

INTISARI

PERBANDINGAN KINERJA ALGORITMA KUNCI PUBLIK UNTUK TANDA TANGAN DIGITAL PADA STEGANOGRAFI CITRA DIGITAL

RENI KOIBUR
14/372359/PPA/04671

Pemanfaatan teknologi informasi (TI) telah merambah hampir semua segi kehidupan masyarakat. Komunikasi terselubung disekitar kita menggunakan kriptografi dan steganografi untuk menghindari pelacakan sehingga tidak terdeteksi. Steganografi digunakan untuk menyembunyikan pesan dan tanda tangan digital (digital signatures) untuk membuktikan (autentifikasi) identitas pengirim dan penerima pesan yang sah. Algoritma kunci publik yang digunakan untuk tanda tangan digital (digital signatures) secara luas adalah algoritma RSA dan El-Gamal dan Gost, namun belum diketahui algoritma mana yang paling efektif dan efisien serta terbaik maka dibutuhkan pengujian kinerja dari algoritma tersebut.

Penelitian ini difokuskan pada perbandingan kinerja algoritma kunci publik RSA, ElGamal dan Gost untuk tanda tangan digital pada steganografi citra digital dengan parameter uji: Big O, Waktu Pembentukan Kunci (Kunci Privat dan Kunci Publik), Waktu Enkripsi, Waktu Dekripsi, Avalance Effec, Koefisien korelasi, Deviasi maksimum, Deviasi ketidakteraturan dan PNSR citra. Penentuan algoritma terbaik dilakukan dengan menggunakan metode SAW (Simple Addictive Weighting) yang dilakukan pada 10 citra digital dengan ekstensi *.jpg dan *.bmp dengan menggunakan 4 skenario uji. Hasil pengujian memperlihatkan bahwa dari sisi efisiensi, algoritma RSA dan ElGamal lebih baik dari Algoritma Gost, tetapi dari sisi efektifitas, algoritma Gost menunjukkan hasil kinerja yang lebih baik dengan nilai pada skenario I (bobot yang sama) sebesar 0,98, skenario II ((Efektifitas) sebesar 0,94 serta skenario III (kualitas) sebesar 0,94.

Kata Kunci: Steganografi, *Digital Signatures*, Algoritma RSA, Algoritma ElGamal, Algoritma Gost, Metode SAW.

ABSTRACT

PERFORMANCE COMPARISON OF PUBLIC KEY FOR DIGITAL SIGNATURES ON STEGANOGRAPHY OF DIGITAL IMAGERY

RENI KOIBUR
14/372359/PPA/04671

Utilization of information technology (IT) has penetrated almost all aspects of community life. The hidden communication around us uses cryptography and steganography to avoid tracking so it is undetectable. Steganography is used to hide messages and digital signatures to authenticate the identity of legitimate senders and recipients. Public key algorithms used for digital signatures are RSA and El-Gamal and Gost algorithms, but it is not yet known which algorithm is the most effective and efficient and the best is required performance testing of the algorithm.

This study focused on the performance comparison of RSA, ElGamal and Gost public key algorithms for digital signatures on digital image steganography with test parameters: Big O, Key Build Time (Private Key and Public Key), Encryption Time, Decryption Time, Avalanche Effect, Coefficients correlation, maximum deviation, deviation of irregularities and image PNSR. The best algorithm determination was done by using SAW (Simple Addictive Weighting) method performed on 10 digital images with extension *.jpg and *.bmp using 4 test scenarios. The test results show that in terms of efficiency, RSA and ElGamal algorithm is better than Gost Algorithm, but in terms of effectiveness, Gost algorithm shows better performance results with value in scenario I (equal weight) of 0.98, scenario II (Effectiveness) of 0.94 and scenario III (quality) of 0.94

Keywords: Steganography, Digital Signatures, RSA Algorithm, ElGamal Algorithm, Gost Algorithm, SAW Me