Kombinasi RSA-CRT dengan Random LSB untuk Keamanan Data di Kanwil Kementerian Agama Prov. Sumatera Utara

Niti Ravika Nasution
Kantor Wilayah Kementerian Agama Provinsi Sumatera Utara
Jl. Jend. Gatot Subroto No.261 Medan
nityravika@gmail.com[1], nitiravika@kemenag.go.id[2]

Abstract

In this study the authors use Cryptographic Algorithms Rivest Shamir Adleman Chinese Remainder Theorem (RSA-CRT) and steganography technique Random Least Significant Bits (LSB). RSA-CRT is basically the same as usual, but utilizing RSA CRT theorem to shorten the bit size decryption exponent d by hiding d on congruent systems that accelerate time decryption, the difference in the key generation process and the decryption process. Cryptographic algorithm RSA-CRT produce ciphertext stored into a picture (image) using Steganography technique Random Least Significant Bits (LSB). The workings of Random LSB is storing the message (ciphertext) in the first bit or the second bit random key for use random number generator Pseudo Random Number Generator (PRNG) with Linear Congruential Generator (LCG) method. Ciphertext stored in a picture (image) has extracted key re-use random number generator at the time of inserting the message. Then the ciphertext is decrypted back by the algorithm RSA-CRT to produce the original text (plaintext). Merging Cryptographic Algorithm RSA-CRT with Steganography Technique Simple LSB than with Random LSB generate higher PSNR and MSE is lower, which means better level of data security and more resistant to attack. Has more difficult to find a secret message by cryptanalysis and steganalyst.

Keywords: *Cryptographic RSA-CRT, steganography random LSB, Pseudo Random Number Generator (PRNG), Linear Congruential Generator (LCG) PSNR MSE, Ministry/Institution*

1. PENDAHULUAN

Teknologi jaringan komputer yang saat ini berkembang memungkinkan satu komputer dapat terhubung dengan komputer lainnya dibelahan dunia ini untuk saling berbagi data dan informasi. Keterhubungan ini akan menjadi persoalan dalam masalah keamanan setiap melakukan transaksi atau pertukaran data dan informasi pada Kementerian/Lembaga khususnya di Kanwil Kementerian Agama Provinsi Sumatera Utara.

Pengiriman maupun penyimpanan data melalui internet terasa cukup banyak dilakukan orang saat ini seperti mengirim email dan penggunaan aplikasi berbasis web yang sudah banyak tersedia di media internet. Kanwil Kemenag Prov.Sumatera Utara dalam hal ini sering melakukan pengiriman data atau informasi ke Kantor Kementerian Agama Pusat maupun ke Kantor Kemenag Kab./Kota jajaran dibawahnya melalui email maupun aplikasi berbasis web lainnya terkadang bersifat rahasia sehingga keamanan data tersebut sangat penting untuk terjaga kerahasiaan data yang dikirim agar aman dari gangguan orang yang tidak bertanggung jawab atau orang yang tidak berhak mengakses data tersebut.

Keamanan pada suatu data atau informasi pada saat ini dapat dibagi menjadi dua metode yakni Kriptografi dan Steganografi. Dari dua metode tersebut, metode yang satu dapat menjadi tambahan dan peningkatan bagi metode yang lain.

Kriptografi adalah seni mengacak informasi atau data yang memiliki makna, menjadi sesuatu yang tidak dapat dipahami atau seolah-olah tidak berarti. Dalam konteks lain, Kriptografi adalah studi teknik matematika yang berkaitan dengan aspek keamanan informasi, seperti kerahasiaan data, keaslian data, integritas data, dan otentikasi data (Buchmann, 2004). Meski menyembunyikan pesan dengan kriptografi dapat meminimalkan risiko keamanan, namun masih ada celah yang bisa dilihat oleh pesan pencuri dalam pesan rahasia.Salah satunya adalah pesan rahasia yang dibuat umumnya

tidak bisa dibaca secara normal sehingga menimbulkan kecurigaan. Karena itu, manusia kembali mengembangkan cara untuk menyembunyikan pesan yang bisa menghilangkan kelemahan tersebut. Akhirnya manusia menemukan ilmu baru, yaitu steganografi.

Berbeda dengan kriptografi, steganografi adalah seni menyembunyikan data, dimana data disembunyikan menjadi media yang terlihat biasa. Media informasi yang umum dipakai adalah media gambar atau citra. Sehingga untuk melakukan penyembunyian pesan ke suatu gambar tidak akan menimbulkan banyak perhatian dari pihak-pihak yang tidak dikehendaki (Wayner, 2009). Dengan ditemukannya steganografi, bukan berarti pengiriman pesan menjadi aman sepenuhnya.Meskipun memiliki kelebihan dibandingkan kriptografi, steganografi pun memiliki kelemahan. Oleh karena itu, pengirim pesan harus mempertimbangkan berbagai aspek dalam mengamankan pesannya dan mempertimbangkan metode apa yang sebaiknya digunakan dalammengamankan pesan atau data.

Untuk melindungi masalah keamanan data atau informasi tersebut diatas digunakan penyandian atau kriptografi yang diberi nama teknik penyandian RSA seperti teknik dasar kriptografi, konsep kriptografi kunci publik dan algoritma RSA. RSA diambil dari penemunya yaitu Ron *Rivest*, Adi *Shamir* and Leonard *Adleman* (1976) dari MIT (*Massachussets Institute of Technology*). Algoritma ini dipatenkan pada tahun 1983 di Amerika Serikat (Stallings, 2005), merupakan algoritma kriptografi kunci publik pertama dan populer karena kehandalannya dalam proses enkripsi. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar, oleh karena alasan itu RSA dianggap aman untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar.Sistem Kriptografi RSA dapat dimodifikasi dengan menggunakan teorema *Chinese Remainder Theorem* (CRT) disebut dengan RSA-CRT. Pada dasarnya RSA-CRT sama dengan RSA biasa namun memanfaatkan teorema CRT untuk memperpendek ukuran bit dan terbukti sistem kriptografi RSA-CRT memiliki waktu komputasi yang lebih singkat daripada sistem kriptografi RSA biasa yaitu sekitar 4 kali lebih cepat.

Berbagai macam teknik steganografi digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah Random Least Significant Bit. Prinsip dasar yang digunakan didalam penyisipan teknik steganografi *Random* LSB hampir sama dengan teknik steganografi LSB. Dimana metode LSB ini bekerja dengan cara menggantikan bit terakhir dari masing-masing *pixel* dengan pesan yang akan disisipkan. Sedikit berbeda dengan Metode *Random* LSB dimana pergantian bit bukan pada bit terakhir saja melainkan dilakukan secara acak bisa pada bit pertama maupun bit kedua sehingga posisi penyembunyian pesan di dalam bit sulit untuk ditebak. Karena pada gambar digital perubahan satu-dua bit pada setiap *pixel* tidak akan berpengaruh pada kontras dan kualitas gambar sehingga tidak akan menimbulkan kecurigaan yang berarti apabila dilihat oleh mata telanjang bahwa gambar tersebut telah disisipi pesan.

Pada penelitian ini penulis tertarik untuk melakukan pengembangan dengan menggunakan dua metode ini yakni mengkombinasikan Kriptografi dan Steganografi dengan Algoritma Kriptografi *Rivest Shamir AdlemanChinese Remainder Theorem* (RSA-CRT) untuk sistem kemanan data melalui enkripsi dengan Teknik Steganografi *Random Least Significant Bits* (LSB) sehingga efektifitas keamanan data lebih ditingkatkan dan terjaga.

2. METODE PENELITIAN

Pada penelitian ini dilakukan penggabungan dari kombinasi Algoritma Kriptografi *Rivest Shamir Adleman Chinese Remainder Theorem* (RSA-CRT) dengan Teknik Steganografi *Random Least Significant Bits* (LSB) sehingga dihasilkan pengembangan dari penggabungan kedua teknik keamanan data tersebut. Dan penulis merancang konsep penggabungan dari algoritma RSA-CRT dengan Teknik Steganografi *Random* LSB sehingga dapat lebih meningkatkan keamanan data dan ketahanan terhadap serangan.

2.1 Analisis Algoritma

Dalam penelitian ini digunakan Algoritma Kriptografi RSA-CRT dan Teknik Steganografi *Random* LSB untuk merancang aplikasi keamanan data, dan terlebih dahulu dilakukan analisis terhadap algoritma-algoritma yang digunakan dalam perancangan sistem keamanan data ini. Adapun algoritma-algoritma yang akan dianalisis adalah Algoritma RSA-CRT, Algoritma Pembangkit Kunci

RSA-CRT, Algoritma Enkripsi RSA-CRT, Algoritma Dekripsi RSA-CRT dan Algoritma Teknik Steganografi *Random* LSB.

2.1.1 Analisis Algoritma RSA-CRT

Sistem kriptografi RSA dapat dimodifikasi dengan menggunakan teorema CRT disebut dengan RSA-CRT. Terbukti sistem kriptografi RSA-CRT memiliki waktu komputasi yang lebih singkat dari pada sistem kriptografi RSA biasa, yaitu sekitar 4 kali lebih cepat. Proses dan cara kerja Algoritma RSA-CRT dapat dilihat sebagai berikut:

1. Membangkitkan bilangan prima besar *p* dan *q*.
2. Melakukan perhitungan $n = p*q$.
3. Melakukan perhitungan nilai *totient* $\varphi(n) = (p-1)(q-1)$.
4. Menentukan nilai kunci enkripsi*e*dengan syarat bahwa bilangan tersebut merupakan bilangan bulat$e \xleftarrow{R} Z_{\varphi(n)}$ dengan $\gcd(e,\varphi(n)) = 1$.
5. Menghitung kunci enkripsi yang dilakukan dengan perhitungan kunci dekripsi dengan rumus$d \equiv e^{-1}$pada $Z_{\varphi(n)}$
6. Eksponen dekripsi (d) tidak secara langsung diberikan pada kunci privat namun dapat dihitung melalui parameterdP, dQ dan qInv yang memiliki ukuran setengah panjang bit d.
7. Rumus untuk parameterdP = $d \bmod (p-1)$
8. Rumus untuk parameterdQ = $d \bmod (q-1)$
9. Rumus untuk parameterqInv = q^{-1} pada Z_p
10. Setelah dihitung parameter tersebut maka diperoleh$K_{publik} = (e.n)$ dan $K_{privat} = (dP, dQ, qInv, p, q)$
11. Rumus untuk melakukan proses enkripsi adalah$C = P^e \bmod n$
12. Sebelum dilakukan proses dekripsi terlebih dahulu ditentukan rumus$m_1 = C^{dP} \bmod p$, $m2 = C^{dQ} \bmod q$dan$h$ = qInv.$(m1-m2) \bmod p$
13. Maka dapat dilakukan proses dekripsi dengan rumus adalah$P = m_2 + h.q$

2.1.2 Analisis Penyisipan Pesan Random LSB

Pada penelitian ini penulis menggunakan teknik steganografi *random* LSB dalam penyisipan pesan rahasia. Dimana bit LSB yang dipakai untuk menampung bit data tidak selalu LSB bit pertama, tetapi juga memakai LSB bit kedua, sehingga steganalisis lebih sukar menebak apakah pesan yang disisipkan secara acak ada pada bit pertama atau pada bit kedua. Karena berbeda dengan LSB biasa yang selalu menyisipkan pesan pada bit pertama. Penerapan metode ini dilakukan bersamaan dengan pembangkitan angka random dari sebuah fungsi *random generator* sebagai acuan untuk penyisipan.

Prosedur penyembunyian data menggunakan bit LSB yang berbeda (*random LSB*) adalah sebagai berikut:

1. Bangkitkan *p*(*pseudo random number*)
2. Lakukan proses penyembunyian dengan cara menyisipkan 1 bit data dengan aturan seperti berikut:
   a. jika p adalah bilangan ganjil, sisipkan 1 bit data b pada LSB (bit pertama)
   b. jika p adalah bilangan genap, sisipkan 1 bit data b pada LSB (bit kedua)

   Untuk membangkitkan angka-angka random, digunakan sebuah fungsi pembangkit bilangan acak *Pseudo Random Generator Number* (PRNG) dengan rumus :

$$X_n = (aX_{n-1} + c) \bmod m \qquad (1)$$

Pembangkit bilangan acak seperti ini disebut *Linear Congruential Generator* (LCG).Dimana :

- Terjadi pengulangan pada periode tertentu atau setelah sekian kali pembangkitan, hal ini adalah salah satu sifat dari pembangkitan metode PRNG pada umumnya.
- LCG mempunyai periode tidak lebih besar dari m
- LCG mempunyai periode penuh (m-1) jika memenuhi syarat berikut :
  - c relatif prima terhadap m
  - a-1 dapat dibagi dengan semua faktor prima dari m
  - a-1 adalah kelipatan 4 jika m adalah kelipatan 4
  - $m > \max(a, c, X_0)$
  - a dan $c > 0$

Algoritma penyisipan *random* LSB:

```
for i = 1...,l(c) do
si ← ci
end for
generate random sequence
ki using seed k
n ← k1
for i = 1,...,l(m) do
sn ← cn mi
n ← n + ki
end for
```

Contoh Proses *Random* LSB

Ciphertext = 2942
Diubah ke Biner = 101101111110
CitraM x N = 6 x 6

*Pixel*1	*Pixel*2	*Pixel*3	*Pixel*4	*Pixel*5	*Pixel*6
*Pixel*7	*Pixel*8	*Pixel*9	*Pixel*10	*Pixel*11	*Pixel*12
*Pixel*13	*Pixel*14	*Pixel*15	*Pixel*16	*Pixel*17	*Pixel*18
*Pixel*19	*Pixel*20	*Pixel*21	*Pixel*22	*Pixel*23	*Pixel*24
*Pixel*25	*Pixel*26	*Pixel*27	*Pixel*28	*Pixel*29	*Pixel*30
*Pixel*31	*Pixel*32	*Pixel*33	*Pixel*34	*Pixel*35	*Pixel*36

Gambar 1. Ilustrasi Pixel citra M x N

RGB

*Pixel*1 → R = 245 G = 163 B = 113
*Pixel*2 → R = 245 G = 188 B = 113
*Pixel*3 → R = 245 G = 210 B = 113
*Pixel*4 → R = 245 G = 236 B = 113
*Pixel*5 → R = 236 G = 245 B = 113
*Pixel*6 → R = 214 G = 245 B = 113

Konversi Biner ke *Pixel*

*Pixel*1 → R = 11110101 G = 10100011 B = 01110001
*Pixel*2 → R = 11110101 G = 10111100 B = 01110001
*Pixel*3 → R = 11110101 G = 11010010 B = 01110001
*Pixel*4 → R = 11110101 G = 11101100 B = 01110001
*Pixel*5 → R = 11101100 G = 11110101 B = 01110001
*Pixel*6 → R = 11010110 G = 11110101 B = 01110001

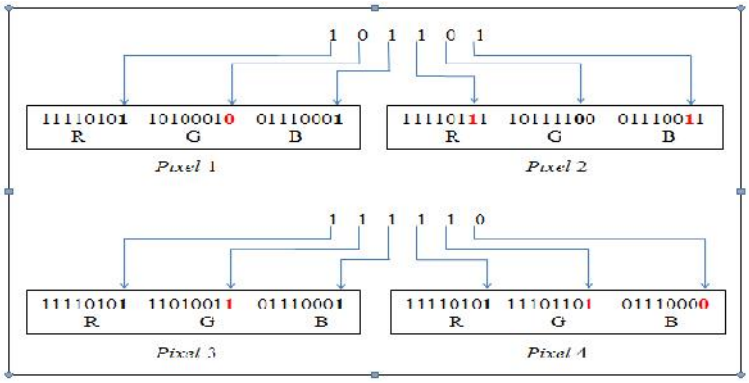
Pembangkit kunci acak dengan rumus

$$X_n = (7X_{n-1} + 11) \bmod 17 \qquad (2)$$

Membangkitkan bilangan acak sebanyak 16 kali dengan
X(0)=3

$X_{(1)}$ = (7(3)+11) mod 17 = 15 (odd)
$X_{(2)}$ = (7(15)+11) mod 17= 14 (even)
$X_{(3)}$ = (7(14)+11) mod 17= 7 (odd)
$X_{(4)}$ = (7(7)+11) mod 17 = 9 (odd)
.....

Proses penyisipan *chipertext* ke gambar (citra) dengan Teknik *Random* LSB
Pesan *chipertext* yang akan disisipi adalah 101101111110



Gambar 2. Ilustrasi Penyisipan Pesan ke Dalam *Pixel* Gambar

2.1.3 Analisis Teknik Pengungkapan Pesan (Ekstraksi) Random LSB

Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (*reveal* atau*extraction*). Posisi penyimpanan bit data di dalam *byte* dapat diketahuidari bilangan acak yang dibangkitkanoleh PRNG (*(pseudo random number generator)*. Bilangan acak yang dihasilkan sama dengan bilangan acak yang dipakai pada waktu penyembunyian data. Dengan demikian, bit-bit data rahasia yang terdapat di setiap *byte* di dalam citra dapat dikumpulkan kembali.

Algoritma proses ekstraksi:

```
generate random sequence kᵢ
using seed k
n ← k₁
for i = 1,...,l(m) do
mᵢ ← LSB(cₙ)
n ← n + kᵢ
end for
```

2.2 Perancangan Sistem Keamanan Data

Langkah-langkah dalam rancangan proses enkripsi, dekripsi dan ekstraksi sebagai berikut :

1. Menginput pesan teks berupa *Plaintext* dalam bentuk ASCII, dimana panjang teks yang diinput ditentukan besarannya.
2. Menentukan kunci publik yang telah disepakati terlebih dahulu oleh pengirim dan penerima pesan menggunakan Algoritma Kriptografi RSA-CRT.
3. Melakukan proses enkripsi, dimana pesan teks berupa *Plaintext* diubah menjadi pesan acak *Chipertext*.
4. Select the image file (cover image) that is larger than the ciphertext message.
5. *Chipertext* dalam bentuk ASCII diubah ke dalam bentuk biner begitu juga pixel gambar diubah ke dalam bentuk biner untuk bisa dilakukan penyisipan pesan.Proses selanjutnya melakukan penyisipan pesan chipertext ke dalam file gambar (*cover image*) menggunakan Teknik Steganografi *Random* LSB, dimana penyisipan pesan tidak hanya dilakukan pada bit pertama melainkan juga pada bit kedua secara acak dengan menggunkan pembangkit kunci acak *Pseudo Random Number Generator* (PRNG) dengan metode *Linear Congruential Generator* (LCG) sehingga menghasilakan gambar yang telah tersisipi pesan (*stego image*).
6. Pada proses selanjutnya data yang diterima oleh penerima berupa hasil enkripsi (*chipertext*) akan dikeluarkan kembali dari file gambar (*stego image*) melalui proses ekstraksi dengan menggunakan pembangkit bilangan acak yang sama pada saat penyisipan pesan yaitu *Pseudo Random NumberGenerator* (PRNG) dengan metode *Linear Congruential Generator* (LCG) dan melalui proses dekripsi data asli berupa pesan teks akan diterima. Sehingga pesan acak dari *chipertext*

kembali seperti semula dalam bentuk *Plaintext* dengan demikian si penerima pesan memperoleh data atau informasi yang diinginkannya dengan aman.

Kelebihan dan Kelemahan dari RSA-CRT

1. Tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor primanya, dalam hal ini tingkat kesulitan dalam memfaktorkan *n* menjadi *p* dan *q*.
2. ketahanannya terhadap berbagai bentuk serangan, terutama serangan *brute force*. Hal ini dikarenakan kompleksitas dekripsinya yang dapat ditentukan secara dinamis dengan cara menentukan nilai *p* dan *q* yang besar pada saat proses pembangitkan pasangan kunci, sehingga dihasilakan sebuah *key space* yang cukup besar, sehingga tahan terhadap serangan.
3. Waktu komputasi lebih pendek dari RSA biasa empat kali lebih cepat.
4. Menghasilkan ciphertext lebih pendek dari RSA biasa.
5. Lebih mudah dalam pemahaman dan penerapannya.
6. Proses enkripsi sangat cepat, sederhana dan banyak digunakan oleh industri, perusahaan besar untuk menjaga keamanan data.

Kelebihan dan Kelemahan dari Random LSB

1. Metode ini bekerja dengan caramengganti bit bukan pada bit pertama saja melainkan juga pada bit kedua yang dilakukan secara random dengan menggunakan fungsi pembangkit bilangan acak.
2. Posisi *pixel*yang mengandung pesan rahasia dilakukan dengan *random* LSB antara bit pertama dan bit kedua sehingga steganalisis lebih sukar menebak penyembunyian pesan berada pada LSB keberapa.
3. Gambar yang telah disisipkan tidak kelihatan berbeda dengan gambar asli sebelum disisipi pesan karena hanya menyebabkan sedikit perubahan yang tidak dapat dideteksi oleh mata manusia.
4. Ukuran gambar tidak akan berubah dan setiap *pixel* bisa disisipi pesan.
5. Kelemahannya adalah pesan yang akan disisipkan terbatas sesuai dengan ukuran gambar apabila memuat pesan yang besar maka ukuran gambar juga harus dipilih yang lebih besar dari besarnya pesan.
6. Ukuran kunci privat yang terlalu besar akan menyebabkan proses dekripsi cukup lambat, terutama untuk ukuran pesan besar.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Implementasi

Algoritma kriptografi *Rivest Shamir AdlemanChinese Remainder Theorem* (RSA-CRT) dan teknik steganografi *Random Least Significant Bits* (LSB) telah diteliti pada penelitian ini.Hasil penelitian ini diimplementasikan menggunakan bahasa pemrograman sederhana bertujuan untuk memperjelas dan menguji keakuratan data hasil enkripsi, dekripsi, penyisipan pesan dan ektraksi pesan yang telah dianalisis oleh penulis. Dimana data tersebut sulit dihitung secara manual sehingga dibutuhkan perhitungan secara komputasi melalui program. Impelementasi ini dibuat dengan menggunakan bahasa Pemrograman Java.

3.2 Pembahasan

Dari hasil rancangan sistem keamanan data yang dibuat, diperoleh beberapa kelebihan yang penulis dapatkan dari aplikasi penggabungan antara kriptografi *Rivest Shamir AdlemanChinese Remainder Theorem* (RSA-CRT) dengan Teknik Steganografi *Random Least Significant Bits* (LSB), diantaranya gambar asli (*cover image*) dengan gambar tersisipi pesan (*stego image*) tidak memiliki perbedaan sedikitpun apabila dilihat dengan mata manusia. Karena perbedaan satu atau dua bit dengan ukuran bit yang sangat kecil tidak akan berpengaruh terhadap gambar yang telah tersisipi pesan dengan gambar aslinya. Berikut ini tampilan dari hasil gambar asli (*cover image*) dengan gambar tersisipi pesan (*stego image*).

Gambar 3. Gambar Asli

Gambar 4. Gambar Tersisipi Pesan

Kelebihan lain dari penggabungan kriptografi RSA-CRT dengan steganografi *random* LSB adalah keamanan pesan lebih terjaga dari pada hanya menggunakan satu kriptografi RSA-CRT maupun steganografi *random* LSB saja, sehingga kriptanalis maupun steganalis lebih sukar untuk mengambil (menguraikan) pesan tersembunyi tersebut.

Kemudian penulis melakukan perbandingan antara gabungan RSA-CRT *random* LSB dengan gabungan RSA *random* LSB untuk menentukan apakah gabungan RSA-CRT *random* LSB lebih cepat dalam hal kecepatan waktu akses , tingkat kemanan datanya maupun tingkat ketahanan terhadap serangan. Dapat diuji dari perbandingan untuk 5 citra yang berbeda dari tampilan di bawah ini :

Gambar 5. Nilai PSNR dan MSE untuk citra pelantikan

Gambar 6. Nilai PSNR dan MSE untuk citra Menag

Gambar 7. Nilai PSNR dan MSE untuk citra Gubernur

Gambar 8. Nilai PSNR dan MSE untuk citra Kanwil

Gambar 9. Nilai PSNR dan MSE untuk ASN

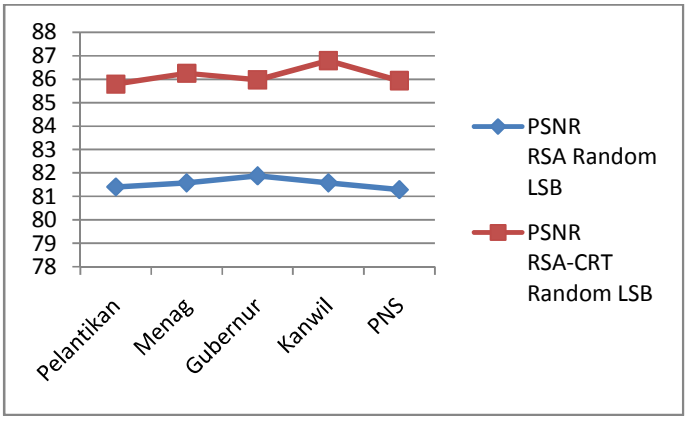
Dari pengujian ke lima citra diatas maka diperoleh kesimpulan bahwa penggabungan RSA-CRT *random* LSB lebih cepat dalam hal waktu akses, lebih tinggi nilai *Peak Signal to Noise Ratio* (PSNR) berarti lebih tinggi tingkat keamanan datanya dan lebih rendah nilai *Mean Square Error* (MSE) yang berarti lebih tinggi tingkat ketahanan terhadap serangan dari pada RSA *random* LSB. Berikut ini ditampilkan tabel perbedaan PSNR, MSE dan waktu akses untuk lima citra yang berbeda :

Table 1. Perbandingan nilai PSNR, MSE dan Waktu Akses

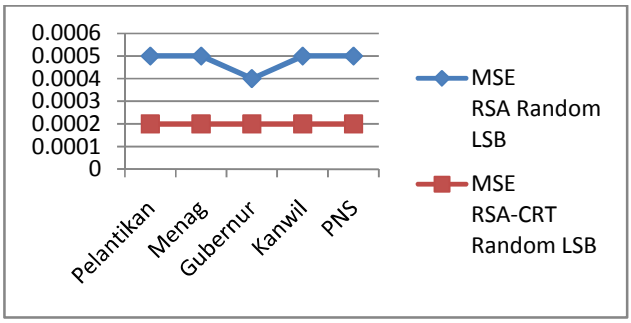
Image	RSA *Random* LSB			RSA-CRT *Random* LSB		
	PSNR	MSE	access time (second)	PSNR	MSE	access time (second)
Pelantikan	81,4061	0,0005	0,1528	85,7862	0,0002	0,0935
Menag	81,5811	0,0005	0,0120	86,2438	0,0002	0,0326
Gubernur	81,8798	0,0004	0,0163	85,9710	0,0002	0,0104
Kanwil	81,5811	0,0005	0,0101	86,7862	0,0002	0,0070
ASN	81,2888	0,0005	0,0032	85,9334	0,0002	0,0065

Keterangan:
1. Jika Nilai PSNR tinggi, maka semakin meningkat keamanan datanya
2. Jika Nilai MSE rendah, maka semakin meningkat ketahanan terhadap serangan

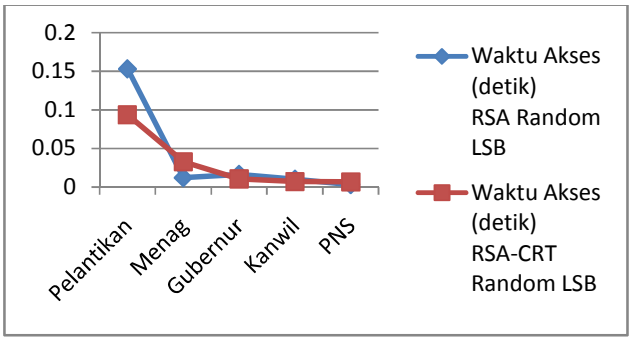
Berikut ini penulis tampilkan grafik perbandingan PSNR, MSE dan waktu akses antara RSA Random LSB dengan RSA-CRT random LSB :



Gambar 10. Grafik Perbandingan PSNR



Gambar 11. Grafik PerbandinganMSE



Gambar 12. Grafik Perbandingan Waktu Akses

Dari tabel di atas, jelas terlihat bahwa nilai PSNR dari gabungan RSA-CRT *random* LSB lebih tinggi dibandingkan nilai PSNR gabungan RSA *random* LSB yang berarti tingkat keamanan datanya lebih tinggi, kemudian nilai MSE dari gabungan RSA-CRT random LSB lebih rendah dibandingkan nilai PSNR gabungan RSA *random* LSB yang berarti tingkat ketahanan terhadap serangan lebih tinggi, dan diperoleh waktu akses yang lebih cepat dari gabungan RSA-CRT random LSB.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan hasil dan pembahasan, dapat ditarik kesimpulan sebagai berikut :

1. Dari pengembangan algoritma kriptografi RSA-CRT dengan teknik steganografi *random* LSB diperoleh hasil bahwa lebih tinggi tingkat keamanan datanya, lebih tahan terhadap serangan dan waktu akses lebih cepat dibandingkan penggabungan RSA *random* LSB.
2. Gambar yang telah tersisipi pesan (*stego image*) tidak jauh berbeda dengan gambar asli (*cover image*) apabila dilihat dengan mata manusia karena perbedaan satu atau dua bit tidak berpengaruh pada kualitas gambar.
3. Penggunaan algoritma kriptografi RSA-CRT lebih baik dari RSA biasa dikarenakan waktu komputasi lebih cepat karena dapat direduksi dengan mengimplementasikan *Chienese Remainder Theorem* (CRT).
4. Pembangkitan bilangan acak *Pseudo Random Number Generator* (PRNG) dengan metode *Linear Congruential Generator* (LCG) memiliki kelebihan dalam pengacakan bilangan namun memiliki kekurangan karena terjadi pengulangan bilangan acak pada periode tertentu.
5. Dengan adanya sistem informasi pengembangan algoritma RSA-CRT dengan teknik steganografi *Random* LSB meningkatkan keamanan data sehingga kerahasiaan data pada sebuah Lembaga/Kementeriaan dapat lebih optimal terjaga.

4.2 Saran

1. Pengembangan dapat ditingkatkan dengan mengunakan metode kriptografi maupun teknik steganografi lain.

2. Pengembangan algoritma kriptografi RSA-CRT dan teknik steganografi *random* LSB perlu dilanjutkan penelitiannya agar lebih baik dari segi keamanan, ketahanan terhadap serangan dan efesiensi waktunya.
3. Untuk pembangkitan bilangan acak perlu dikembangkan dengan metode lain agar pengacakannya lebih baik tanpa harus berulang pada periode tertentu.
4. Sebuah Lembaga/Kementerian sudah seharusnya memiliki sebuah sistem informasi keamanan data yang baik sehingga kerahasiaan data dapat terjaga dengan baik.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Muhammad Irwan Padli Nasution yang telah memberikan dukungan terhadap penelitian ini.

BAHAN REFERENSI

[1] Buchmann, J.A. 2004. *Introduction to Cryptography.* 2nd ed. New York. Springer.

[2]G.N.Shinde & H.S.Fadewar, 2008.*ICCES*, vol.5, no.4, pp.255-261.Faster RSA Algorithmfor DecryptionUsing Chinese Remainder Theorem.

[3]Gupta, S., Goyal, A.& Bhushan, B., 2012. Information Hiding Using Least Significant Bit Steganography and Cryptography, *I.J.Modern Education and Computer Science*, **6**, 27-34.*Published Online June 2012 in MECS* (http://www.mecs-press.org/). DOI: 10.5815/ijmecs.2012.06.04

[4] Hellman, M.E. 1987. An Overview of Public Key Cryptography, *IEEE Communication Society Magazine.*

[5] Johnson et al. 2012. Resilient Cryptographic Scheme, *United States Patent*.

[6] Kekre, H. B., Athawale, A.A, & Patki, S.A. 2011. Improved Steganalysis of LSB Matching Steganography Based on Counting Alteration. *ICWET '11: Proceeding s of the International Conference & Workshop on Emerging*.

[7] Laksito, W.Y.S, 2008. Modifikasi Least Significant Bit dalam Steganografi.*Indonesian Scientific Jurnal Database (ISJD). Database Jurnal Ilmiah Indonesia* ISSN : 1693 – 1173. Jakarta

[8] Mahajan, S., Singh, M. 2014. Performance Analysis of Efficient RSA Text Encryption Using NVIDIA CUDA-C and OpenCL. *ICONIAAC '14: Proceedings of the 2014 International Conference on Interdisciplinary*.

[9] Nasution, Muhammad Irwan Padli, 2008, Urgensi Keamanan Pada Sistem Informasi, *Jurnal Iqra' Volume 02 Nomor 02*, https://www.researchgate.net/publication/305726044_URGENSI_KEAMANAN_PADA_SISTEM_INFORMASI

[10] Rauzy P. & Guilley S. 2014.*Journal of Cryptographic Engineering*.A formal proof of countermeasures against fault injection attacks on CRT-RSA. September 2014, Volume 4, Issue 3, pp 173-185.

[11] Reddy, V.L, Subramanyam, A., & Reddy, P.C. 2012. Implementation of Least Significant Bit Steganography and Statistical Steganalysis. *CCSEIT '12: Proceedings of the Second International Conference on Computational*.

[12] Schmeh, K. 2003. *Cryptography and Public Key Infrastructure on the Internet.*West Sussex, John Wiley & Sons Ltd

[13] Schneier, B. 1996.*Applied Cryptography*.2nd Edition, John Wiley & Sons, Inc. Canada.

[14] Thangadurai, K., Sudha, D.V. 2014. An analysis of LSB Based Image Steganography Techniques.*Computer Communication and Informatics (ICCCI), International Conference on.IEEE Conference Publications*. Pages:1-4, DOI:10.1109.

[15] Wayner, P. 2009. *Disappearing Cryptography, – Information Hiding: Steganography & Watermaking*. 3rd ed. Burlington. Elsevier Inc.

[16] Wohlgemuth, S. 2002. IT-Security: Theory and Practice: *Steganography and Watermarking*, University of Freiburg, Denmark.