

# IMPLEMENTASI METODE STEGANOGRAFI LEAST SIGNIFICANT BIT DENGAN ALGORITMA RSA PADA CITRA BMP

**Muhammad Fajar Alamsyah**

Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro

Jl. Nakula I No. 5-11, Semarang, Jawa Tengah 50131 - (024) 3517261

E-mail : alamsyah\_gates@yahoo.com

---

## **Abstrak**

Salah satu bidang yang masih sering menjadi bahan penelitian dalam ilmu komputer untuk teknik keamanan data adalah steganografi LSB (Least Significant Bit). Penggunaan steganografi LSB tanpa dilengkapi sistem keamanan akan terpengaruh dari upaya untuk menghilangkan pesan yang akan disisipkan sehingga perlu dikembangkan dengan mengkombinasikan algoritma RSA. Implementasi metode steganografi LSB dengan algoritma RSA dapat meningkatkan keamanan pesan yang akan disisipkan. Pesan rahasia dienkripsi dengan algoritma RSA lalu disisipkan dalam citra digital. Penelitian ini bertujuan menganalisa kualitas citra hasil steganografi LSB yang telah dikombinasikan algoritma RSA dengan pengujian visual, PSNR dan pengujian ketahanan. Dari hasil pengujian visual citra hasil steganografi tidak mengalami perubahan jika dilihat secara kasat mata namun nilai PSNR yang didapatkan akan semakin menurun dengan bertambahnya jumlah karakter pesan. Pada pengujian ketahanan citra tidak dapat bertahan dari perubahan, karena pesan pada citra hasil stego tidak dapat diekstrak dengan baik. Pada penelitian ini citra hasil steganografi dengan kombinasi algoritma RSA tidak dapat bertahan terhadap manipulasi citra. Oleh sebab itu diperlukan pengembangan lebih lanjut agar dapat tahan terhadap manipulasi citra.

**Kata Kunci :** *Steganografi, Kriptografi, Least Significant Bit, Algoritma RSA*

## **Abstract**

One area that is often the subject of research in computer science to engineering data security is steganography LSB (Least Significant Bit). The use of steganography LSB without a security system would be affected include efforts to eliminate the message to be inserted so as to be developed by combining the RSA algorithm. Implementation of LSB steganographic method with the RSA algorithm can improve the security of the message that will be inserted. Secret messages encrypted with RSA algorithm then inserted in the digital image. This research aimed to analyze the quality of the image of the LSB steganographic algorithm RSA has combined with visual examination, PSNR and robustness. From the results of testing visual image steganography results did not change when seen by naked eye but PSNR values obtained will be decreased by increasing the number of characters of the message. In the endurance test image can not survive the change, because the messages on the results of stego image can not be extracted properly. In this research the results of image steganography by a combination of RSA algorithm can not stand against manipulation of the image. It therefore requires further development in order to withstand manipulation of the image.

**Keyword:** *Steganography, Cryptography, Least Significant Bit, RSA Algorithm*

## **1. Pendahuluan**

### **1.1 Latar Belakang**

Berkembangnya teknologi dan informasi turut berkembang pula kejahatan teknologi seperti interupsi, penyadapan, modifikasi, dan fabrikasi. Tanpa adanya jaminan keamanan dalam data, dapat memungkinkan pihak lain dengan mudah mendapatkan pesan, data atau informasi yang dikirimkan melalui jaringan atau internet.

Salah satu bidang yang masih sering menjadibahkan penelitian dalam ilmu komputer untuk teknik keamanan data adalah steganografi. Steganografi merupakan suatu teknik untuk menyembunyikan pesan atau data yang bersifat rahasia didalam media digital. Dalam steganografi pesan/data yang akan disisipkan dalam citra digital harus memenuhi sifat ketahanan. Maksud dari sifat ketahanan adalah pesan/data yang disisipkan tidak terpengaruh dari upaya untuk menghilangkan atau merusak pesan/data tersebut baik sengaja atau tidak sengaja.

Steganografi dipandang sebagai kelanjutan kriptografi terkait dengan pesan rahasia yang akan disisipkan dalam citra. Pesan rahasia dienkripsi dengan algoritma kriptografi lalu disembunyikan dalam citra. Teknik ini dapat meningkatkan kemananan pesan/data yang akan disisipkan.

Metode LSB (Least Significant Bit) merupakan salah satu metode steganografi dalam teknik domain spasial. Metode LSB merubah nilai komponen warna bit terakhir dengan bit pesan yang akan disembunyikan sehingga menghasilkan citra yang mirip dengan aslinya. Metode ini dapat dikembangkan pada penguatan pesan

yang akan disisipkan dengan algoritma kriptografi.

Salah satu metode kriptografi asimetri yang dapat digunakan adalah algoritma RSA. Algoritma RSA yang dikembangkan oleh Ron Rivest, Shamir, dan Leonard Adleman dapat digunakan karena merupakan algoritma yang kokoh untuk enkripsi pesan karena panjang kunci dalam bit dapat diatur, dengan semakin panjang bit maka semakin sukar untuk dipecahkan karena sulitnya memfaktorkan dua bilangan yang besar tersebut [5].

Melalui penelitian ini, penulis akan mengimplementasikan metode steganografi Least Significant Bit dengan algoritma RSA untuk meningkatkan tingkat keamanan pesan yang akan disisipkan kedalam citra.

### **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah, pesan yang akan disisipkan pada citra dengan steganografi LSB tanpa dilengkapi sistem keamanan akan terpengaruh dari upaya untuk menghilangkan atau merusak pesan/data [3] sehingga perlu dikembangkan dengan mengombinasikan algoritma RSA.

### **1.3 Tujuan Penelitian**

1. Mengimplementasikan metode steganografi LSB dengan algoritma RSA untuk mendapatkan tingkat keamanan pada pesan.
2. Mengetahui penyisipan pesan yang sudah terenkripsi dengan algoritma RSA dapat dideskripsikan seperti semula.
3. Mengetahui kualitas citra hasil steganografi melalui pengujian visual, PSNR dan ketahanan citra hasil steganografi.

## 2. Metode Penelitian

### 2.1 Teknik Analisis Data

Data yang dijadikan cover-object dalam penelitian ini adalah citra berformat \*.bmp dengan ukuran 512 x 512 px. Sedangkan untuk pesan yang akan disisipkan menggunakan karakter huruf.

#### 1. Proses Pengacakan Pesan

Contoh pesan rahasia : HARI INI,  
kunci publik (e, N) : 79, 3337

- Konversi plaintext HARI INI dalam pengkodean ASCII : 7265827332737873
- Pecah X menjadi blok yang lebih kecil, misalnya X dipecah menjadi enam blok yang berukuran 3 digit:

x1 = 726                      x4 = 273  
x2 = 582                      x5 = 787  
x3 = 733                      x6 = 003

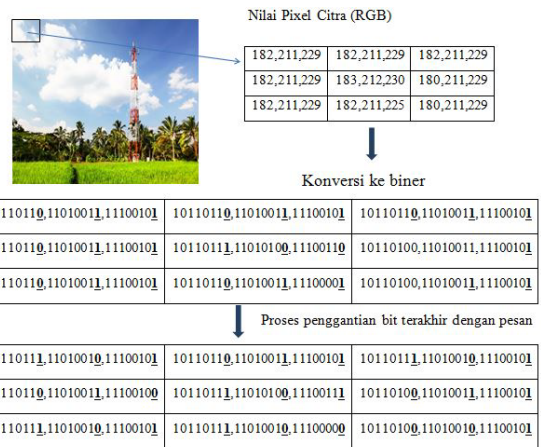
- Blok-blok plaintexts dienkripsi sebagai berikut:

$72679 \text{ mod } 3337 = 215 = y1$   
 $58279 \text{ mod } 3337 = 776 = y2$   
 $73379 \text{ mod } 3337 = 1743 = y3$   
 $27379 \text{ mod } 3337 = 933 = y4$   
 $78779 \text{ mod } 3337 = 1731 = y5$   
 $00379 \text{ mod } 3337 = 158 = y6$

- Jadi, ciphertexts yang dihasilkan adalah 215 776 1743 933 1731 158.
- Pesan rahasia selanjutnya disisipkan kedalam citra menggunakan metode LSB.

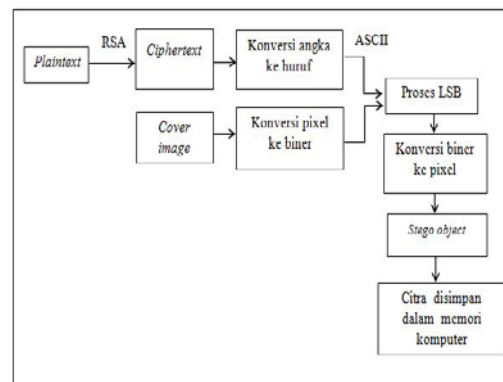
#### 2. Proses Penyisipan Pesan

Contoh konversi nilai piksel :



## 2.2 Metode yang Diusulkan

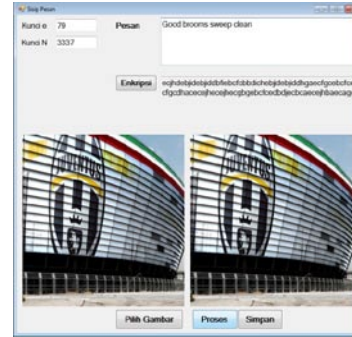
### 2.2.1 Prosedur Penyisipan Pesan



Proses penyisipan pesan dengan algoritma RSA dan metode LSB dijelaskan langkah demi langkah sebagai berikut:

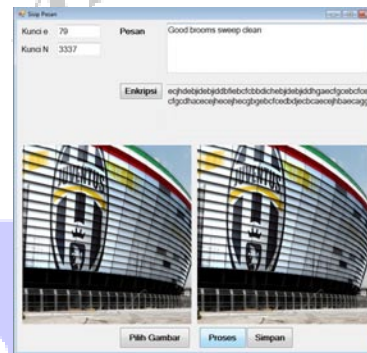
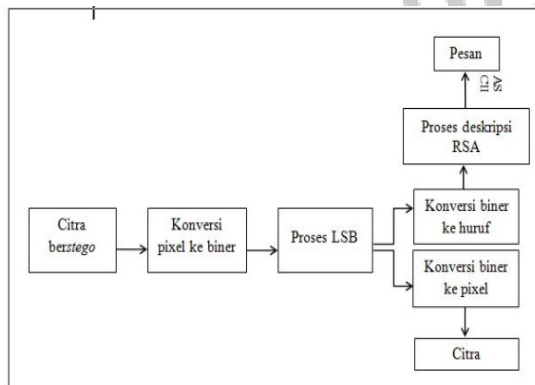
- Lakukan proses enkripsi pesan dengan algoritma RSA, lalu konversi hasil dari algoritma RSA dari bilangan desimal menjadi huruf.
- Langkah berikutnya menyiapkan citra yang akan disisipi pesan enkripsi.
- Proses menghitung LSB dari setiap nilai pixelcitra dan mengkonversi setiap nilai pixelnya ke biner.

4. Proses penyisipan pesan enkripsi dengan LSB.
5. Selanjutnya proses konversi dari biner ke nilai pixel.
6. Hasil dari citra yang telah disisipkan pesan enkripsi disimpan kedalam memori komputer.



Gambar 1: Proses penyisipan pesan

## 2.2.2 Prosedur Pengekstrakan Pesan



Gambar 2 :Proses pengekrakan pesan



Proses ekstraksi citra bersteigo dengan metode LSB dan pembacaan pesan enkripsi dengan algoritma RSA dijelaskan langkah demi langkah sebagai berikut:

1. Lakukan konversi citra menjadi bilangan biner.
2. Proses menghitung LSB dari setiap nilai pixel citra.
3. Pada saat akan membaca pesan, hasil dari langkah kedua dikonversi ke huruf lalu dilakukan proses deskripsi dengan RSA.
4. Pada saat akan mengembalikan citra asli, hasil langkah kedua dikonversi dari biner ke pixel.

## 4.2 Proses Pengujian Citra Hasil Steganografi

### 4.2.1 Pengujian Visual

Tabel 1: Uji visual

Citra Asli	Pesan	Citra Hasil Penyisipan
	Good brooms sweep clean	

Secara uji visual, dapat dilihat pada citra sebelum dan sesudah proses penyisipan pesan rahasia tidak ada perbedaan jika dilihat secara kasat mata.

## 4. Hasil dan Pembahasan

### 4.1 Aplikasi Hasil Perancangan

#### 4.2.2 Pengujian PSNR

Tabel 2: Hasil uji PSNR

Jumlah Karakter	PSNR (db)
50	74,33
80	72,52
110	71,14
140	70,15
170	69,29

Dari tabel 2 dapat dilihat bahwa nilai PSNR yang didapatkan akan semakin menurun dengan bertambahnya jumlah karakter pesan yang disisipkan pada citra hasil stego.

Resize	120 x 120	Gagal	-
	460 x 460	Gagal	-
	768 x 768	Gagal	-
	1024 x 1024	Gagal	-

#### 4.2.3 Pengujian Ketahanan

Tabel 4: Hasil uji ketahanan

Pengujian	Nilai	Hasil Uji	Hasil PSNR (db)
Kecerahan (Brightness)	-5	Gagal	11,90
	+5	Gagal	11,64
	+10	Gagal	11,35
	+20	Gagal	10,98
Ketajaman (Contrast)	-5	Gagal	35,95
	+5	Gagal	38,32
	+10	Gagal	32,82
	+20	Gagal	27,37
Rotasi	30	Gagal	-
	60	Gagal	-
	90	Gagal	7,71
	80	Gagal	7,17

### 5. Kesimpulan dan Saran

#### 5.1 Kesimpulan

Dari pengujian-pengujian yang telah dilakukan dalam penelitian ini, penulis dapat mengambil kesimpulan sebagai berikut :

1. Metode Least Significant Bit (LSB) dapat diimplementasikan dengan algoritma RSA untuk mendapatkan tingkat keamanan pada pesan.
2. Dalam penelitian ini pesan yang akan disisipkan kedalam citra di enkripsi terlebih dahulu dengan algoritma RSA, dan hasil penyisipan disimpan dalam memori komputer dengan ekstensi \*.bmp dan pesan dapat diekstrak kembali.
3. Dari pengujian visual, kualitas citra sebelum dan sesudah disisipi pesan setelah melalui proses LSB tidak terlalu banyak mengalami perbedaan dan tidak terlihat perbedaannya. Dari pengujian pada citra hasil steganografi dengan menyisipkan jumlah

karakter pesan yang berbeda-beda nilai PSNR, kualitas citra tergolong sangat baik karena nilai PSNR yang dihasilkan lebih dari 60 db yaitu antara 69,29 – 74,33.

4. Dari pengujian dengan memanipulasi citra hasil steganografi yang dilakukan antara lain penambahan nilai berbeda-beda brightness, contrast, resize dan rotasi, citra tidak dapat bertahan dari perubahan, karena pesan pada citra hasil steganografi tidak dapat diekstrak dengan baik.
5. Kualitas citra dengan memanipulasi citra hasil steganografi yang dilakukan pada brightness, resize dan rotasi tergolong citra dapat tidak digunakan karena nilai PSNR dihasilkan dibawah 20 db. Sementara pada manipulasi contrast tergolong tidak baik karena nilai PSNR dihasilkan lebih 30 db.

## 5.2 Saran

1. Citra yang digunakan dalam penelitian ini hanya menggunakan format bitmap (.bmp) sebagai wadah penampung pesan yang sudah terenkripsi, untuk pengembangannya dapat digunakan format lain seperti JPG dan PNG.
2. Citra hasil steganografi dalam penelitian ini tidak dapat bertahan manipulasi citra. Oleh karena itu dapat dikembangkan lebih lanjut agar dapat tahan terhadap manipulasi citra.
3. Media yang digunakan untuk penyisipan pesan dalam penelitian ini hanya

menggunakan citra, untuk pengembangannya dapat dikembangkan untuk implementasi penyisipan pesan ke dalam media lain seperti audio dan video.

## Daftar Pustaka

1. Sriherlina, "Keamanan omputer," [Online]. Available: <http://sriherlina9.files.wordpress.com/>. [Accesed 25 November 2014].
2. T.Tiwari, A., Yadav, S.R., and Mittal, N.K., "A Review on Different Image Steganografi Techniques," *International Journal of Engineering and Innovative Techonology (IJEIT)*, vol. III, no. 7, 2014.
3. B. Rahmat and M. Fairuzabadi, "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4," *Dinamika Informatika*, vol. V , pp. 1-17, 2010.
4. Hasibuan Zuhadi, "Perancangan Aplikasi Steganografi Dengan Metode Least Significant Bit Untuk Data Terenkripsi Dari Algoritma Hill Cipher," *Pelita Informatika Budi Darma*, vol. VI, 2014.
5. Raphael Joseph, A., Sundaram, V., (2011), *Cryptography and Steganography - A Survey*, *International Journal Computer Tech*, (volume 2, issue 3)
6. T. Sutoyo, Edy M, Vincent S, Oky Dwi N, and Wijanarto "Teori Pengolahan Citra Digital", Yogyakarta: Andi & UDINUS, 2009.
7. O. Susila, "Teori Dasar Pengolahan Citra Digital," [Online]. Available: <http://www.lintasinformatika.com/>. [Accessed 26 Oktober 2014].
8. M. Wahid, "Steganografi Citra Digital Dengan DCT dan DWT," Skripsi Teknik Informatika- Universitas Dian Nuswantoro, Semarang, 2014.
9. M. M. Amin, "Image Steganografi Dengan Metode Least Bit Significant Bit (LSB)," *Jurnal CSRID*, vol. VI, pp. 01-64, 2014.
10. Y. Kurniawan, Kriptografi Keamanan Internet dan Jaringan Telekomunikasi, Bandung: Informatika, 2004.
11. Constans Mike, "Signal to Noise Ratio," [Online]. Available: [http://www.cctv-information.uk/constant2/sn\\_ratio.html](http://www.cctv-information.uk/constant2/sn_ratio.html). [Accessed 12 April 2015].
12. Juvepoland Wallpapers, "Juventus Stadium Walpapers," [Online]. Available: <http://www.tapety.juvepoland.com/index.php?/wallpapers/show/676>. [Accessed 12 April 2015].