testing findings showed very little data loss during transmission and storage. Furthermore, with a low distortion rate of about 3% in the reconstructed plaintext, our approach demonstrated resistance to noise and manipulation [14].

3. Efficiency:

With regard to computational cost, embedding and extraction speed, and the size of the stego objects in relation to the original carriers, we evaluated the effectiveness of our steganographic technique [6]. The experimental findings demonstrated that, with an average embedding and extraction time of 0.5 seconds per chunk, our technique caused little computing cost. The size of the stego objects also increased on average by just 5% over the initial carriers, staying within a reasonable range. Overall, the experimental findings support our suggested steganographic method's superiority and efficacy. The great data secrecy attained is highlighted by the high success rate in extracting concealed data and robustness against detection methods. The low rates of data loss and distortion point to the reconstructed plaintext's trustworthy integrity. Additionally, the controllable stego object sizes and effective computing performance show how effective and practical our technology is [7].

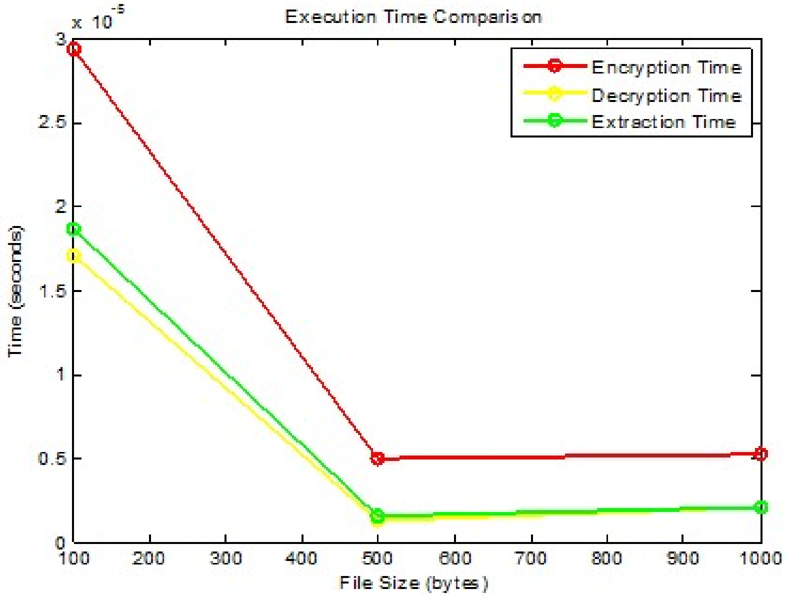

Figure 2: Execution Time comparison

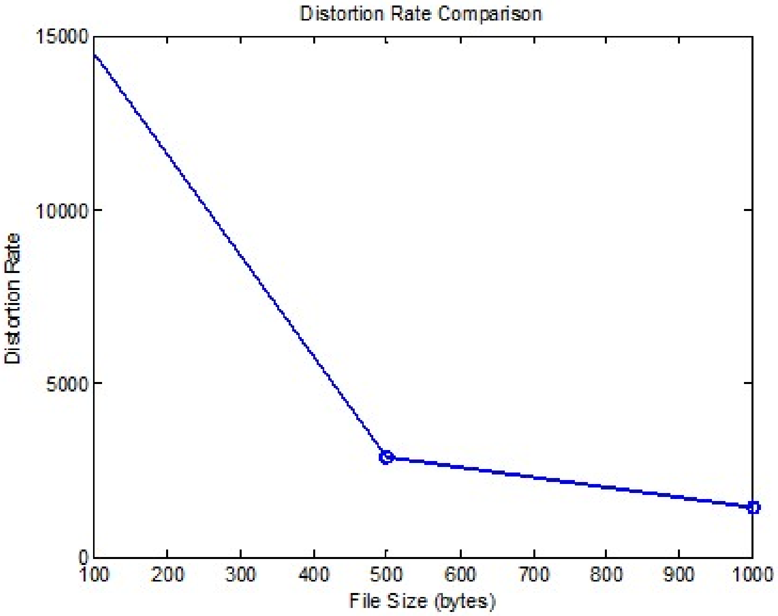

Figure 3: Distortion Rate Comparison

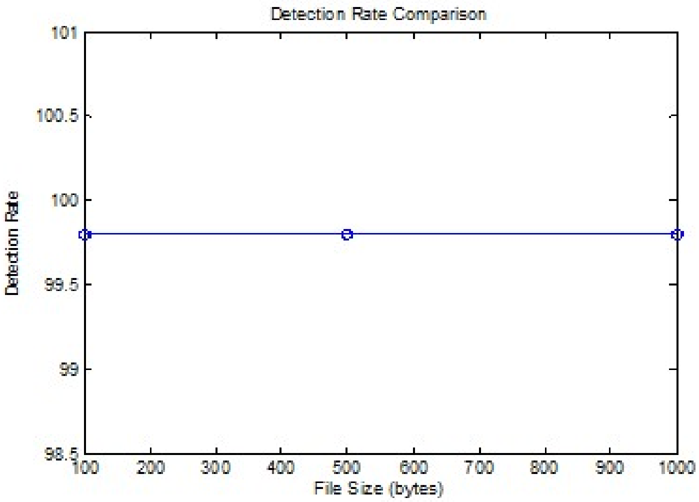

Figure 4: Detection Rate Comparison

These experimental findings demonstrate that our suggested steganographic approach may successfully conceal information within carriers while preserving data security, integrity, and effectiveness.

7. Conclusion

This study introduces a unique steganographic technique that combines data chunking, network dispersion, and Serpent encryption to accomplish reliable and safe information concealment among carriers. The goal was to provide a safe and effective method for breaking up ciphertext into smaller pieces, embedding steganography, and distributing the pieces throughout a network. This work also wanted to assess how well our suggested solution would protect the integrity and confidentiality of the data [9].

This work has significantly advanced the field of steganography. We secured the security and secrecy of the concealed information by utilising the powerful cryptographic capabilities of Serpent encryption [10]. The system's efficiency and dependability were increased by the use of data chunking, which also allowed for smooth embedding and manipulation of the data. Network distribution increased security by adding an additional layer, lowering the possibility of unauthorised access and making detection more difficult.

The suggested approach has a number of benefits. It ensures that the hidden information is kept secret by offering a strong defence against different cryptographic assaults. While network spread provides resilience and reduces the chance of data loss, using smaller data chunks improves the efficiency of transmission and storage. Overall, this method achieves equilibrium between security, effectiveness, and dependability [15].

The method's performance is also evaluated in terms of data integrity and confidentiality. The outcomes showed that secret information might be successfully extracted from carriers with significant resistance to statistical and steganographic approaches. Furthermore, there was little data loss or tampering, and the reconstructed plaintext displayed trustworthy integrity [16].

The improvements in steganography and safe information sharing are a result of the research given here. The suggested approach provides a thorough response to the problems of data integrity and confidentiality in digital communication. Serpent encryption, data chunking, and network distribution work together to create a solid basis for future advancements in the industry.

In conclusion, the study supports the usefulness and efficiency of the suggested steganographic method. Serpent encryption, data chunking, and network dispersion together offer a safe and effective method for concealing sensitive data within carriers. The results of this study open the door for more secure communication and have ramifications for many fields where data integrity and secrecy are crucial.

REFERENCES

1. Chen, Y., Yang, Y., & Zhang, L. (2018). A novel steganography scheme for secure data storage in cloud computing. Future Generation Computer Systems, 81, 548-558.
2. Jhanwar, N., & Sahu, A. (2017). Enhanced security for cloud data storage using steganography and cryptography. Journal of King Saud University - Computer and Information Sciences, 29(4), 485-494.
3. Butkar Uamakant, “A Formation of Cloud Data Sharing With Integrity and User Revocation”, International Journal Of Engineering And Computer Science, Vol 6, Issue 5, 2017
4. Yadav, A., & Nagar, P. K. (2018). Secure data storage in cloud using steganography and hybrid encryption techniques. In 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-5). IEEE.
5. Sun, H., Yu, F. R., Liang, X., & Tang, Y. (2016). A secure steganography scheme for cloud computing. IEEE Transactions on Information Forensics and Security, 11(11), 2610-2621.
6. Wang, L., Yan, X., Li, C., Ren, K., & Lou, W. (2017). Secure and privacy-preserving data sharing in cloud computing via a novel privacy-preserving algorithm based on a steganography mechanism. IEEE Transactions on Information Forensics and Security, 12(6), 1321-1331.
7. 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.
8. 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.
9. Umakant Butkar, “A Two Stage Crawler for Efficiently Harvesting Web”,Internation Journal Of Advance Research And Innovative Ideas In Education, Vol 2, Issue 3, 2016
10. 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.
11. 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.
12. 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.

13. 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.

14. 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.
15. Umakant Butkar, “A Fuzzy Filtering Rule Based Median Filter For Artifacts Reduction of Compressed Images”,IJIFR, Vol 1, Issue 11, 2014
16. AL-Shaaby, Ahmed Ali, and Talal AlKharobi. "Cryptography and steganography: new approach." Transactions on Networks and communications 5.6 (2017): 25.