PENINGKATAN KEAMANAN TEKS MENGGUNAKAN KRIPTOGRAFI DAN STEGANOGRAFI

Siti Agustini, Muchamad Kurniawan
Institut Teknologi Adhi Tama Surabaya
Email: sitiagustini@itats.ac.id

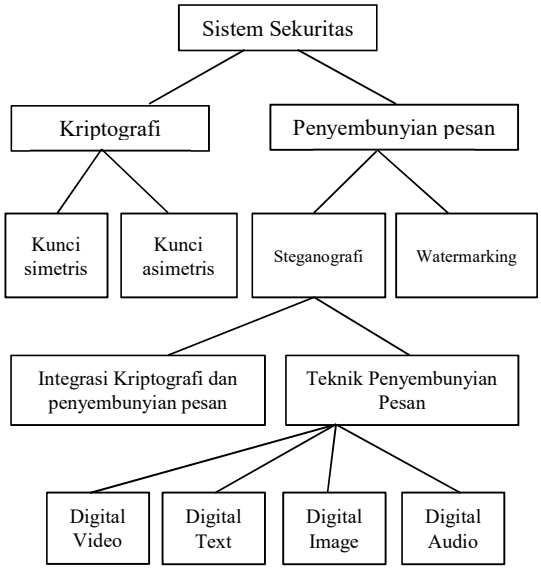
Abstrak. *Keamanan informasi telah diterapkan dengan berbagai metode. Dalam penelitian ini, kami menggabungkan metode kriptografi dan steganografi untuk mengamankan informasi. Informasi rahasia yang digunakan adalah sebuah teks. Informasi rahasia dienkripsi dengan algoritma RSA dan kemudian ciphertext disembunyikan ke dalam sebuah media gambar dengan algoritma XOR. Bit-bit pesan rahasia disematkan pada 3 bit terakhir dari piksel gambar menggunakan algoritma XOR. Metode yang diusulkan memiliki gambar hasil steganografi yang baik dan running time yang cukup singkat pada proses enkripsi dan ekstraksi serta kualitas steganografi lain seperti MSE rata-rata mencapai 0,8768, PSNR rata-rata sekitar 50,1588. Perbandingan histogram antara gambar asli dan gambar stego tidak menunjukkan perbedaan yang signifikan, hal ini menunjukkan stego image memiliki karakter seperti gambar asli.*

Kata Kunci: keamanan data, RSA, XOR

Mengamankan data atau informasi dapat dilakukan dengan menggunakan beberapa metode termasuk kriptografi dan steganografi. Kriptografi adalah seni atau ilmu yang mempelajari bagaimana suatu pesan dapat disampaikan oleh pengirim kepada penerima dengan aman dengan mengkodekan pesan tersebut sehingga tidak dapat dibaca [1]. Kriptografi akan menjaga kerahasiaan informasi dari orang yang tidak berwenang. Steganografi adalah seni atau ilmu untuk menyembunyikan pesan sehingga hanya pengirim dan penerima tahu isi pesan sementara yang lain tidak akan menyadari pesan tersembunyi [2]. Kriptografi dan steganografi dapat digunakan bersama untuk meningkatkan keamanan data untuk memastikan kerahasiaan informasi.

Pada Gambar 1, kriptografi dibagi menjadi 2, yaitu kunci simetris dan kunci asimetris. Kunci simetris adalah metode enkripsi di mana pengirim dan penerima menggunakan kunci yang sama. Sedangkan kunci publik dan kunci privat. Algoritma ideal kategori kunci simetris adalah DES, sedangkan kategori kunci asimetris adalah RSA.

Algoritma RSA memiliki tingkat keamanan yang lebih tinggi daripada DES dan layanan aman yang lebih beragam, yaitu kerahasiaan, integritas, dan non-repudiation [4]. Untuk memperkuat keamanan data atau informasi, kriptografi juga dapat digunakan bersamaan dengan steganografi. Data atau informasi dapat disembunyikan melalui beberapa media seperti video digital, teks digital, gambar digital, dan video digital.



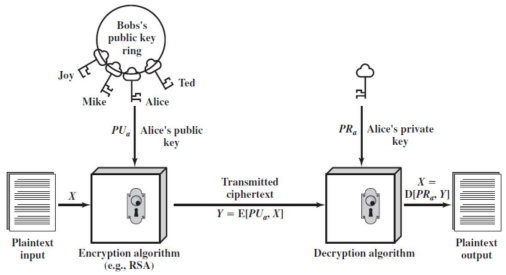
Gambar 1. Kategori Kriptografi dan Steganografi [3]

enggambarkan kualitas steganografi termasuk undetecability (impercetibility), robustness, dan kapasitas muatan [5]. Berdasarkan [6] steganografi menggunakan algoritma XOR dapat memberikan kapasitas tinggi. Selain itu, algoritma XOR dapat diterapkan untuk steganografi karena mudah diterapkan. Dalam penelitian ini, keamanan data teks dilakukan di mana teks akan dienkripsi dengan RSA, kemudian steganografi dilakukan melalui media gambar menggunakan algoritma XOR.

Tinjauan Pustaka

Algoritma RSA

Algoritma ini dikembangkan oleh Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1977 [7-9]. RSA adalah salah satu algoritma yang termasuk dalam kriptografi kunci asimetris dan merupakan algoritma yang paling populer. Gambar 2 menunjukkan bagaimana kunci asimetris bekerja dengan kunci publik dan kunci pribadi. Kriptografi asimetris menghasilkan sepasang kunci (kunci privat dan kunci publik). Kunci publik digunakan untuk proses enkripsi dan semua orang mungkin tahu. Kunci pribadi digunakan untuk mendekripsi ciphertext untuk mendapatkan plaintext. Kunci pribadi ini dikenal oleh penerima. Tingkat keamanan RSA terletak pada sulitnya memfaktorkan jumlah besar menjadi faktor utama [10].



Gambar 2. Proses enkripsi dan dekripsi dengan kunci asimetris

Algoritma RSA dimulai dari pembangkitan sepasang kunci yaitu kunci public key dan private key. Public key yang telah terbentuk akan digunakan pada proses enkripsi. Sedangkan private key akan digunakan penerima untuk proses dekripsi pesan. Formula lengkap algoritma RSA dapat dilihat pada gambar 3.

Pembangkitan Kunci

1. Pilih angka random prima yang besar p dan q
2. Hitung n=p.q
3. Hitung m=(p-1)(q-1)
4. Hitung kunci enkripsi e
   Dimana 1<e<m dan gcd(e,m)=1
5. Tentukan kunci dekripsi
   e.d=1 mod m dimana 0≤d≤n
6. Public key KU={e,n}
7. Private key KR={d,n}

Enkripsi	**Dekripsi**
$C = M^e mod\ n$ (M < n)	$M = C^d mod\ n$

Gambar 3. Algoritma RSA

Algoritma XOR

Pada penelitian ini, algoritma XOR digunakan untuk proses steganografi atau penyembunyian pesan melalui media gambar. Pesan disembunyikan dalam media gambar grayscale. 3 bit terakhir dari piksel gambar akan disematkan data atau pesan rahasia, namun pesan rahasia tersebut harus diubah ke dalam bentuk biner terlebih dahulu. Proses penyematan ketiga bit antara piksel gambar dan bit karakter menggunakan XOR.

Misalkan sebuah pesan rahasia yang telah dikonversi ke dalam biner adalah 101 dan piksel gambar 1000010. Maka ambil 3 bit terakhir dari piksel dan kemudian di-XOR-kan.

Bit piksel gambar asli : 1000010

Bit teks : 101

Bit piksel gambar Stego : 1000111

Sedangkan untuk proses ekstraksi gambar dilakukan juga proses XOR antara bit piksel gambar stego dan bit gambar asli. Ilustrasinya adalah sebagai berikut :

Bit piksel gambar asli : 1000010

Bit piksel gambar Stego : 1000111

Bit teks : 101

Data

Data yang digunakan dalam proses kriptografi merupakan suatu teks dengan ukuran 86, 181, 200, 400, 600, dan 1000 byte. Sedangkan media gambar yang digunakan untuk menyembunyikan pesan ada 2 contoh yaitu adel.png dan street.png

Gambar asli		Pesan (byte)
		86
		181
		200
		400
		600
adel.png	street.png	1000

I. Metodologi

Penelitian ini merupakan kombinasi algoritma RSA dan XOR. Algoritma RSA digunakan untuk mengenkripsi teks atau pesan rahasia. Algoritma XOR memiliki peran untuk menyembunyikan pesan terenkripsi pada media gambar. Skema penelitian ini dibagi dalam 2 proses seperti skema enkripsi dan skema ekstraksi. Gambar 4 menunjukkan skema enkripsi dan gambar 5 menunjukkan skema ekstraksi.

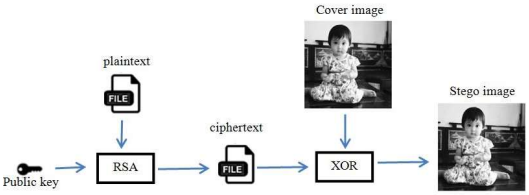
Skema Enkripsi

Tahapan skema enkripsi adalah sebagai berikut :

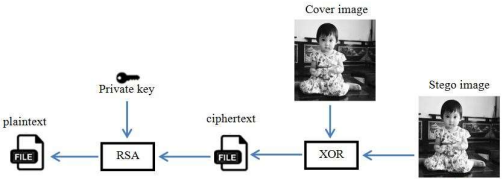
1. Plaintext (pesan rahasia) dienkripsi dengan algoritma RSA menjadi ciphertext.
2. Ciphertext akan disembunyikan ke dalam gambar asli dengan algoritma XOR. Hasil dari proses ini adalah stego image.

Skema Ekstraksi

1. Ulangi operasi algoritma XOR antara gambar stego dan gambar asli sehingga bisa didapatkan ciphertext
2. Ciphertext dapat didekripsi dengan RSA dan hasilnya adalah plaintext.



Gambar 4. Skema enkripsi



Gambar 5. Proses ekstraksi

Untuk mengukur kualitas hasil steganografi pada penelitian ini maka dihitung nilai dari MSE (Mean Square Error), Peak Signal To noise Ratio (PSNR), running time, dan histogram.

Mean Square Error (MSE)

Mean square error mengukur rata-rata dari kesalahan yang terjadi kemudian dikuadratkan [16]. Untuk steganografi yang diterapkan pada gambar, MSE dihitung berdasarkan perbedaan pada gambar asli dan stego image. Semakin kecil nilai MSE maka stego image semakin mendekati gambar aslinya [17].

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(p(i,j)-q(i,j))^2}{r*c} \quad (1)$$

Peak Signal to Noise Ratio

Dari nilai MSE yang didapat, bisa dihitung nilai PSNR. Stego image dengan kualitas yang bagus memiliki nilai PSNR lebih dari 40dB.

$$PSNR = 10\ log\frac{255^2}{\sqrt{MSE}} \quad (2)$$

II. Hasil dan Pembahasan

Salah satu hal penting tentang kriptografi adalah *running time. Running time* yang lebih cepat juga diperlukan untuk enkripsi dan dekripsi. Waktu proses enkripsi dan dekripsi akan menunjukkan kecepatan perhitungan proses kriptografi. Tabel 1 dan tabel 2 menunjukkan waktu berjalan skema enkripsi dan skema ekstraksi dengan ukuran pesan dan gambar yang berbeda.

Tabel 1. Pengukuran *Running Time* (Enkripsi)

		Skema Enkripsi		Skema Ekstraksi	
Cover Image	Pesan (byte)	Enkripsi RSA (detik)	Stegano (detik)	Ekstraksi stegano (detik)	Dekripsi RSA (detik)
adel	86	0.1930	0.0981	0.2588	0.239999
	181	0.4007	0.1032	0.3918	0.551113
	200	0.6123	0.1019	0.5188	0.616093
	400	0.9201	0.1007	0.9392	1.250849
	600	1.4127	0.0987	1.3745	1.838554
	1000	2.3962	0.0994	2.4527	3.365040
street	86	0.1990	0.1217	0.2147	0.244058
	181	0.2012	0.0871	0.3829	0.557246
	200	0.6012	0.0998	0.9514	0.621646
	400	0.9189	0.0759	1.9921	1.218690
	600	1.3225	0.0718	2.3545	1.883092
	1000	2.3765	0.0897	3.7425	3.185787
	Rata-rata	1.2633	0.09567	1.297825	1.214347
	Total	1.35897		2.512172	

Tabel 2. Pengukuran *Running Time* (Ekstraksi)

		Skema Enkripsi		Skema Ekstraksi	
Cover Image	Pesan (byte)	Enkripsi RSA (detik)	Stegano (detik)	Ekstraksi stegano (detik)	Dekripsi RSA (detik)
adel	86	0.1930	0.0981	0.2588	0.239999
	181	0.4007	0.1032	0.3918	0.551113
	200	0.6123	0.1019	0.5188	0.616093
	400	0.9201	0.1007	0.9392	1.250849
	600	1.4127	0.0987	1.3745	1.838554
	1000	2.3962	0.0994	2.4527	3.365040
street	86	0.1990	0.1217	0.2147	0.244058
	181	0.2012	0.0871	0.3829	0.557246
	200	0.6012	0.0998	0.9514	0.621646
	400	0.9189	0.0759	1.9921	1.218690
	600	1.3225	0.0718	2.3545	1.883092
	1000	2.3765	0.0897	3.7425	3.185787
	Rata-rata	1.2633	0.09567	1.297825	1.214347
	Total	1.35897		2.512172	

Tabel 1 menunjukkan hubungan antara ukuran pesan dan persyaratan waktu untuk skema enkripsi (enkripsi RSA & Stegano) dan skema ekstraksi (ekstrak stego & dekripsi RSA). Hasil menunjukkan bahwa waktu

berjalan tergantung pada ukuran pesan. Ukuran pesan yang lebih besar dapat mencapai waktu berjalan yang lebih besar.

Kualitas hasil steganografi dapat diukur dengan MSE dan PSNR. Parameter kualitas pertama adalah MSE. MSE dilakukan dengan membandingkan setiap piksel antara gambar asli dan gambar stego. Ketika nilai MSE kecil, hasil gambar stego semakin mirip dengan gambar asli. Dari tabel 2, nilai rata-rata MSE yang dihasilkan adalah 0,8768. Nilai MSE sangat kecil dan menunjukkan bahwa metode ini dapat menghasilkan gambar stego seperti gambar asli. Parameter kualitas kedua adalah PSNR. Hasil tes menunjukkan nilai PSNR rata-rata 50,1588. Nilai ini di atas nilai standar rata-rata kualitas steganografi minimum yang baik yaitu di atas 40dB.

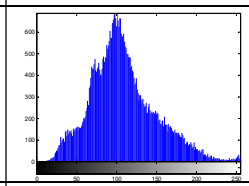
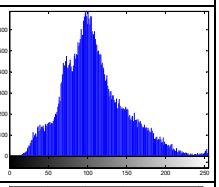
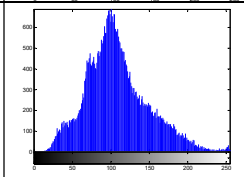
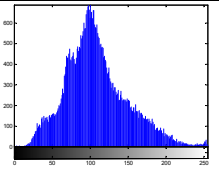
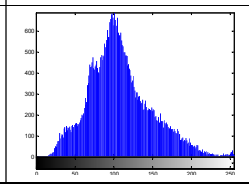
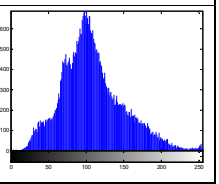
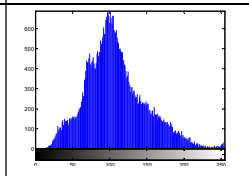
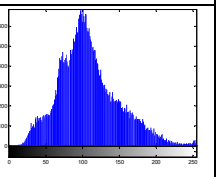
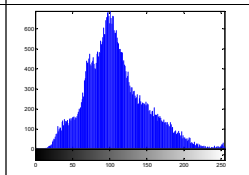
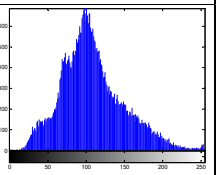
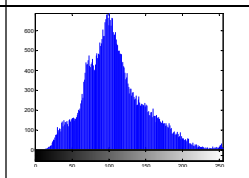
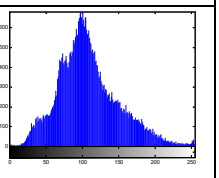
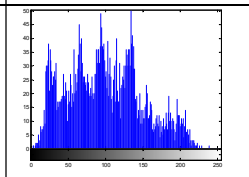
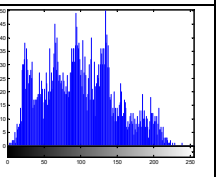
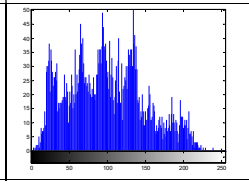
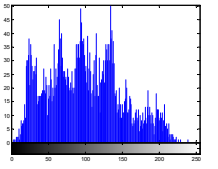
Berdasarkan tabel 3, kita dapat menyimpulkan bahwa hanya beberapa perbedaan piksel antara gambar asli dan gambar stego. Dengan media gambar dan ukuran file yang berbeda-beda, metode ini dapat memberikan sedikit perbedaan pada histogram. Perbedaan histogram yang kecil atau hampir mirip seperti gambar asli, dapat memperkuat keamanan data karena gambar yang diterima hampir mirp seperti gambar asli. Sehingga ketika ada penyusup, akan mengira bahwa ini hanya gambar biasa dan tidak menyadari bahwa ada pesan yang disisipkan ke dalam gambar tersebut.

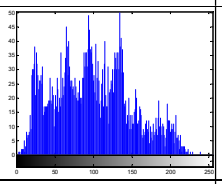
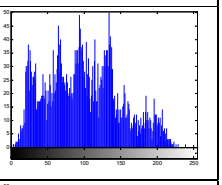
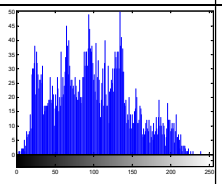
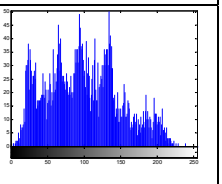
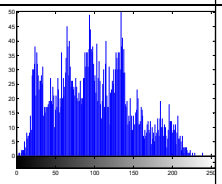
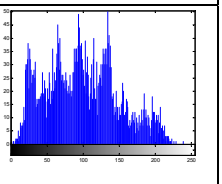
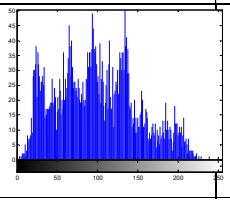
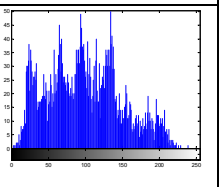
Tabel 2. Pengukuran Kualitas Steganografi

Cover Image	Pesan (byte)	MSE	PSNR (dB)
adel	86	1.421	45.6701
	181	1.4129	45.1267
	200	1.4762	45.7812
	400	1.4666	45.5066
	600	1.4291	45.6511
	1000	1.4164	45.6771
street	86	0.09	58.8059
	181	0.09	58.80
	200	0.12	57.3083
	400	0.32	53.0486
	600	0.48	51.3791
	1000	0.8	49.1514
Rata-rata		0.8768	50.1588

Ukuran pesan yang disisipkan bervariasi mulai 86 byte sampai 1000 byte dan metode ini berhasil menyematkan data teks sampai 1000 byte. Sehingga metode ini juga dapat meningkatkan kapasitas muatan pesan yang dapat disematkan pada gambar. Secara keseluruhan, metode yang diusulkan ini menghasilkan citra stego yang bagus.

Tabel 3. Histogram

Pesan (byte)	(street.png)	Stego image
86		
181		
200		
400		
600		
1000		
86		
181		

Pesan (byte)	(street.png)	Stego image
200		
400		
600		
1000		

III. Kesimpulan

Penelitian ini menggabungkan kriptografi dan steganografi antara algoritma RSA dan XOR, menghasilkan steganografi yang baik dengan evaluasi kualitas. Kualitas hasil steganografi dievaluasi oleh MSE dan PSNR. MSE rata-rata mencapai 0,8768 dan PSNR mencapai 50,1588. Histogram antara gambar asli dan gambar stego tidak ada perbedaan dari visualisasi manusia. Hasil kualitas gambar ini membuktikan bahwa metode yang diusulkan dapat menghasilkan steganografi yang baik.

IV. Daftar Pustaka

[1] Pooja R, Preeti S. Cryptography Using Image Steganography. International Journal of Computer Science and Mobile Computing. 2016; 5(7):451-456.

[2] Varsha, Rajender SC. Data Hiding Using Steganography and Cryptography. International Journal of Computer Science and Mobile Computing. 2015; 4(4):802-805.

[3] Nedhal AM. Hybrid Medical Colored Image LSB Steganography Based on Primitive Root Numbers. International Journal of Computer Science and Network Security. 2017;17(2).

[4] Yogesh K, Rajiv M, Harsh S, Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures. International Journal of Computer Science and Management Studies. 2011; 11(3).

[5] Nagham H, Abid Y, Badlislah A, Osamah MA. Image Steganography Techniques : An Overview. International Journal of Computer Science and Security. 2012; 6(3).

[6] Rohit S, Anuj KA, Singh. Data Security by (Information XOR Image) Along with High Capacity Encryption to overcome Steganography. International Journal of Computational Intelligence Research. 2015; 11(1):27-36.

[7] R. Bhaskar, G. Hehde, and P.R. Vaya. An Efficient hardware model for RSA encryption sistem using Vedic mathematics. Procedia Engineering 30. 2012: 124-128.

[8] A. Berzati, C. Canovas-Dumas, L. and Goubin. A Survey of Differential Fault Analysis against Classical RSA Implementation. Fault Analysis in Cryptography. Springer. 2012:111-124.

[9] C. Aumuller, P. Bier, W. Fischer, et al. Fault Attacks on RSA with CRT : Concrete Results and Practical Countermeasures. International Workshop on Cryptographic Hardware and Embedded Systems. Springer. 2001.

[10] J. H. Hong and C. W. Wu. Rsa Public Key Crypto-processor core Design and Hierarchical System Test Using IEEE 1149 Family. National Tsing-Hua University, Taiwan, Doctoral dissertation. 2000

[14] William S. Crypto and Network Security : Priciples and Practice, 5th Edition, Prentice Hall.2010.

[15] N. Dhawale. Impementation of Huffman Algorithm and Study for Optimization. In:2014 International Conference on Advances in Communication and Computing Technologies. IEEE. 2014:1-6

[16] A. Sarkar and S. Karforma. Image Steganography using Password Based Encryption Technique to Secure e-Banking Data. International Journal of

Applied Engineering Research. Vol.13, No.22. 2018:15477-15483.

[17] Farahani MRD, Pourmohammad A. A DWT Based Perfect Secure and High Capacity Image Steganography Method. In: 2013 International Conference on Parallel and Distributed Computing, Applications and Technologies. IEEE. 2013: 314–317.

[18] Setiadi DRIM, Jumanto J. An enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel edge detection. Cybern Inf Technol. 2018; 18(2): 74–88.

[19] Memon F.,Unar A,M. and Memon S.,"Image Quality Assessment for Performance Evaluation of Focus Measure Operators",MURJET, Vol. 34, No. 4, October 2015.