ABSTRAK

Novandi Ahmad Ramdhan. 51422256

PENGEMBANGAN DAN PERBANDINGAN ALGORITMA ENKRIPSI BERBASIS FUNGSI CHAOS MS GAUSS MAP DAN GAUSS MS MAP UNTUK KEAMANAN CITRA DIGITAL MEDIS

Skripsi. Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Gunadarma, 2026.

Kata Kunci: Enkripsi Citra Medis, Kriptografi Chaos, Fungsi Komposisi, MS Map, Gauss Map

(xv + 147 + Lampiran)

Perkembangan Sistem Informasi Manajemen Rumah Sakit (SIMRS) telah mendorong digitalisasi rekam medis elektronik (EHR), termasuk citra diagnostik beresolusi tinggi seperti MRI, CT-Scan, dan histopatologi. Penyimpanan data tersebut dalam basis data lokal sangat rentan terhadap serangan siber dan pencurian data, sehingga penerapan enkripsi menjadi suatu keharusan mutlak Kriptografi berbasis chaos menjadi solusi unggulan karena sifat pseudo-random, sensitivitas ekstrem terhadap kondisi awal, serta komputasi yang efisien untuk data citra berukuran besar. Penelitian ini mengembangkan algoritma pembangkit kunci (key stream) baru menggunakan fungsi komposisi MS-Gauss Map ($g \circ f$) sebagai kebaruan (novelty), kemudian membandingkannya secara analitis dengan fungsi komposisi pendahulunya Gauss-MS Map ($f \circ g$). Metode penelitian meliputi perancangan dan implementasi kedua fungsi komposisi sebagai komponen stream cipher berbasis XOR, pengujian sifat chaotic menggunakan Lyapunov Exponent, diagram bifurkasi, dan scatter plot, serta evaluasi keacakan kunci menggunakan 15 uji statistik NIST SP 800-22. Kualitas enkripsi diukur melalui uji Goodness of Fit (Chi-Square), analisis korelasi piksel, entropi Shannon, analisis diferensial (NPCR dan UACI), serta kualitas citra (MSE dan PSNR) pada 20 citra medis (grayscale X-Ray/MRI dan RGB histopatologi). Hasil penelitian menunjukkan bahwa kedua algoritma lulus seluruh 15 uji NIST SP 800-22, menghasilkan nilai entropi Shannon yang hampir identik, korelasi piksel mendekati nol, NPCR dan UACI yang sempurna, serta pemulihan citra yang sepenuhnya lossless (MSE = 0, PSNR = ∞ dB). Penelitian ini membuktikan bahwa fungsi komposisi Gauss-MS Map ($f \circ g$) yang dikembangkan memiliki performa keamanan yang ekuivalen secara kriptografis dengan MS-Gauss Map ($g \circ f$), sehingga layak diimplementasikan sebagai alternatif sistem enkripsi rekam medis yang andal.

Daftar Pustaka (2008-2026)