September 1, 2025

To: Editor-in-Chief
Journal: Knowledge-Based Systems
Publisher: Elsevier

Subject: Submission of Original Research Article - "MedDef: An Efficient Self-Attention Model for Adversarial Resilience in Medical Imaging with Unstructured Pruning"

Dear Editor,

We are pleased to submit our original research article titled **"MedDef: An Efficient Self-Attention Model for Adversarial Resilience in Medical Imaging with Unstructured Pruning"** for consideration for publication in Knowledge-Based Systems.

Research Significance and Contribution

This manuscript addresses a critical and timely challenge in the intersection of artificial intelligence and healthcare: the vulnerability of medical imaging AI systems to adversarial attacks. As AI-powered diagnostic tools become increasingly prevalent in clinical settings, their susceptibility to malicious perturbations poses serious risks to patient safety and diagnostic reliability.

Our work makes several significant contributions to the field:

1. **Novel Architecture Innovation:** We introduce the Defense-Aware Attention Mechanism (DAAM), the first comprehensive solution that integrates adversarial robustness directly into the feature extraction process, rather than relying on post-hoc defensive measures.

2. **Counterintuitive Discovery:** We demonstrate that strategic unstructured pruning, traditionally viewed as potentially harmful to model robustness, actually enhances security when properly calibrated for medical imaging applications—a finding that challenges conventional wisdom in the field.

3. **Breakthrough Performance:** Unlike existing approaches that sacrifice diagnostic accuracy for security (with reported drops of 5-16%), MedDef achieves exceptional

adversarial accuracy of 97.52% while maintaining high diagnostic performance on clean images.

4. **Clinical Viability:** Our comprehensive evaluation on Retinal OCT and Chest X-Ray datasets against four major attack methodologies (FGSM, PGD, BIM, and JSMA) demonstrates real-world applicability.

Alignment with Journal Scope

This research aligns perfectly with Knowledge-Based Systems' focus on intelligent systems and their practical applications. Our work combines:

- Knowledge-based AI systems for medical diagnosis
- Intelligent security mechanisms for healthcare applications
- Novel attention-based architectures with domain-specific knowledge integration
- Practical deployment considerations for safety-critical environments

Novelty and Impact

The paper presents the first comprehensive solution that makes adversarial robustness practical for real-world clinical deployment. This addresses a critical barrier to the widespread adoption of AI in healthcare settings where patient safety is paramount. The research has immediate implications for clinical AI system designers, healthcare technology developers, medical device regulators, and hospital IT security teams.

Methodology and Validation

Our approach is rigorously validated through comprehensive ablation studies across multiple model variants, attack intensity analysis across different epsilon values, compression-security trade-off analysis, state-of-the-art comparative evaluation, and interpretability analysis through saliency mapping.

Author Contributions and Ethics

All authors have made substantial contributions to this research and have approved the final manuscript. The research was conducted in accordance with ethical standards, utilizing publicly available datasets (Retinal OCT and Chest X-Ray datasets). We declare all funding sources and potential conflicts of interest in our Declaration of Interest Statement.

Manuscript Status

This manuscript is original work that has not been published elsewhere and is not under consideration by any other journal. All co-authors have reviewed and approved the submission.

Conclusion

We believe this research makes a significant contribution to the field of knowledge-based systems, particularly in the critical domain of healthcare AI security. The practical implications for clinical deployment and patient safety make this work highly relevant to the Knowledge-Based Systems readership.

We respectfully request that you consider our manuscript for publication and look forward to your review process. We are prepared to address any comments or suggestions from reviewers to improve the manuscript.

Thank you for your time and consideration.

Sincerely,

E.K. Dongbo (Submitting Author)
School of Information Science and Engineering
University of Jinan
Email: enoch.dongbo@stu.ujn.edu.cn
ORCID: 0009-0005-5213-9834

S. Niu (Corresponding Author)
School of Information Science and Engineering
University of Jinan

Email: sjniu@hotmail.com
ORCID: 0000-0002-1401-9859

Manuscript Details

- **Article Type:** Original Research Article
- **Word Count:** Approximately 10,000 words
- **Figures:** 4 main figures plus supporting visualizations
- **Tables:** 5 comprehensive evaluation tables
- **References:** 38 current and relevant citations
- **Keywords:** Adversarial Resilience, Medical Imaging, Defense-Aware Attention Mechanism, Unstructured Pruning, Robust Model