ABSTRAK

Steganalisis merupakan salah satu metode untuk menyerang sistem steganografi, salah satunya adalah steganalisis yang berbasis pada substitusi sinonim. Serangan steganalisis ini dilakukan dengan menganalisis nilai kesesuaian konteks kalimat. Sistem steganografi berbasis substitusi sinonim dengan menetapkan nilai kesesuaian konteks teks sampul tidak pada nilai maksimum diusulkan menggunakan metode ini. Steganalisis tidak dapat membedakan antara sampul dan teks stego. Untuk mewujudkan steganografi ini digunakan metode, diantaranya context fitness digunakan untuk memberikan nilai context fitness dari sebuah kalimat, Context-free grammar untuk membuat cover text, Quantum Random Number Generator untuk mendapatkan nilai biner yang digunakan untuk memodifikasi cover text, Zero-Width Character untuk menyembunyikan kunci biner, dan Sistem T-Lex untuk proses penyisipan pesan yang bekerja dengan mengganti kata dengan sinonimnya dimana dalam memilih sinonim ditentukan berdasarkan kode pesan rahasia yang sesuai. Dengan menggunakan metode yang diusulkan, akurasi steganalisis berkisar dari 5,58 % hingga 16,00 % sedangkan menggunakan metode sebelumnya akurasi steganalisis berkisar dari 86,41% hingga 97,91%. Bukti ini membuktikan bahwa steganalisis berbasis penyisipan kata dengan steganalisis sinonim tidak dapat bekerja secara efektif pada metode steganografi yang diusulkan..

Kata kunci: Steganography, Steganalysis, Natural Language Processing, QRNG, Zero Width Character, Support Vector Machine, Context-Free Grammar