ABSTRACT

Novandi Ahmad Ramdhan. 51422256

DEVELOPMENT AND COMPARISON OF ENCRYPTION ALGORITHMS BASED ON CHAOS FUNCTION MS GAUSS MAP AND GAUSS MS MAP FOR MEDICAL DIGITAL IMAGE SECURITY

Thesis. Informatics Engineering Study Program, Faculty of Industrial Technology, Gunadarma University, 2026.

Keywords: Medical Image Encryption, Chaos Cryptography, Composition Function, MS Map, Gauss Map

(xv + 147 + Appendix)

The advancement of Hospital Management Information Systems (HMIS) has driven the digitalization of Electronic Health Records (EHR), including high-resolution diagnostic images such as MRI, CT-Scan, and histopathology slides. Storing these data in local databases is highly vulnerable to cyberattacks and data theft, making the implementation of robust encryption an absolute necessity. Chaos-based cryptography has emerged as a leading solution due to its pseudo-random properties, extreme sensitivity to initial conditions, and efficient computation for large image data. This study develops a new key stream generator algorithm using the MS-Gauss Map composition function ($f \circ g$) as a novelty and analytically compares it with its predecessor, the Gauss-MS Map ($g \circ f$). The research methodology includes designing and implementing both composition functions as XOR-based stream cipher components, testing chaotic properties using Lyapunov Exponent, bifurcation diagram, and scatter plot, and evaluating key randomness using 15 NIST SP 800-22 statistical tests. Encryption quality is measured through Goodness of Fit (Chi-Square), pixel correlation analysis, Shannon entropy, differential analysis (NPCR and UACI), and image quality metrics (MSE and PSNR) on 20 medical images (grayscale X-Ray/MRI and RGB histopathology). Results show that both algorithms pass all 15 NIST SP 800-22 tests, produce nearly identical Shannon entropy values, pixel correlation close to zero, perfect NPCR and UACI, and fully lossless image recovery (MSE = 0, PSNR = ∞ dB). This study proves that the developed Gauss-MS Map ($f \circ g$) has cryptographically equivalent security performance to MS-Gauss Map ($g \circ f$), making it a viable alternative for reliable medical record encryption systems.

References (2008-2026)