Review of: "A Unified Framework for Cyber Oriented Digital Engineering using Integration of Explainable Chaotic Cryptology on Pervasive Systems"

Alessandro Carrega

Potential competing interests: No potential competing interests to declare.

The document provides a comprehensive exploration of the integration of explainable chaotic cryptology in multimedia content protection, focusing on the application of chaotic cryptology primitives to enhance security and transparency in cryptographic systems. It emphasizes the significance of transparent encryption processes, user trust, and security in cryptographic applications, and discusses the properties and characteristics of explainable approaches in multimedia security. The authors delve into the taxonomy of explainable approaches, distinguishing between ante-hoc and post-hoc explanations, and provide an analysis of different types of chaotic maps and their usability in various cryptographic applications. The document also addresses the challenges and proposed solutions in implementing chaotic cryptology in multimedia content protection, highlighting the need for integration with existing systems, interoperability with diverse platforms, resource allocation, and scaling. Additionally, it presents research outcomes on a real use-case of AI-automated cyber-oriented digital engineering (CODE-pilot), providing a unified framework for efficient integration across cyber-physical embedded IoT platforms. Overall, the document offers valuable insights into the evolving field of explainable chaotic cryptology, bridging the gap between cryptographic strength and user comprehension in multimedia content protection. It provides a structured framework for understanding the integration of explainable chaotic cryptology in cryptographic systems and offers potential avenues for future research and practical implementations in securing multimedia content.

The chaotic cryptology implementations could be improved for better scalability and integration with existing systems by focusing on the following aspects:

Adaptive Mechanisms: Research should focus on refining existing chaotic ciphers with adaptive mechanisms to ensure seamless integration with diverse platforms and systems. This would enable the chaotic cryptology implementations to dynamically adjust to the requirements of different systems, enhancing their scalability and interoperability.

Time-Delay Time-Lock Puzzles: The integration of time-delay time-lock puzzles into chaotic multimedia ciphers represents a futuristic approach to bolstering security. By introducing temporal constraints and dynamic key components, these ciphers become resilient against attacks attempting to exploit static parameters. This approach aligns with the evolving nature of multimedia content protection needs and can enhance the scalability and security of chaotic cryptology implementations.

Advanced Adversarial Evaluations: Employing advanced adversarial evaluations can help in refining chaotic ciphers to ensure they are not only resistant to known attacks but also resilient against emerging threats. This multifaceted approach ensures that the cryptographic systems are robust and adaptable to evolving security challenges.

Regarding the impact of ante-hoc and post-hoc explanations on user trust and comprehension in multimedia content protection:

Ante-Hoc Explanation:

- **Transparency**: Ante-hoc explanations ensure transparency in the encryption process, allowing users to comprehend how their multimedia content is being secured. This fosters a sense of trust in the system.
- **User Understanding**: Ante-hoc explanations communicate the properties of chaotic systems in a clear manner, enabling users to understand how the cryptographic algorithms manipulate their data before the encryption process begins.
- **Parameter Accessibility**: Users have access to key parameters and variables involved in the chaotic encryption, enabling them to grasp the intricacies of the cryptographic operations applied to their multimedia content.

Post-Hoc Explanation:

- **Outcome Interpretability**: Post-hoc explanations focus on clarifying the results of the decryption process, allowing users to understand why certain outcomes occurred and gain insights into the decrypted multimedia content.
- **Error Analysis**: Post-hoc explanations provide a means for users to analyze and comprehend the reasons behind decryption errors or unexpected outcomes, enhancing system diagnostics.
- **Traceability**: Users can trace the cryptographic steps taken during decryption, aiding in the reconstruction of the original multimedia content. This traceability enhances the recovery process and overall system reliability.

In summary, both ante-hoc and post-hoc explanations play a crucial role in enhancing user trust and comprehension in multimedia content protection. Ante-hoc explanations provide transparency and facilitate trust, while post-hoc explanations allow users to understand the outcomes of the decryption process and analyze any errors, ultimately contributing to a holistic understanding of the cryptosystem's functionality and outcomes.