

Abstract: Enhancing Data Security through AI and Chaos Theory

Today, digital data permeates every aspect of our personal and professional interactions. However, this ubiquity creates a growing risk of sophisticated cryptanalysis attacks designed to compromise sensitive personal information. While traditional cryptography has been a primary defense for decades, the advent of AI-based adversarial techniques has significantly lowered the vulnerability threshold of once-robust cryptographic algorithms. This evolution necessitates a paradigm shift in how we secure information. Our research proposes a new defense framework that integrates the unpredictability of chaotic systems with the adaptive power of artificial intelligence. By leveraging the initial condition sensitivity inherent in chaos theory and the pattern recognition capabilities of AI models, we have developed a hybrid protection technique capable of withstanding advanced cyber threats. The synergy of these three domains: AI, chaos theory, and cryptography constitutes a formidable barrier against intrusions. The experimental results presented in this study demonstrate that this integrated approach offers a superior level of security, guaranteeing data integrity and confidentiality in an increasingly hostile digital environment.