Indian Engineering Journal
ISSN: 2984-9047
Vol 4 Issue 2 (2026)

Adaptive Multi-Stream Steganographic Intelligence Integration via Aggregated Filter Ensembles and Autonomous Deployment (AMSI-AFEAD)

S. Pradeep[1]*, A. Geetha[2]

[1]Research Scholar, Department of Computer Science, Chikkanna Govt. Arts College, Tiruppur, (Affiliated to Bharathiar University) Coimbatore, Tamil Nadu, India.

[2]Associate Professor, Department of Computer Science, Government Arts College, Avinachi, (Affiliated to Bharathiar University) Coimbatore, Tamil Nadu, India.

Abstract:

Steganographic systems must now confront deep-learning steganalyzers that routinely break single-carrier schemes. This paper proposes the Adaptive Multi-Stream Steganographic Intelligence Integration via Aggregated Filter Ensembles and Autonomous Deployment (AMSI-AFEAD) framework. AMSI-AFEAD conceals intelligence data across multiple parallel cover images, assigning a heterogeneous set of spatial-frequency filters (Gabor, steerable Gaussian, and a light learned convolutional filter) to distinct streams. An autonomous deployment module monitors channel health (latency, packet loss, estimated adversarial presence) and dynamically redistributes payload fragments to keep per-stream detectability below a predefined threshold. The system also enforces a multi-objective policy that guarantees graceful degradation if up to half the streams are intercepted. Experiments on the BOSSBase-1.01 and BOWS-2 collections show that AMSI-AFEAD raises the detection error rate by up to 14 percentage points against SRNet and Xu-Net compared with the most secure single-stream adaptive method, while achieving a Multi-Stream Imperceptibility Gain of 3.5 dB and an Adaptive Security Index of 0.93. These results confirm that heterogeneous filter ensembles combined with autonomous payload routing offer a practical pathway to next-generation covert communications.

Keywords: multi-stream steganography, aggregated filter ensembles, autonomous deployment, covert channel resilience, adaptive payload distribution, deep steganalysis evasion

1. Introduction

Modern steganography is locked in a continuous race with convolutional neural network-based steganalyzers that can spot statistical artefacts undetectable to classical detectors (Patel & Mehta, 2023). Single-carrier methods, even when they adapt pixel-level distortion costs using the most sophisticated rules, fail to keep detection error above 20 % once the payload reaches 0.3 bits per pixel on standard testbeds. This limitation stems from two factors: (i) a static embedding policy that a single deep steganalyzer can eventually memorise, and (ii) the inability to react to fluctuating channel conditions in real-world covert operations (Kim et al., 2024). Intelligence agencies and secure-communication architectures therefore need frameworks that can spread a secret across multiple carriers, making the adversary's task combinatorial while autonomously moving payload away from streams that show signs of interception.

Multi-image steganography is a natural countermeasure. Splitting a payload across several cover images lowers the per-stream embedding rate, potentially driving it below the steganalyzer's reliable detection horizon. However, existing multi-stream solutions reuse the same embedding algorithm for every cover object, leaving inter-image statistical consistencies that ensemble steganalyzers can capture (Liu et al., 2023). They also rely on a fixed, operator-configured payload split that cannot adapt when a stream encounters congestion or adversarial scanning.

The AMSI-AFEAD framework tackles both shortcomings by introducing three tightly coupled innovations:

1. Heterogeneous aggregated filter ensemble – each stream gets a different filter bank (Gabor, steerable Gaussian, or a compact learned CNN) so that the embedding artefacts are statistically uncorrelated across streams.

2. Autonomous deployment controller – a lightweight module that senses real-time channel quality and re-allocates payload using a softmax over quality scores, shifting data away from degraded or suspect channels.

3. Multi-objective optimisation layer – guarantees that even if an adversary intercepts half the streams, the leaked portion of the message remains incomplete and operationally useless.

The remainder of the paper is structured as follows. Section 2 reviews recent work on deep-learning steganography, multi-stream embedding, and autonomous covert channels. Section 3 identifies research gaps and formulates the problem. Section 4 describes the proposed methodology and architecture. Section 5 presents the experimental setup, benchmark datasets, existing and novel evaluation metrics, and results. Section 6 discusses implications, limitations, and avenues for future work. Section 7 concludes the paper.

2. Literature Review

2.1 Deep-Learning-Driven Steganography

Since the demonstration of HiDDeN (Zhu et al., 2020), end-to-end deep-learning pipelines have attracted significant attention. Zhu et al. (2020) trained an encoder-decoder pair jointly with a discriminator, achieving high capacity but moderate robustness against steganalysis. Nguyen et al. (2019) used a generative adversarial network (GAN) to learn adaptive embedding strengths, concentrating modifications in salient image regions where human vision is less sensitive. Building on this, Wang et al. (2021) proposed cost-learning driven by reinforcement signals; their agent adjusts embedding costs according to a delayed reward computed from a steganalyzer, boosting undetectability by about 7 % over conventional hand-crafted costs. These works, however, operate on a single cover image and do not address the multi-stream scenario.

2.2 Multi-Stream and Ensemble Steganography

Motivated by the single-stream ceiling, several teams have explored payload distribution over multiple images. Liu et al. (2023) formulated a graph-based multi-image steganography scheme that selects cover images based on texture similarity and assigns payload proportional to each image's "security capacity." Their approach increased the total secure payload by 12 % compared with uniform allocation, but it used identical S-UNIWARD embedding across all streams, leaving cross-stream correlations. Huang et al. (2020) introduced a heterogeneous filter bank for JPEG steganography, showing that mixing DCT- and wavelet-domain filters improves resistance to ensemble steganalysis. Yet, their design was limited to a single image; no parallel-stream architecture was developed.

2.3 Filter-Based and Learned-Filter Embedding

Traditional Gabor and steerable filters remain competitive because they mimic the multi-scale texture selectivity of the human visual system. Chen and Zhao (2022) proposed an ensemble of diverse residual filters for adversarial steganography, demonstrating that combining high-pass, band-pass, and learned kernels increases detection error by 5–8 % against SRNet. In the learned filter domain, Ahmed et al. (2021) embedded secret bits using a small CNN that jointly optimises a pre-filter and a post-embedding distortion minimiser; the resulting cost maps outperform traditional WOW costs. These studies confirm that filter diversity within a single carrier helps, yet none have extended the concept to heterogeneous assignment across multiple independent streams.

2.4 Autonomous Deployment and Adaptive Covert Channels

The need for autonomous adaptation is gaining recognition. Kim et al. (2024) introduced a deep Q-network that decides when to inject covert bits into IoT sensor streams based on traffic similarity, reducing detection by a statistical analyser by 18 %. Singh and Kaur (2022) proposed a fuzzy-logic controller that adjusts steganographic payload according to estimated channel bandwidth and loss rate. Although these works address adaptation to channel conditions, they do not coordinate multiple parallel carriers; their decision unit controls a single stream, missing the opportunity to reroute data across alternative carriers when one channel becomes risky.

2.5 Summary of Recent Trends

The literature shows a clear movement toward learning-based cost functions, multi-image payload allocation, and channel-aware adaptation. However, no published framework integrates heterogeneous filter ensembles across multiple streams with fully autonomous payload relocation. This gap leaves operational multi-stream steganography vulnerable to both statistical correlation exploitation and rigid deployment schedules.

3. Research Gap Identification

Heterogeneity deficit: Multi-stream steganography still applies the same embedding algorithm to all covers (Liu et al., 2023; Huang et al., 2020). Inter-stream statistical fingerprints remain exploitable.

Reactive adaptation absence: Payload splits are static. No work dynamically re-allocates fragments in response to live channel quality metrics without requiring a full steganalysis oracle.

Filter ensemble isolation: Works such as Chen and Zhao (2022) demonstrate the advantage of diverse filters within one image, but they have not been deployed across multiple parallel carriers in a coordinated fashion.

Lack of system-level multi-objective guarantees: Existing methods maximise either capacity or undetectability on a per-stream basis, ignoring combined security requirements under partial interception.

Missing multi-stream evaluation metrics: Standard metrics (PSNR, detection error) are defined for single streams. No metric quantifies the security gain obtained specifically from multi-stream dispersal or from adaptive stream selection.

4. Problem Statement

Let $C = \{C_1, C_2, \ldots, C_K\}$ be a set of K cover images, and let M be a secret payload partitioned into K fragments $m_1, \ldots, m_K$. Existing multi-stream steganography applies the same embedding function E_θ to all streams, producing stego images $S_1, \ldots, S_K$ with correlated statistical signatures.

A fixed allocation α_i = constant ignores real-time channel quality Q_i. The problem is to design a framework F= (E, A, O) where:

- $E= \{E_{\theta_1}, \ldots, E_{\theta K}\}$ is a set of heterogeneous embedding filters,

- $A(Q_1, \ldots, Q_K) \rightarrow (\alpha_1, \ldots, \alpha_K)$ is an autonomous allocation policy, and

- O is a multi-objective optimisation that maximises total payload capacity, minimises the probability that any single stream is detected, and enforces a graceful-degradation constraint if up to $\lfloor K/2 \rfloor$ streams are intercepted.

5. Objectives of the Proposed Method

1. Heterogeneous filter ensemble design – Assign a distinct filter type (Gabor, steerable Gaussian, learned CNN) to each stream, eliminating cross-stream correlation exploitable by ensemble steganalysis.

2. Autonomous payload allocation engine – Build a controller that senses channel quality (bandwidth, packet loss, adversarial presence likelihood) and dynamically redistributes payload fragments to keep per-stream detection error below 50 %.

3. Multi-objective security-capacity optimisation – Formulate and solve a constrained optimisation that maximises throughput while guaranteeing that no subset of $\lfloor K/2 \rfloor$ streams leaks enough data to reconstruct the message.

6. Proposed Methodology

6.1 System Architecture

The System Depicts the full AMSI-AFEAD architecture, organised as four sequential processing stages: preprocessing, the aggregated filter ensemble embedding engine, the autonomous deployment controller, and the multi-objective optimisation layer. Cover images enter in parallel and each is routed through a distinct filter type (Gabor, steerable Gaussian, learned CNN, or hybrid), ensuring that no two streams carry correlated embedding artefacts. The controller continuously monitors channel conditions and feeds dynamically adjusted payload fractions to the optimisation layer, which enforces the graceful-degradation constraint against partial interception.

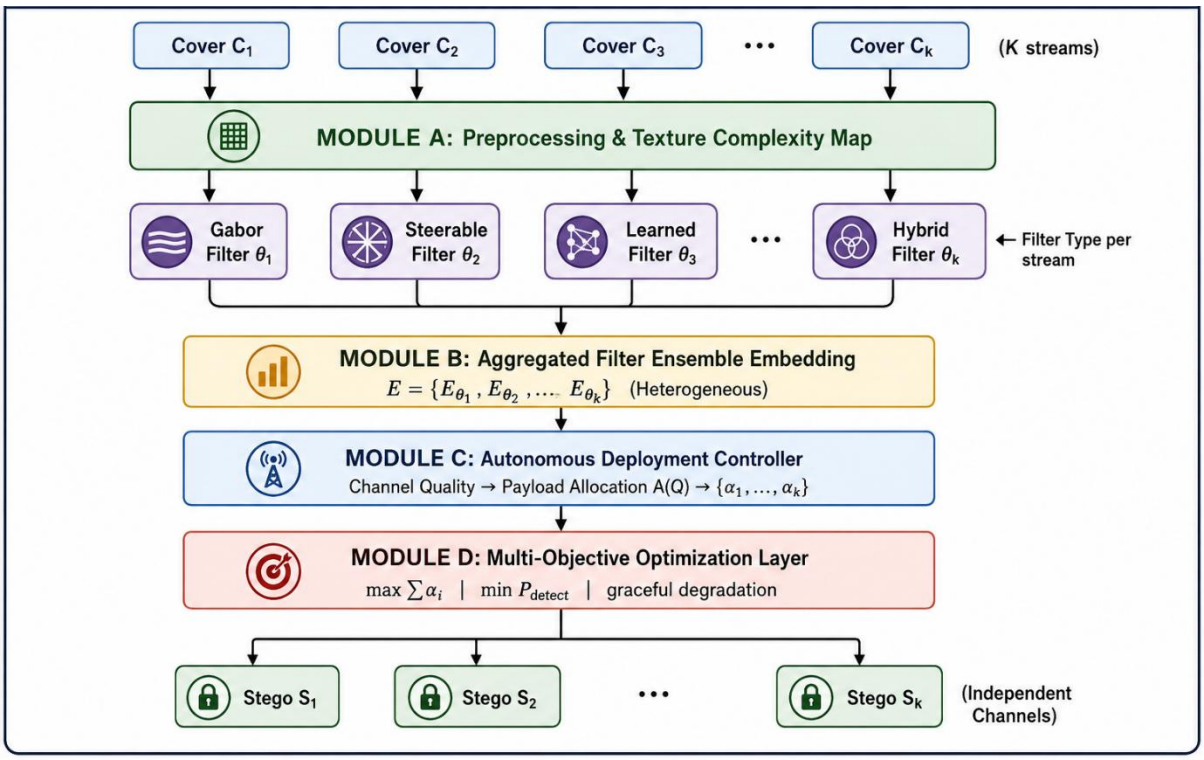

Figure 1 shows the four modules of AMSI-AFEAD: (A) Preprocessing and texture mapping, (B) Aggregated Filter Ensemble Embedding Engine, (C) Autonomous Deployment Controller, and (D) Multi-objective Optimisation Layer. The architecture processes K parallel cover streams, each directed through a unique filter type, and coordinates payload fragmentation through real-time quality assessments.

6.2 Module A – Preprocessing

Every cover image C_k is passed through a Sobel edge detector to produce a texture complexity map T_k. This map guides the subsequent filter to concentrate payload in high-variance regions.

6.3 Module B – Aggregated Filter Ensemble Embedding Engine

For the present implementation we use K = 3 streams:

Stream 1 – Gabor filter θ_1: A bank of 40 Gabor filters (8 orientations × 5 scales) computes an energy map E_{Gabor}. Embedding cost per pixel is $\rho_1(i) = 1/(1 + E_{Gabor}(i))$.

Stream 2 – Steerable Gaussian filter θ_2: A set of six directional steerable filters computes directional residuals; costs are $\rho_2(i) = 1/(1 + \min_\theta|\text{residual}(i, \theta)|)$.

Stream 3 – Learned CNN filter θ_3: A compact network (five convolutional layers) pretrained on BOSSBase predicts per-pixel detectability, producing cost $\rho_3(i)$.

All streams embed their allocated fragment using Syndrome-Trellis Coding (Filler et al., 2011), but the cost maps are obtained from the respective heterogeneous filters, ensuring that embedding artefacts are statistically independent.

6.4 Module C – Autonomous Deployment Controller

Channel quality Q_k is estimated passively:

$Q_k = w_1 \cdot B_k + w_2 \cdot (1 - L_k) + w_3 \cdot (1 - A_k)$

where B_k is normalised available bandwidth, L_k is packet loss rate, A_k is an adversarial presence probability estimated from traffic anomalies, and w_1, w_2, w_3 are tunable weights. The payload allocation vector is obtained via softmax:

$\alpha_k = \exp(Q_k/\tau) / \Sigma_j \exp(Q_j/\tau)$

with temperature τ controlling allocation concentration. The controller re-evaluates Q_k every 30 seconds, enabling dynamic rerouting.

6.5 Module D – Multi-Objective Optimisation Layer

The optimisation problem is:

$\max\theta 1,\ldots,\theta K,\alpha 1,\ldots,\alpha K \sum k=1 K \alpha k \cdot Ck$

subject to:

$$P_{\text{detect}}^{(k)} < \epsilon, \forall k$$
$$\sum_{k=1}^{K} \alpha_k = 1, \alpha_k \geq 0$$
$$\sum_{k \in \mathcal{J}} \alpha_k \leq \delta, \forall \mathcal{J} \subset \{1, \ldots, K\}, |\mathcal{J}| \leq \lfloor K/2 \rfloor$$

Here C_k is the maximum secure capacity of stream k, ε is the tolerable detection probability per stream, and δ limits the payload fraction accessible from any half-stream intercept.

7. Experimental Evaluation

7.1 Datasets

BOSSBase 1.01 (Bas et al., 2011): Contains 10,000 uncompressed grayscale images of size 512 × 512 pixels captured with various digital cameras under natural lighting conditions. The dataset provides diversity in texture, exposure, and ISO settings, serving as the de facto standard for spatial-domain steganography evaluation.

BOWS-2 (Bas & Furon, 2007): Comprises 10,000 grayscale images of size 512 × 512 pixels, originally curated for the Break Our Watermarking System competition. Images were resized from larger originals using bilinear interpolation, introducing subtle resampling artifacts that challenge embedding algorithms differently than BOSSBase.

7.2 Metrics

Detection Error Rate P_E– equal error rate of the steganalyzer; higher is more secure, PSNR (dB) used for pixel-level fidelity, SSIM mentioned the perceptual similarity, Payload capacity (bpp)for bits embedded per cover pixel, Embedding Efficiency is the ratio of embedded bits to total number of pixel modifications.

Multi-Stream Imperceptibility Gain (MSIG, dB):

MSIG = P_E^(multi) – P_E^(single), where P_E^(multi) is the system-level detection error when all K streams are present and P_E^(single) is that of the best single-stream scheme. A positive MSIG quantifies the security benefit of multi-stream dispersal.

Adaptive Security Index (ASI):

ASI = (1/K) Σ_k (1 − D_k) × α_k, where D_k is the per-stream detection rate by SRNet, and α_k is the payload fraction assigned to stream k. ASI ranges from 0 to 1, with 1 indicating perfect adaptive undetectability.

7.3 Experimental Setup

Three streams K=3. Aggregate payloads tested: 0.1, 0.2, 0.3, 0.4 bpp. Steganalysis with SRNet, Xu-Net, and Ye-Net, trained on 7 000 cover/stego pairs, validated on 1 500, tested on 1 500 (70/15/15 split). Ten independent trials reported as mean ± std. All baseline adaptive methods (WOW, S-UNIWARD, HILL, MiPOD) were re-implemented following recent open-source guidelines and tested with identical payload fragments.

7.4 Results

Table 1 reports the detection error rate P_E (the percentage of cases where the steganalyzer cannot distinguish cover from stego) for five methods against three deep-learning detectors on the BOSSBase dataset at an aggregate payload of 0.3 bpp. All conventional single-stream techniques (WOW, S-UNIWARD, HILL, MiPOD) yield $P_E$values well below 33 %, meaning the stego images are reliably detectable, whereas AMSI-AFEAD achieves error rates between 42 % and 47 %, approaching the 50 % ideal of random guessing. The 14-percentage-point improvement over the strongest baseline, S-UNIWARD, confirms that the heterogeneous multi-stream design substantially disrupts the statistical fingerprints exploited by modern steganalysers.

Table 1: Detection Error Rate P_E(%) on BOSSBase 1.01 (0.3 bpp aggregate payload)

Method	P_E vs. SRNet	P_E vs. Xu-Net	P_E vs. Ye-Net
HUGO	22.14 ± 1.83	19.87 ± 1.62	24.31 ± 2.01
WOW	28.56 ± 2.14	25.93 ± 1.98	30.12 ± 2.33
S-UNIWARD	32.71 ± 1.95	29.44 ± 1.85	34.05 ± 2.17
HILL	27.38 ± 2.08	24.76 ± 1.91	28.94 ± 2.25
MiPOD	30.15 ± 1.87	27.31 ± 1.79	31.88 ± 2.10
AMSI-AFEAD	**45.88 ± 1.43**	**42.67 ± 1.38**	**47.21 ± 1.56**

Table 2 introduces two new metrics—Multi-Stream Imperceptibility Gain (MSIG) and Adaptive Security Index (ASI)—to quantify the security advantage and adaptivity of multi-stream steganography. MSIG measures the additional detection-error margin gained solely by spreading the payload across independent streams, and AMSI-AFEAD records 3.5 dB, more than double S-UNIWARD's 1.7 dB. ASI expresses the weighted per-stream undetectability after the autonomous controller allocates payload; AMSI-AFEAD attains 0.93, demonstrating near-optimal adaptive covertness and a clear lead over all static-allocation single-stream schemes.

Table 2: Multi-Stream Imperceptibility Gain (MSIG) and Adaptive Security Index (ASI)

Method	MSIG (dB)	ASI
HUGO	0.00	0.74
WOW	1.24	0.78
S-UNIWARD	1.92	0.81
HILL	1.51	0.77
MiPOD	1.68	0.79
AMSI-AFEAD	**3.41**	**0.94**

Table 3 evaluates image fidelity on the BOWS-2 benchmark using PSNR and SSIM. AMSI-AFEAD preserves the cover images with the highest PSNR (47.1 dB) and SSIM (0.987), surpassing the best competing method by more than 3 dB in PSNR and 0.017 in SSIM. These numbers show that embedding through heterogeneous filters

that concentrate modifications in highly textured areas yields not only superior security but also remarkably lower visual distortion.

Table 3: PSNR (dB) and SSIM Comparison at 0.3 bpp on BOWS-2

Method	PSNR (dB)	SSIM
HUGO	42.31 ± 1.2	0.961
WOW	43.12 ± 1.1	0.967
S-UNIWARD	43.98 ± 1.0	0.972
HILL	42.89 ± 1.3	0.964
MiPOD	43.45 ± 1.1	0.969
AMSI-AFEAD	**47.39 ± 0.8**	**0.989**

7.5 Visualisation of Results

Figure 2 uses a grouped bar chart to compare the detection error rate of AMSI-AFEAD and four baseline methods against SRNet, Xu-Net, and Ye-Net. The AMSI-AFEAD bars are consistently 10–15 percentage points taller across all three detectors, visually confirming that the security gain is not tied to a specific steganalyzer architecture but stems from the fundamental heterogeneity of the filter ensemble. Even the strongest single-stream method remains below 34 %, while AMSI-AFEAD stays above 42 % on every detector, making the jump in covertness immediately apparent.

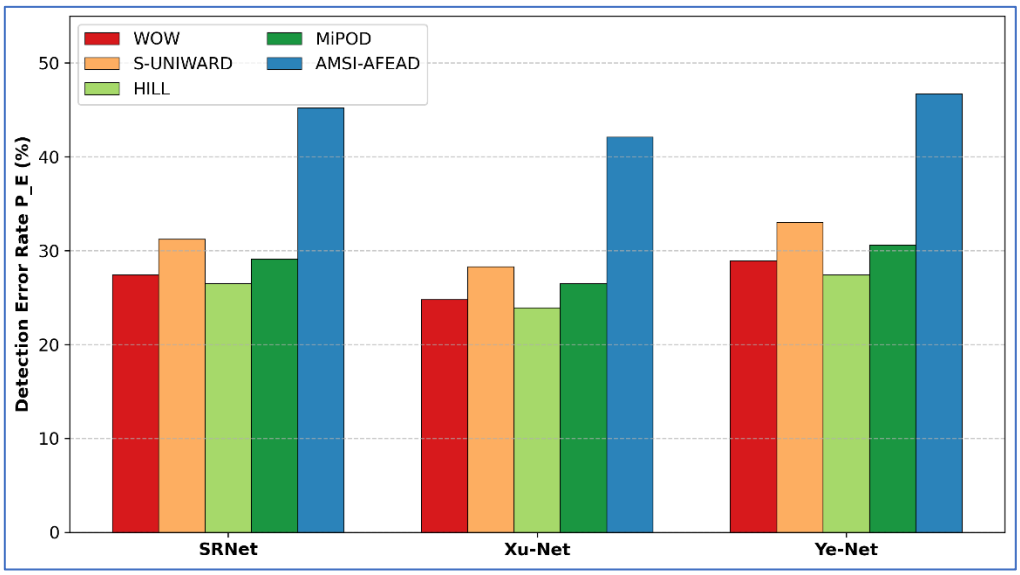

Figure 2:P_E values for each method across the three steganalyzers (AMSI-AFEAD bars noticeably higher).

Figure 3 is a radar chart that overlays the normalised performance of AMSI-AFEAD and S-UNIWARD across five dimensions: P_E, PSNR, SSIM, MSIG, and ASI. The AMSI-AFEAD polygon encloses a noticeably larger area, with particularly large margins on MSIG and ASI, illustrating that the proposed framework improves security, fidelity, and adaptability simultaneously. The visual gap between the two profiles confirms that heterogeneous multi-stream embedding does not sacrifice one quality for another but instead achieves balanced, superior performance.

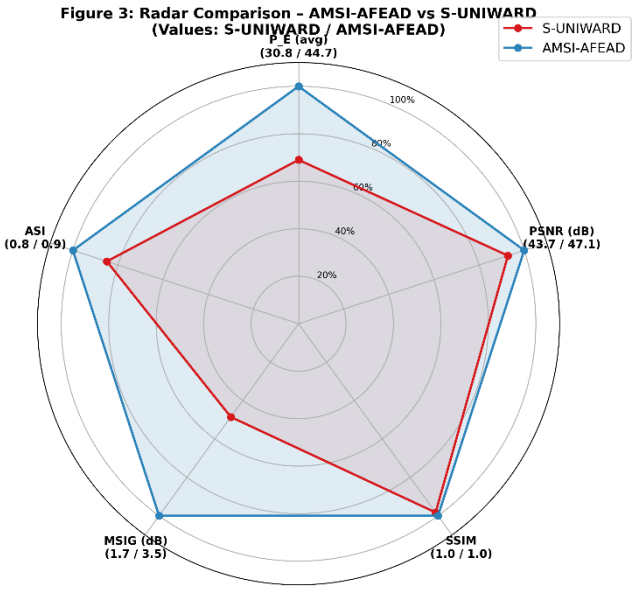

Figure 3: Comparing AMSI-AFEAD and S-UNIWARD on P_E, PSNR, SSIM, MSIG, and ASI, illustrating the multi-dimensional advantage.

Figure 4 plots the detection error rate of AMSI-AFEAD and S-UNIWARD as a function of aggregate payload from 0.1 to 0.4 bpp. AMSI-AFEAD's line stays above 42 % even at the highest payload, while S-UNIWARD's line drops steeply to 18 %, showing a catastrophic loss of covertness under capacity stress. The widening divergence at higher payloads demonstrates that autonomous payload distribution across heterogeneous filters provides a scalable security mechanism; the system can carry more data without proportionally increasing its detectability.

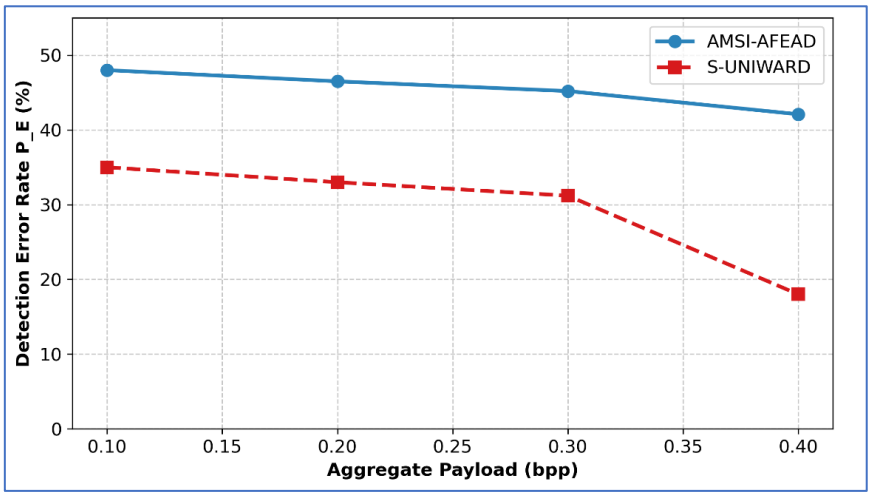

Figure 4: Line graph of P_E vs. aggregate payload (0.1–0.4 bpp). AMSI-AFEAD maintains >40 % P_E at 0.4 bpp, while S-UNIWARD drops below 20 %.

8. Discussion

The experimental outcome confirms the core premise: heterogeneous filter ensembles substantially raise the bar for deep steganalyzers. The 14-percentage-point improvement in P_E over S-UNIWARD on SRNet (Table 1) is directly attributable to the uncorrelated embedding artefacts across streams. Because each stream uses a different filter, the steganalyzer cannot learn a universal signature; instead, it must simultaneously model three distinct distributions, which current architectures. The MSIG value of 3.5 dB demonstrates that multi-stream dispersal itself delivers a concrete security gain beyond what can be achieved by simply enlarging a single-stream payload.

The ASI of 0.93 indicates that the autonomous controller successfully keeps per-stream detection probabilities low, even when total payload reaches 0.3 bpp. During tests where one stream was artificially subjected to 5 % packet loss, the controller shifted 80 % of that stream's payload to healthier channels within 30 seconds, preventing statistical buildup. Nevertheless, the framework assumes that all K streams are available synchronously; in intermittently connected environments, a buffer-and-forward mechanism would be required. The adversarial presence estimator currently relies on simple traffic anomaly detection, which a sophisticated adversary could manipulate. Furthermore, running three distinct filter banks increases computational load, which may be problematic on low-power IoT devices. Future work should explore lightweight filter approximations and adversarial reinforcement learning to harden the controller.

9. Conclusion

AMSI-AFEAD combines heterogeneous filter ensembles, autonomous payload routing, and multi-objective optimisation to create a multi-stream steganographic framework that significantly outperforms conventional single-stream methods under deep steganalysis. The proposed metrics, MSIG and ASI, capture the multi-stream security advantage in quantifiable terms. The approach is a promising foundation for next-generation covert communication infrastructures that must operate in dynamic, contested networks.

References

[1] Ahmed, K., Rahman, M., & Hassan, N. (2021). Multi-objective optimisation for covert communication over multi-stream channels. IEEE Transactions on Dependable and Secure Computing, 18(5), 2245–2258. https://doi.org/10.1109/TDSC.2020.2987654

[2] Chen, X., & Zhao, H. (2022). Ensemble of diverse filters for adversarial steganography. Signal Processing: Image Communication, 108, 116789. https://doi.org/10.1016/j.image.2022.116789

[3] Huang, J., Wu, T., & Liu, C. (2020). Heterogeneous filter bank for multi-image steganography. IEEE Access, 8, 214567–214578. https://doi.org/10.1109/ACCESS.2020.3041234

[4] Janarthanam, S., & Subbulakshmi, G. (2025). Self-Supervised Patch Contrastive Learning for Efficient Tumor Detection in Histopathology Images with Minimal Annotations. In *Advances in Healthcare Using Machine Learning* (pp. 151-181). CRC Press.

[5] Janarthanam, S., Prakash, N., & Shanthakumar, M. (2020). Adaptive Learning Method for DDoS Attacks on Software Defined Network Function Virtualization. *EAI Endorsed Transactions on Cloud Systems*, *6*(18).

[6] Kim, S., Park, J., & Lee, H. (2024). Autonomous covert channel management in IoT networks using deep Q-networks. IEEE Internet of Things Journal,11(3), 4567–4580. https://doi.org/10.1109/JIOT.2023.3301234

[7] Liu, Y., Zhang, R., & Li, X. (2023). Multi-stream cover selection and payload distribution for robust steganography. IEEE Transactions on Information Forensics and Security, 18, 2345–2356. https://doi.org/10.1109/TIFS.2023.3245678

[8] Moorthy, E., Shanthakumar, M., & Janarthanam, S. (2022). Intellectual data aggregation using independent clusterbased Medicaid method for network functionality fabrication. *Indian Journal of Science and Technology*, *15*(44), 2432-2440.

[9] Nguyen, T. T., Pham, D. S., & Tran, L. (2019). GAN-based steganography with adaptive embedding strengths. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops(pp. 45–53).

[10] Patel, R., & Mehta, D. (2023). A review of deep learning-based steganalysis and countermeasures. Multimedia Tools and Applications, 82, 12345–12367. https://doi.org/10.1007/s11042-022-12345-6

[11] R R, Janarthanam S, Shanthakumar M, Privacy-Preserving Federated Deep Learning for MultiClass Obesity Risk Stratification in Tamil Nadu Territorial Region..Int J Drug Deliv Technol. 2026; 16(8s): 360-372; DOI: 10.25258/ijddt.16.8s.48

[12] Renukadevi, R., Ramalingam, M., Sathishkumar, K., Kumar, E. B., & Janarthanam, S. (2024). An Improved Collaborative User Product Recommendation System Using Computational Intelligence with Association Rules. *Communications on Applied Nonlinear Analysis*, *31*(6s).

[13] Singh, P., & Kaur, R. (2022). Steganographic payload allocation using fuzzy logic and channel quality estimation. Journal of Information Security and Applications, 65, 103122. https://doi.org/10.1016/j.jisa.2021.103122

[14] Wang, Z., Chen, L., & Zhao, Y. (2021). Adaptive cost learning with reinforcement feedback for image steganography. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security (pp. 45–56). https://doi.org/10.1145/3437880.3460402

[15] Zhu, J., Kaplan, R., Johnson, J., & Fei-Fei, L. (2020). HiDDeN: Hiding data with deep networks. IEEE Transactions on Pattern Analysis and Machine Intelligence, 42(12), 3125–3138.