RESEARCH ARTICLE OPEN ACCESS

A Multi-Layer Network Steganography Framework Using ICMP and NTFS Alternative Data Streams for Secure Covert Communication

Salam Ghanim Najeeb[1], Noor Alhuda fadhil[2]
1(Department of Medical Laboratories College of Health and Medical Techniques, Sawa University, Almuthana, Iraq.
Email: salam@sawauniversity.edu.iq)
2 (Department of computer science, University of technology, Iraq.
Email: cs.22.17@grad.uotechnology.edu.iq)

Abstract:

With the rapid expansion of digital communication networks, protecting sensitive information against interception, traffic analysis, and cyber surveillance has become increasingly challenging. While cryptography secures the content of messages, it does not hide the existence of communication, making encrypted traffic vulnerable to detection and blocking. Network steganography addresses this limitation by embedding secret data into legitimate network traffic using covert channels. However, most existing network steganography techniques rely on single layer hiding mechanisms, which suffer from limited bandwidth, low robustness, and high detectability under modern intrusion detection systems.

This paper proposes a multi-layer network steganography framework that integrates ICMP-based covert channels with NTFS Alternative Data Streams (ADS) to significantly enhance capacity, security, and stealth. The proposed approach hides secret files and messages inside ADS at the file-system level and then encapsulates the ADS-based payload within ICMP packets at the network level, forming a hierarchical covert communication architecture. This layered model is inspired by multi-layer steganography principles and onion-routing-style security, where each layer provides an additional level of protection.

Experimental analysis demonstrates that the proposed multi-layer framework achieves higher hidden data capacity and stronger resistance to detection compared to conventional ICMP-based covert channels, while maintaining normal network behavior. The results confirm that combining file-system-level and network-level steganography offers a powerful mechanism for secure covert communication in modern networks.

Keywords — **Network steganography, covert channels, ICMP, NTFS Alternative Data Streams, multi-layer security, information hiding.**

I. INTRODUCTION

The exponential growth of Internet-based services has transformed modern society, enabling fast and ubiquitous communication between users, organizations, and governments. However, this same infrastructure has also become a target for surveillance, cyber espionage, and unauthorized data interception. Traditional security mechanisms such as encryption focus primarily on protecting the content of communication, but they do not conceal the existence of the communication itself. Encrypted traffic can easily be identified, monitored, blocked, or flagged for further investigation by network security systems. Steganography provides a complementary security mechanism by hiding secret messages inside innocuous carriers, making the communication appear ordinary and thus avoiding suspicion. In digital environments, steganography can be applied to multimedia files such as images, audio, and video[1-3], or to structured carriers such as file systems and network protocols. Network steganography exploits the flexibility, redundancy, and ambiguity of network protocols to create covert channels that can transmit hidden data without being detected by conventional monitoring tools. Despite its potential, most network steganography techniques rely on single-layer covert channels, where hidden data is embedded directly into a single protocol field,

packet sequence, or timing behaviour. Such approaches suffer from several limitations. First, the available bandwidth is often very small, as only a few bits can be safely hidden per packet without causing anomalies. Second, single-layer methods are fragile against traffic normalization, packet loss, and protocol validation. Third[4-7], modern intrusion detection systems (IDS) and network traffic analyzers can increasingly identify statistical deviations introduced by single-layer covert channels.

In contrast, multi-layer steganography has been shown in multimedia domains to significantly improve capacity and robustness by distributing hidden data across multiple embedding layers. Inspired by this concept, this paper extends the idea of multi-layer steganography to the network domain by integrating ICMP covert channels with NTFS Alternative Data Streams (ADS). ADS is a feature of the NTFS file system that allows files to contain multiple hidden data streams without altering their apparent size or behaviour, making it a powerful file-system-level steganographic carrier. By combining file-system-level hiding (ADS) with network-level hiding (ICMP), we create a two-layer covert communication framework that significantly enhances the secrecy, capacity, and resilience of hidden communications. This approach not only increases the amount of data that can be transmitted covertly but also makes detection far more difficult, as an adversary would need to identify and break multiple independent hiding layers.

The main contributions of this paper are:

1. A novel multi-layer network steganography framework combining ICMP covert channels and NTFS ADS.
2. A mathematical model for analyzing the capacity and security gain of multi-layer network hiding.
3. An experimental implementation demonstrating covert communication using ADS-embedded files transmitted via ICMP.
4. A comparative analysis showing the advantages of the proposed method over traditional single-layer network steganography.

II. RELATED WORK

Network steganography has attracted increasing attention as a technique for establishing covert communications over public and private networks. Numerous researchers have proposed methods to exploit unused, optional, or flexible fields in network protocols to hide secret information. These methods can be broadly categorized into storage-based covert channels, timing-based covert channels, and hybrid approaches.

Early work on covert channels focused on exploiting protocol header fields such as the IP identification field, TCP sequence numbers, and unused flags. These fields can be manipulated to encode bits of hidden data while still producing syntactically valid packets. Other approaches hide data by altering packet ordering, retransmission patterns, or inter-packet delays. Although such methods are relatively easy to implement, they typically offer very low bandwidth and are vulnerable to traffic normalization and active wardens[5-12].

ICMP-based covert channels are particularly attractive because ICMP packets, such as Echo Request and Echo Reply messages, are widely used for network diagnostics and are often allowed through firewalls. Several studies have demonstrated that the data field of ICMP packets can be used to carry hidden messages, as long as the payload conforms to expected formats and sizes. However, ICMP covert channels are still limited by payload size and are susceptible to detection through deep packet inspection and anomaly detection. Another line of research has explored covert channels in file systems, especially within NTFS. Alternative Data Streams (ADS) allow files to contain multiple hidden streams that are not visible in standard directory listings or file size reports. ADS has been used for both benign and malicious purposes, including hiding malware, embedding secret data, and bypassing forensic tools. Because ADS operates at the file-system level, it provides a powerful and stealthy storage mechanism for hidden information.

More recently, researchers have proposed combining cryptography and steganography to

improve security, as well as developing adaptive covert channels that adjust their behaviour based on network conditions. However, most existing approaches still rely on a single embedding layer, either at the network or file system level.

The idea of multi-layer steganography, widely studied in image and multimedia domains, suggests that distributing hidden data across multiple layers can significantly improve capacity and security. Yet, this principle has rarely been applied systematically to network steganography. This paper addresses this gap by proposing a multi-layer network steganography model that integrates ICMP covert channels with NTFS ADS.

III. THEORETICAL BACKGROUND

A. Network Steganography and Covert Channels

Network steganography is a branch of information hiding that exploits the properties of network protocols to transmit secret information in a way that is invisible to third parties. Unlike cryptography, which only protects the content of a message, network steganography hides the very existence of the communication. This is achieved through covert channels, which are communication paths not originally intended for information transfer but that can be manipulated to carry data secretly[4, 10, 13-17].

A covert channel can be defined as any communication channel that allows information transfer in a manner that violates the security policy of a system. In network environments, covert channels can be created by modifying protocol headers, packet payloads, packet timing, packet ordering, or protocol state transitions. Such channels are often classified into storage-based covert channels, where bits are stored in packet fields, and timing-based covert channels, where information is encoded in the timing or sequencing of packets[18-24].

ICMP (Internet Control Message Protocol) is particularly suitable for storage-based covert channels because its Echo Request and Echo Reply messages contain data fields that are typically ignored by network devices. This flexibility allows attackers or covert communicators to embed hidden information inside ICMP payloads without affecting normal network operations[10, 16, 17].

B. NTFS Alternative Data Streams

NTFS Alternative Data Streams (ADS) are a feature of the Windows NTFS file system that allows a single file to contain multiple data streams. Each file has a primary data stream that is visible to the user, but it can also contain one or more hidden streams that do not affect the file's size or appearance. These hidden streams can store arbitrary data such as text, images, executables, or encrypted payloads.

From a steganographic perspective, ADS provides an extremely powerful hiding mechanism because standard file management tools do not reveal the existence of hidden streams. Furthermore, ADS can store large amounts of data without modifying the observable characteristics of the carrier file, making it highly suitable for covert storage and transmission.

C. Multi-Layer Steganography Principle

Multi-layer steganography extends the idea of hiding information by embedding secret data across multiple independent layers. In traditional single-layer steganography, a message is hidden directly into one carrier[1-3, 5, 13, 25-30]. In contrast, multi-layer steganography embeds a hidden object into another hidden object, creating a hierarchy of concealment.

This principle is analogous to onion routing in secure communications, where each layer of encryption and encapsulation adds a new level of protection. The same idea can be applied to steganography: by hiding data within ADS and then hiding ADS within ICMP traffic, two independent hiding layers are created. An attacker must detect and extract both layers in order to recover the secret data, dramatically increasing security[31].

IV. PROPOSED MULTI-LAYER ETWORK STEGANOGRAPHY FRAMEWORK

A. System Architecture

The proposed framework consists of two main layers:

- Layer 1 (File-System Layer): Secret data is embedded into NTFS Alternative Data Streams attached to legitimate carrier files.
- Layer 2 (Network Layer): The ADS-based payload is encapsulated and transmitted inside ICMP packets across the network.

The overall communication process is illustrated as follows:

Secret File → ADS Embedding → Carrier File → ICMP Encapsulation → Network Transmission → ICMP DE capsulation → ADS Extraction → Secret Recovery

This architecture ensures that even if ICMP packets are inspected, the embedded ADS payload remains hidden as a normal data stream.

B. Embedding Process

1. The sender selects a legitimate NTFS file as the carrier.
2. The secret message or file is embedded into an ADS attached to the carrier file.
3. The carrier file containing ADS is fragmented and encoded into ICMP payloads.
4. ICMP Echo Request packets are sent to the receiver containing the ADS fragments.
5. The receiver reconstructs the ADS and extracts the hidden data.

C. Extraction Process

The receiver monitors incoming ICMP packets and extracts the payload data. Once all fragments are received, the ADS stream is reconstructed and attached to a carrier file. The hidden data is then extracted from the ADS using standard NTFS commands or custom scripts.

V. MATHEMATICAL MODEL

Let:

- M= number of ICMP packets
- b= bits of payload per ICMP packet
- a= ADS encoding efficiency
- k= number of steganographic layers

Single-layer capacity

$$C' = M \times b$$

Multi-layer capacity

$$C = M \times b \times a^k$$

Capacity gain

$$K = \frac{C - C'}{C'} \times 100$$

As $k$increases, the hidden data capacity increases exponentially while preserving stealth.

VI. EXPERIMENTAL SETUP

The experimental platform was implemented on Windows systems using NTFS. ADS were created using command-line and scripting tools. ICMP packets were generated using custom programs to encapsulate ADS data. Network traffic was monitored using Wireshark and Windump to ensure that the packets appeared normal.

Two scenarios were tested:

1. ICMP-based covert channel only (single-layer).
2. ICMP + ADS multi-layer covert channel.

VII. RESULTS AND ANALYSIS

The experimental evaluation clearly demonstrates that the proposed multi-layer steganography framework (ADS + ICMP) achieves significantly higher data capacity and lower detectability compared to a traditional single-layer ICMP covert channel. In the single-layer approach, the ICMP payload is directly used to transmit the secret data, which inevitably increases the statistical irregularities of packet contents and makes the covert channel more vulnerable to detection by traffic analysis tools. In contrast, in the proposed framework, ICMP packets only carry fragments of ADS-encoded data, which appear as ordinary binary payloads and therefore do not introduce abnormal traffic patterns.

From a traffic analysis perspective, commonly used network monitoring tools such as Wireshark and packet analysers were unable to differentiate the multi-layer covert traffic from legitimate ICMP echo requests and replies. Packet size distributions, transmission intervals, and protocol behaviour remained consistent with normal diagnostic traffic, indicating that the ADS encapsulation effectively masks the hidden communication. This demonstrates that the proposed framework significantly reduces the statistical footprint of the

covert channel, making it far more resistant to detection through deep packet inspection or anomaly-based intrusion detection systems.

Furthermore, the system exhibited strong robustness against packet loss and network noise. In traditional ICMP covert channels, even a small number of lost or reordered packets can corrupt the hidden message and prevent successful reconstruction. However, because the secret data in the proposed framework is first stored in ADS and then transmitted in fragments, the receiver can reassemble the ADS stream even when some ICMP packets are missing. This allows partial retransmission and error tolerance without compromising the entire hidden file.

Experimental results confirmed that hidden files of various types (text, images, and executables) were successfully reconstructed in full at the receiver side, even under conditions of moderate packet loss and variable network delay. This demonstrates that the multi-layer architecture provides not only enhanced stealth but also improved reliability, making it suitable for real-world network environments where packet loss and traffic fluctuations are unavoidable.

VIII. CONCLUSION

This paper presented a multi-layer network steganography framework that integrates NTFS Alternative Data Streams (ADS) with ICMP-based covert channels to provide a secure, high-capacity, and stealthy method for hidden communication. By combining file-system-level hiding and network-level hiding, the proposed architecture introduces two independent layers of protection, making detection, extraction, and forensic reconstruction significantly more difficult than in traditional single-layer covert channels. Even if one layer is compromised, the second layer continues to conceal the hidden information, reflecting a defense-in-depth and onion-style security architecture.

The proposed model demonstrated superior performance in terms of capacity, robustness, and resistance to detection. ADS allows large volumes of data to be hidden without altering the observable properties of files, while ICMP provides a legitimate and widely accepted transport mechanism that blends naturally into network traffic. This dual-layer strategy reduces the statistical footprint of the covert channel, increases resilience against packet loss and traffic normalization, and enhances the overall stealth of the communication. As a result, the framework is well suited for applications in secure communications, cyber defense, covert data exchange, and digital forensics research.

Future extensions of this work will focus on expanding the multi-layer framework to additional network protocols such as TCP, DNS, and HTTPS, enabling covert communication over encrypted and high-volume application traffic. Furthermore, integrating cryptographic protection within the ADS layer will provide confidentiality and integrity even in the event of partial exposure. Additional research will also explore adaptive and intelligent embedding strategies, using machine learning to dynamically optimize protocol selection and embedding behavior, further strengthening resistance against advanced network steganalysis techniques.

REFERENCES

1. Utama, S., et al., *Analytical and Empirical Insights into Wireless Sensor Network Longevity: The Role MAC Protocols and Adaptive Strategies.* Journal of Advanced Research in Computing and Applications, 2024. **36**(1): p. 52-60.
2. Qasim Almaliki, A.J., et al., *Application of the Canny Filter in Digital Steganography.* Journal of Advanced Research in Computing and Applications, 2024. **35**(1): p. 21-30.
3. Din, R., et al., *Exploring Steganographic Techniques for Enhanced Data Protection in Digital Files.* International Journal of Advanced Research in Computational Thinking and Data Science, 2024. **1**(1): p. 1-9.
4. Qasim, A.J., R. Din, and F.Q.A. Alyousuf, *Review on techniques and file formats of image compression.* Bulletin of Electrical Engineering and Informatics, 2020. **9**(2): p. 602-610.
5. Alyousuf, F.Q.A., R. Din, and A.J. Qasim, *Analysis review on spatial and transform domain technique in digital steganography.* Bulletin of Electrical Engineering and Informatics, 2020. **9**(2): p. 573-581.
6. Al-Yousuf, F.Q.A., R.J.I.J.o.E.E. Din, and C. Science, *Review on secured data capabilities of cryptography, steganography, and watermarking domain.* 2020. **17**(2): p. 1053-1059.
7. Tao, J., et al., *Towards robust image steganography.* IEEE Transactions on Circuits and Systems for Video Technology, 2019. **29**(2): p. 594-600.
8. Din, R., A.J.J.B.o.E.E. Qasim, and Informatics, *Steganography analysis techniques applied to audio and image files.* 2019. **8**(4): p. 1297–1302.
9. Din, R., et al., *Review on steganography methods in multi-media domain.* 2019. **8**(1.7): p. 288-292.
10. Roshidi Din, O.G., Alaa Jabbar Qasim, *Analytical Review on Graphical Formats Used in Image Steganographic Compression.* Indonesian Journal of Electrical Engineering and Computer Science, 2018. **Vol 12, No 2**: p. pp. 441~446.
11. Poljicak, A., et al., *Portable real-time DCT-based steganography using OpenCL.* Journal of Real-Time Image Processing, 2018. **14**(1): p. 87-99.
12. Hussain, M., et al., *Image steganography in spatial domain: A survey.* Signal Processing: Image Communication, 2018. **65**: p. 46-66.
13. Alaa Jabbar, Q., D. Roshidi, and A. Farah Qasim Ahmed, *Extended Method of Least Significant Bits on Colour Images in Steganography.* QALAAI ZANIST SCIENTIFIC JOURNAL, 2024. **9**(3): p. 1146-1158.

14. Alaa Jabbar, Q. and A. Farah Qasim Ahmed, *History of Image Digital Formats Using in Information Technology.* QALAAI ZANIST SCIENTIFIC JOURNAL, 2021. **6**(2): p. 1098-1112.
15. Qasim, A.J., et al., *Review on techniques and file formats of image compression.* 2020. **9**(2): p. 602–610.
16. Altaay, A.A.J., S.B. Sahib, and M. Zamani. *An introduction to image steganography techniques*. in *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*. 2012. IEEE.
17. Qasim, A.J. and R. Din, *Capacity Performance of LSB Method On Multi-Layer Images in Steganography.*
18. Sai Virali Tummala, V.M., *Comparison of Image Compression and Enhancement Techniques for Image Quality in Medical Images.* 2017.
19. Sedighi, V., R. Cogranne, and J. Fridrich, *Content-adaptive steganography by minimizing statistical detectability.* IEEE Transactions on Information Forensics and Security, 2016. **11**(2): p. 221-234.
20. Swetha, V., V. Prajith, and V. Kshema, *Data Hiding Using Video Steganography-A Survey.* International Journal of Science, Engineering and Computer Technology, 2015. **5**(6): p. 206.
21. Sidhik, S., S. Sudheer, and V.M. Pillai, *Performance and analysis of high capacity steganography of color images involving wavelet transform.* Optik, 2015. **126**(23): p. 3755-3760.
22. QASSIM, A.J. and Y. SUDHAKAR, *Information Security with Image through Reversible Room by using Advanced Encryption Standard and Least Significant Bit Algorithm.* 2015.
23. Nasreen, S.M., G. Jalewal, and S. Sutradhar, *A Study on Video Steganographic Techniques.* Internatinal Journal of Computational Engineering Research, 2015. **5**(10).
24. Samagh, R. and S. Rani, *Data Hiding using Image Steganography.* 2015.
25. Rani, N. and J. Chaudhary, *Text steganography techniques: A review.* International Journal of Engineering Trends and Technology (IJETT), 2013. **4**(7): p. 3013-3015.
26. Qian, Z., X. Han, and X. Zhang. *Separable reversible data hiding in encrypted images by n-nary histogram modification*. in *International Conference on Multimedia Technology (ICMT 2013), Guangzhou*. 2013.
27. Preeti Hooda , K.R., *Steganography in Multiple Data: Review.* International Journal of Latest Trends in Engineering and Technology (IJLTET), 2013.
28. Patel, K., S. Utareja, and H. Gupta, *Information hiding using least significant bit steganography and blowfish algorithm.* International Journal of Computer Applications, 2013. **63**(13).
29. Neufeld, A. and A.D. Ker. *A study of embedding operations and locations for steganography in H. 264 video*. in *IS&T/SPIE Electronic Imaging*. 2013. International Society for Optics and Photonics.
30. Mulla, A., N. Gunjikar, and R. Naik, *Comparison of Different Image Compression Techniques.* International Journal of Computer Applications, 2013. **70**(28).
31. Sunariya Utama Alaa Jabbar Qasim Almaliki, O.G., Roshidi Din, *Comparative Analysis of LSB, PVD, and EMD-Based Stenographic Methods with Hybrid Optimization in Digital Images.* International Journal of Engineering and Techniques, 2025. **11**: p. 351-357.
32. Satyavathy, G. and M. Punithavalli, *LSB, 3D-DCT and Huffman Encoding based Steganography in Safe Message Routing and Delivery for Structured Peer-to-Peer Systems.* IJCA Special Issue on Artificial Intelligence Techniques, 2011: p. 1-5.
33. Raval, M., et al., *Image Tampering Detection Using Compressive Sensing Based Watermarking Scheme.* Proceedings of MVIP 2011, 2011.
34. Sharma, M., *Compression using Huffman coding.* IJCSNS International Journal of Computer Science and Network Security, 2010. **10**(5): p. 133-141.
35. Kumar, K.S., et al. *Coherent steganography using Segmentation and DCT*. in *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*. 2010. IEEE.