Review of: "WaveBit — Nonbinary Computation: I Symmetric Cryptography"

Nithiyanantham Janakiraman[1]

1 KLN College of Engineering

Potential competing interests: No potential competing interests to declare.

Review Comments on WaveBits Encryption:

This work presents a novel and intriguing approach to data encryption using continuous waves and frequencies. Here are some key review comments:

Strengths:

- **Originality:** The concept of using waveforms for encryption is fundamentally different from traditional binary methods, representing a significant departure from the norm.
- **Efficiency:** Encoding 128 WaveBits with only 7 frequencies demonstrates impressive data representation efficiency.
- **Versatility:** The capability to encrypt various data types beyond text, including images and multimedia, opens up diverse application possibilities.
- **Resource Optimization:** Potential for reduced resource usage in terms of RAM, storage, and processing time makes it attractive for resource-constrained environments.
- **Future Potential:** Exploring applications in Spectral Neural Networks and Large Language Models holds promise for future advancements.

Weaknesses:

- **Security Analysis:** The paper lacks a thorough analysis of the encryption's security against common attacks, which is crucial for real-world adoption.
- **Implementation Details:** More information on the practical implementation and feasibility of the method, including potential hardware or software requirements, would be beneficial.
- **Comparison with Existing Methods:** A comparison of WaveBits encryption with established methods in terms of security, efficiency, and resource usage would provide valuable context.
- **Technical Discussions:**

- While the paper mentions the potential application of Spectral Neural Networks (SNN) for training Large Language Models (LLMs), it lacks concrete proof of concepts in this regard. Including some preliminary results or examples would enhance the credibility of this claim.
- The article could benefit from more in-depth discussions on the technical aspects of the proposed methodology,

especially regarding its robustness and potential vulnerabilities.

- The paper could benefit from clearer explanations of some technical concepts for a broader audience.
- Mentioning the limitations of the current work and potential challenges for future development would strengthen the research.

Overall:

This work presents a promising new direction for data encryption with its unique approach and potential advantages. However, further research is needed to address security concerns, provide implementation details, and compare it with existing methods for a more comprehensive evaluation.