METODE *DYNAMIC PARITY BIT* STEGANOGRAFI BERDASARKAN MODIFIKASI METODE *LEAST SIGNIFICANT BIT* (LSB)

I Komang Wiratama*[1], Retantyo Wardoyo[2]
[3]Jurusan Ilmu Komputer dan Elektronika, FMIPA UGM, Yogyakarta
e-mail: *[1]wiratama.komang@gmail.com, [2]rw@ugm.co.id

Abstrak

Pengiriman informasi rahasia dapat dilakukan dengan menyembunyikan informasi ke dalam suatu media dengan teknik steganografi. Salah satu metode steganografi yang paling sering digunakan adalah Least Significant Bit (LSB), namun metode LSB sangat mudah diekstrak. Dalam penelitian ini diusulkan modifikasi metode LSB menjadi metode Dynamic Parity Bit Steganografi pada citra bitmap. Metode ini melakukan penyisipan pesan dengan membuat parity yang besarnya berubah-ubah pada bit terakhir dari beberapa byte dalam cover image. Beberapa pengujian yang dilakukan dalam penelitian ini adalah pengujian kapasitas penyimpanan pesan, pengujian kualitas citra, pengujian waktu penyisipan dan ekstraksi pesan, perhitungan kompleksitas algoritma, dan pengujian keamanan pesan. Pengujian kapasitas penyimpanan pesan menghasilkan persamaan $N = C \ div \left(\frac{D}{K}\right)$. Pengujian kualitas citra hasil penyisipan pesan menghasilkan nilai diatas 70 dB pada saat disisipkan pesan dengan memenuhi seluruh kapasitas pesan yang artinya kualitas citra sangat baik. Waktu penyisipan dan ekstraksi pesan dengan metode ini relatif lebih lama dibandingkan dengan LSB karena kompleksitas algoritma yang dimiliki lebih tinggi. Keamanan pesan dari metode lebih baik dibandingkan dengan metode LSB karena akan membutuhkan waktu yang lebih lama untuk melakukan ekstraksi pesan secara brute force.

Kata kunci—Steganografi, Dynamic Parity Bit, Citra Bitmap, LSB

Abstract

Delivery of secret information can be done by hiding the information into a particular medium with steganography techniques. One of the most commonly used steganographic method is LSB. However, the LSB method is very easy to extract. In this research, Dynamic Parity Bit Steganography method is proposed on bitmap image. This method is inserting a message by creating a parity of varying magnitude on the last bit of a few bytes on the cover image. Some of the test applied in this research were testing of message storage capacity, image quality testing, message insertion and extraction time testing, calculation of algorithm complexity, and security of the message testing. Storage capacity testing generates equation $N = C \ div \left(\frac{D}{K}\right)$. Image quality testing after message insertion result in value above 70 dB when inserted message by fulfilling all message capacity which means very good image quality. Time of insertion and extraction of the message with this method is relatively longer compared to LSB because of the higher algorithm complexity. Message security of this method is better than LSB because it will take a longer time to extraction the message by brute force.

Keywords— Steganography, Dynamic Parity Bit, Bitmap Image, LSB

1. PENDAHULUAN

Seganografi bukanlah bidang ilmu yang baru. Penyembunyian data rahasia pada suatu media tertentu telah dimulai berabad-abad yang lalu. Steganografi sendiri berakar dari Bahasa Yunani, yaitu dari kata steganos yang berarti membungkus atau menyembunyikan dan graphy yang berarti tulisan atau gambar (Cole, (2003). Steganografi adalah ilmu atau seni penyembunyian pesan, dimana pesan yang disembunyikan ditanamkan pada suatu cover media dengan tujuan agar orang yang tidak berhak tidak menyadari adanya data tersembunyi di dalamnya. Cover media dapat terdiri dari berbagai file digital seperti teks, gambar, video, suara, dan lain sebagainya (Kalita dan Tuithung, 2016). Seiring berjalanya waktu, media gambar menjadi yang paling banyak digunakan karena system pengelihatan manusia lebih tidak sensitif dibandingkan dengan system pendenganran manusia (Malekmohamadi dan Ghaemmaghami, 2009).

Perbedaan paling mendasar dari watermarking dan steganografi terletak pada tujuan yang ingin dicapai oleh penggunanya. Dalam watermarking, citra yang digunakan merupakan hal yang paling penting sedangkan data yang dimasukkan ke dalam citra tersebut berguna untuk melindungi hak cipta dari pembuat citra tersebut, sedangkan dalam steganografi data yang disisipkan ke dalam citra merupakan komponen utama dari penerapan seteganografi. Citra yang digunakan untuk menyembunyikan pesan di dalamnya hanya berguna sebagai cover (Akhtar, dkk, 2017).

Steganografi secara umum dapat diterapkan kedalam dua domain yang berbeda, yaitu steganografi dalam domain spasial dan dalam domain transform atau frekuensi. Least Significant Bit (LSB) merupakan metode yang sering digunakan dalam steganografi karena proses komputasinya yang ringan dan kapasitas penyimpanan data yang cukup besar (Nurhayati dan Ahmad, 2016). Metode ini beroperasi dalam domain spasial pada citra digital. Namun penerapan metode ini biasanya dapat menimbulkan kecurigaan karena terkadang dapat dideteksi oleh aplikasi pendeteksi steganografi dan sangat mudah diekstrak (Arya dan Sarahan, 2015).

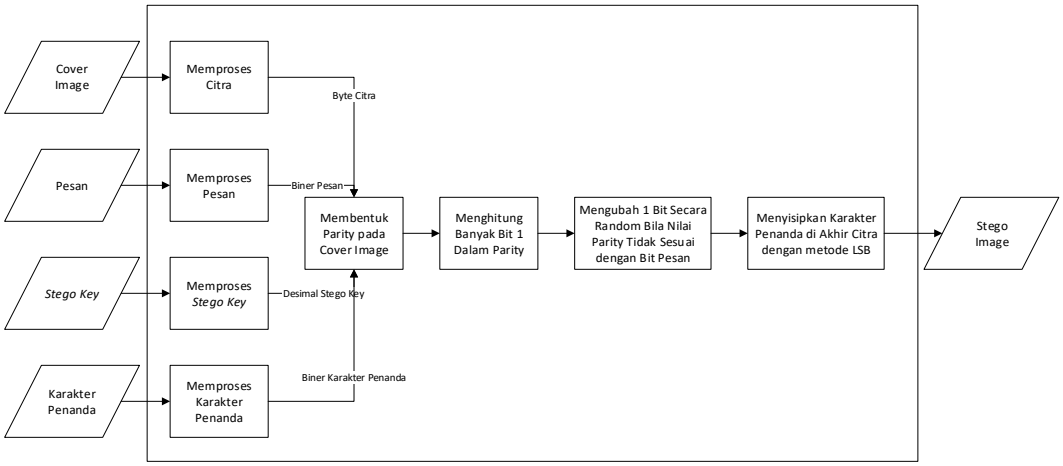
Melihat kekurangan dalam metode LSB terutama dari segi keamanan pesan yang disisipkan, penulis melakukan penggabungan metode LSB dengan metode parity bit dan melakukan modifikasi sehingga dihasilkan parity dengan ukuran yang dinamis sesuai dengan kebutuhan pengguna. Berdasarkan penggabungan dan modifikasi metode tersebut, penulis mengusulkan nama metode Dynamic Parity Bit Steganografi. Sebelumnya Bandyopadhyay dan Banik (2012) pernah melakukan penyisipan dua buah pesan ke dalam satu media audio menggunakan metode LSB untuk pesan pertama dan metode Parity untuk menyisipkan pesan kedua. Selain itu, Dighe dan Kapale (2013) pernah melakukan penelitian yang memanfaatkan parity dari 2 bit terakhir dari red piksel citra sebagai control untuk menyisipkan bit pesan ke dalam piksel green atau blue. Berdasarkan pustaka yang telah dikaji, steganografi pada citra dengan memanfaatkan parity coding yang bersifat dinamis seperti pada penelitian ini belum pernah dilakukan sebelumnya.

2. METODE PENELITIAN

2.1. Deskripsi Sistem

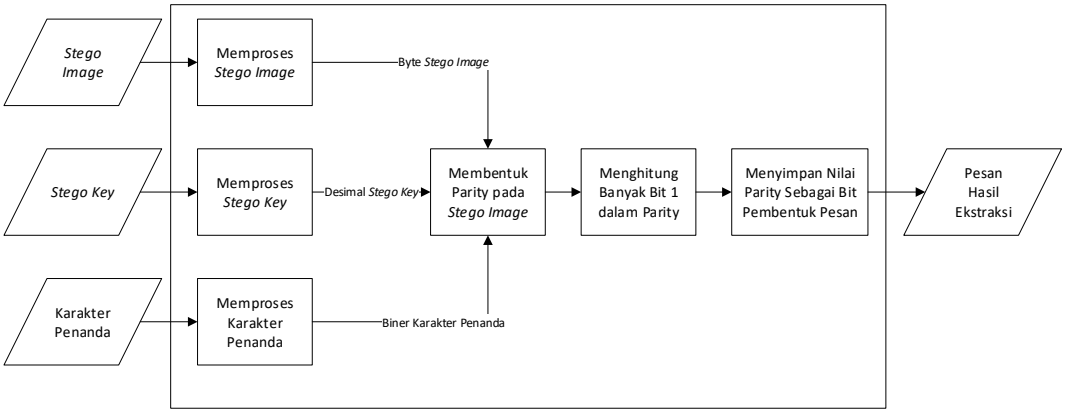
Pada penelitian ini penulis mencoba menggabungkan metode LSB dan parity bit kemudian melakukan modifikasi dengan menggunakan parity yang besar framenya berubah-ubah sesuai dengan kebutuhan pengguna. Berdasarkan pada penggabungan dan

modifikasi kedua metode tersebut, penulis mengusulkan metode yang dihasilkan dengan nama *Dynamic Parity Bit* Steganografi. Berikut ini adalah gambaran sistem steganografi citra secara umum dengan menggunakan metode *Dynamic Parity Bit* Steganografi untuk proses penyisipan pesan dan ekstraksi pesan. Sistem penyisipan pesan pada *cover image* membutuhkan masukan berupa citra bitmap sebagai *cover image*, pesan yang disisipkan, pesan berupa file teks berisi *pritntable* 8 bit ASCII karakter, *stego key* sebagai ukuran pembentukan frame parity pada *cover image*, dan karakter penanda sebagai tanda akhir pada pesan. Lokasi *bit* paling pertama yang dilakukan proses penyisipan merupakan komponen yang sangat penting untuk menjaga kerahasiaan data yang tersimpan dalam citra, sehingga lokasi *bit* pertama yang digunakan tidak akan sama antara satu *stego image* dengan *stego image* lainnya tergantung pada *stego key* yang digunakan.



Gambar 1. Proses penyisipan pesan secara umum dengan metode *Dynamic Parity Bit* Steganografi

Proses ekstraksi pesan pada *stego image* diperlukan tiga buah masukan yaitu citra bitmap yang mengandung pesan (*stego image*), *stego key* yang harus sama dengan *stego key* yang digunakan dalam proses penyisipan pesan dan karakter penanda yang juga harus sama dengan yang digunakan pada saat proses penyisipan pesan. Ekstraksi pesan dilakukan dengan membuat frame parity dengan ukuran yang sesuai dengan nilai decimal dari *stego key*. Banyaknya nilai 1 dari bit terakhir setiap byte yang tergabung dalam parity akan dilakukan operasi mod 2. Apabila hasil dari operasi mod 2 tersebut bernilai 0, maka bit pesan pada frame parity tersebut adalah 0. Sedangkan apabila hasil dari operasi mod 2 tersebut bernilai 1, maka bit pesan dalam frame parity tersebut adalah 1. Setiap kali system berhasil melakukan ekstraksi terhadap satu bit pesan, system akan melakukan pengecekan terhadap keberadaan karakter penanda pada beberapa byte berikutnya sesuai dengan karakter penanda yang dimasukkan oleh pengguna. Apabila karakter penanda ditemukan, maka proses ekstraksi pesan akan berhenti. Sedangkan apabila karakter penanda belum ditemukan, maka proses ekstraksi pesan akan dilanjutkan.



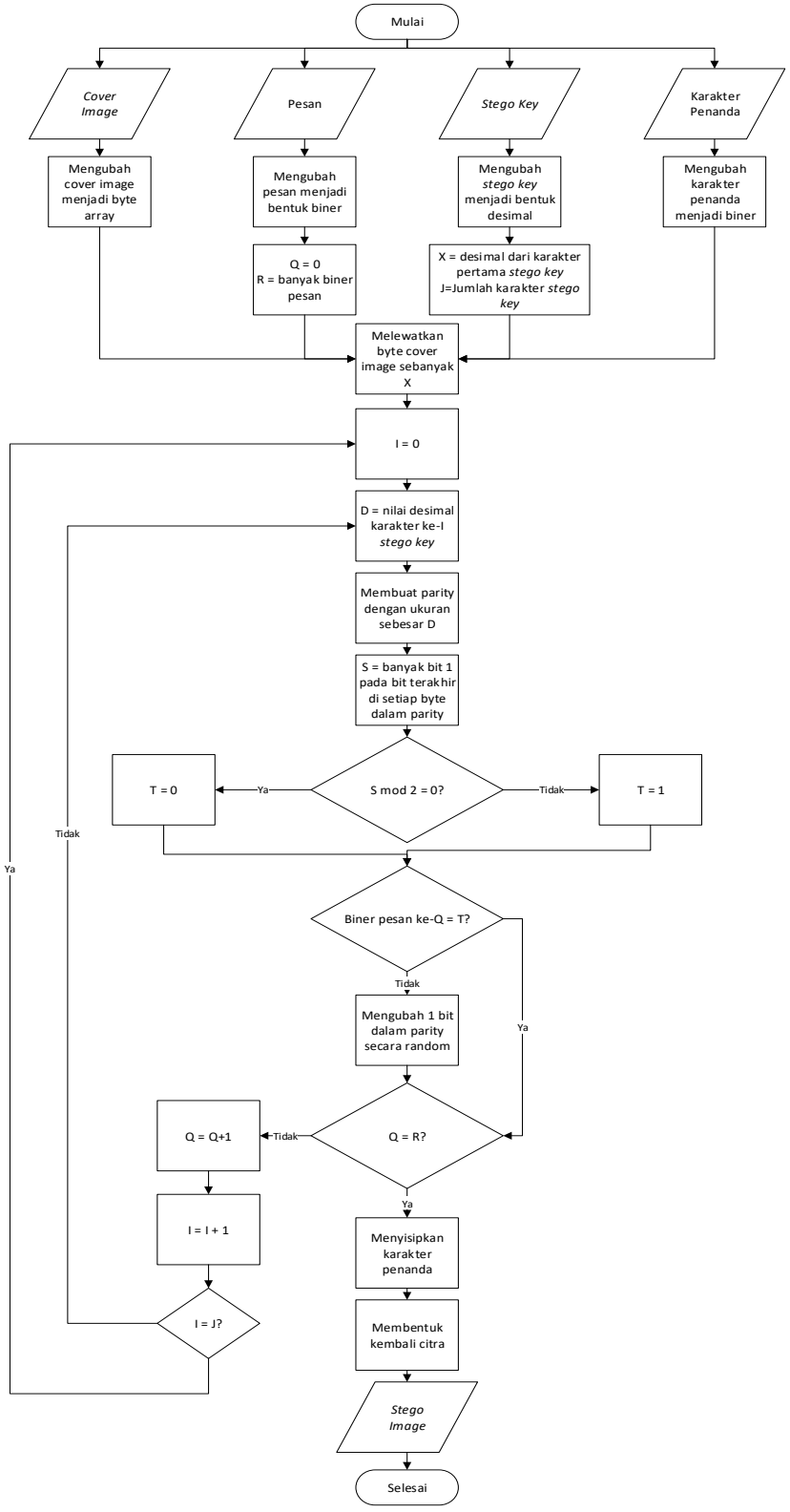
Gambar 2. Proses ekstraksi pesan secara umum dengan metode *Dynamic Parity Bit* Steganografi

2.2 Analisis Proses

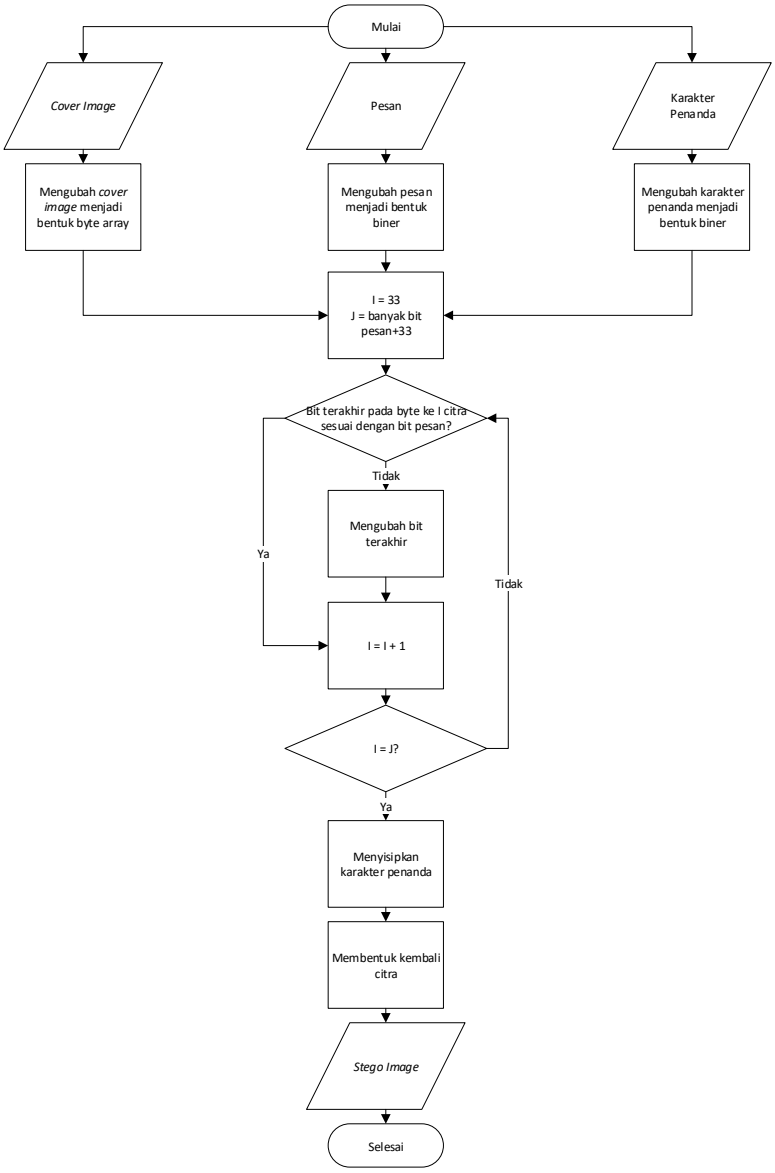
Dalam analisis proses ini akan dibahas proses penyisipan dan ekstraksi pesan dengan menggunakan metode LSB dan metode *Dynamic Parity Bit* Steganografi.

2.2.1 Proses Penyisipan pesan

Proses penyisipan pesan dengan metode *Dynamic Parity Bit* Steganografi membutuhkan empat buah data *input*, yaitu *cover image* berupa citra bitmap yang diproses menjadi berbentuk byte array sebagai media penampung pesan yang akan disembunyikan, pesan berupa file teks berisi *printable* 8 bit ASCII karakter yang dalam system setiap karakter dalam file pesan diproses menjadi berbentuk biner, *stego key* berupa *printable* 8 bit ASCII karakter yang dalam system setiap karakter dari *stego key* diubah menjadi bentuk desimal, dan karakter penanda berupa *printable* 8 bit ASCII karakter yang disisipkan pada bagian akhir pesan dalam *cover image*. Proses penyisipan pesan dilakukan dengan membuat frame parity pada cover image sebesar nilai desimal dari karakter *stego key*. Nilai *parity coding* yang dihasilkan dari frame tersebut dicocokkan dengan bit pesan yang disisipkan. Apabila belumsesuai, maka satu bit terakhir dalam parity tersebut akan diubah secara acak. Setelah seluruh pesan disisipkan dalam *cover image*, maka karakter penanda akan disisipkan tepat setelah bit terakhir pesan dengan metode LSB. Flowchart proses penyisipan pesan dengan metode *Dynamic Parity Bit* Steganografi dapat dilihat pada Gambar 3.



Gambar 3. Flowchart proses penyisipan pesan dengan metode *Dynamic Parity Bit Steganografi*



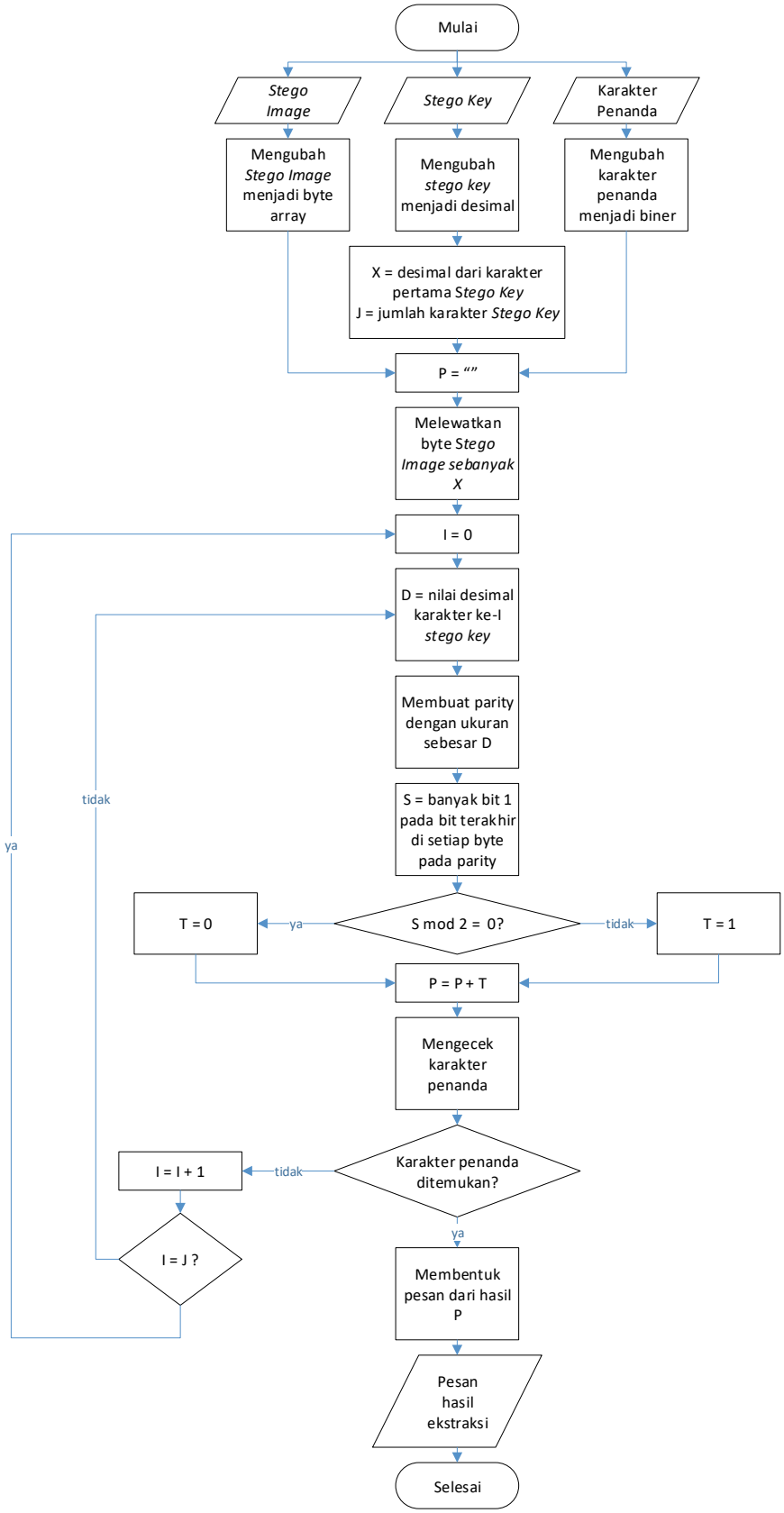
Gambar 4. Flowchart proses penyisipan pesan dengan metode LSB

Proses penyisipan pesan dengan metode LSB membutuhkan tiga buah data *input*, yaitu cover image berupa *cover image* berupa citra bitmap sebagai media penampung pesan yang akan disembunyikan, pesan berupa file teks berisi *printable* 8 bit ASCII karakter yang dalam system setiap karakter dalam file pesan diproses menjadi berbentuk biner, dan karaker penanda berupa *printable* 8 bit ASCII karakter yang disisipkan pada bagian akhir pesan dalam *cover image*. Proses penyisipan pesan dimulai dari byte ke-33 dari *cover image* untuk menghindari kerusakan *header* citra. Setiap bit terakhir dari *cover image* dibandingkan dengan setiap bit pesan yang disisipkan. Bit terakhir dari setiap byte *cover image* yang tidak sesuai dengan bit pesan akan diubah sehingga sesuai dengan bit pesan. Setelah seluruh pesan berhasil disisipkan, dilakukan penyisipan karakter penanda sebagai tanda bahwa pesan tersebut telah berakhir. Flowchart proses penyisipan pesan dengan metode LSB dapat dilihat pada Gambar 4.

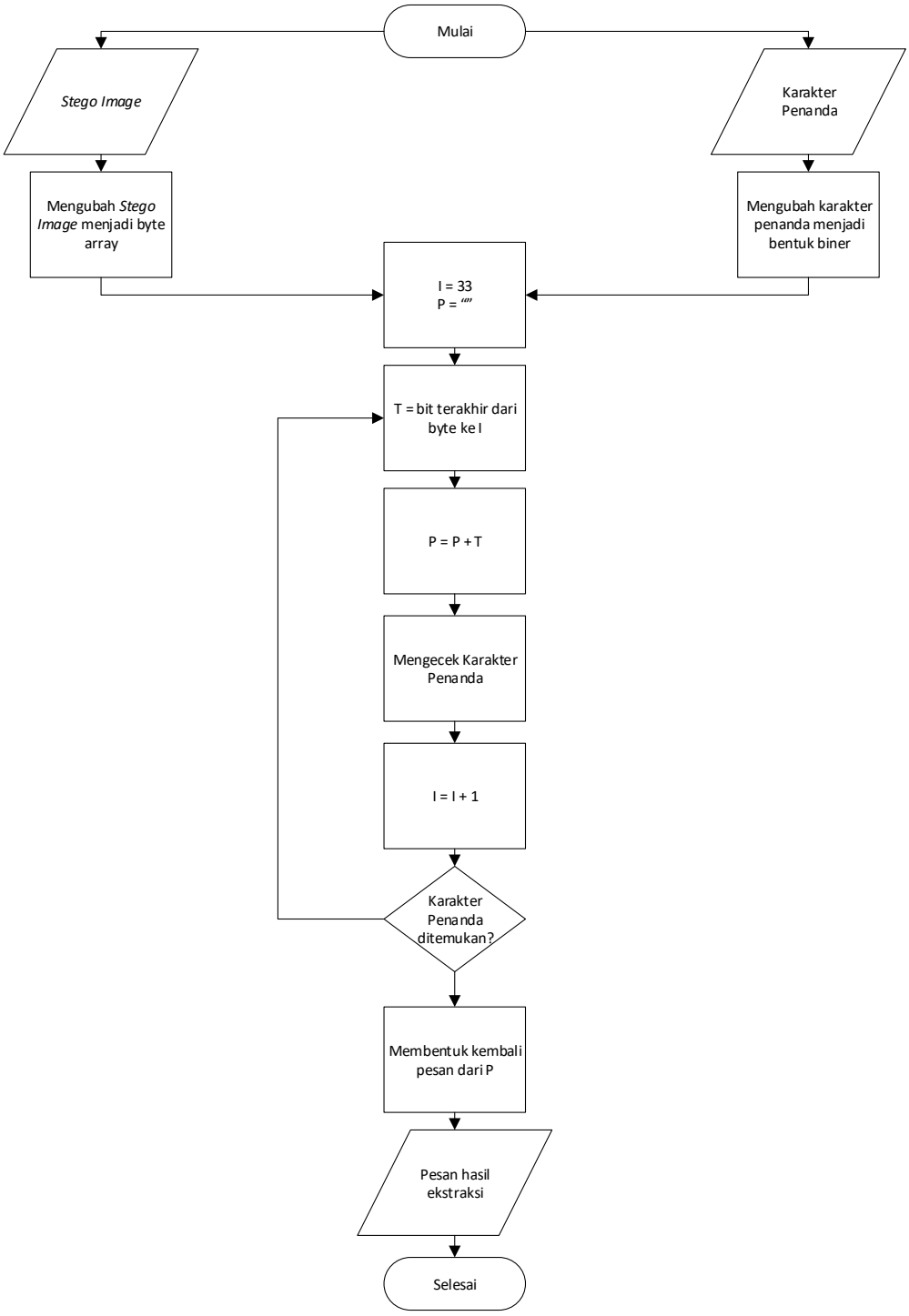
2. 2.2 Proses Ekstraksi Pesan

Proses ekstraksi pesan yang disisipkan dengan metode *Dynamic Parity Bit* Steganografi membutuhkan tiga data *input*, yaitu *stego image* berupa citra bitmap yang mengandung pesan rahasia di dalamnya, *stego key* berupa *printable* 8 bit ASCII karakter yang dalam system diubah ke dalam bentuk desimal, dan karakter penanda berupa *printable* 8 bit ASCII karakter yang menandakan bagian akhir dari pesan dalam *stego image*. Proses ekstraksi pesan dilakukan dengan membentuk frame parity pada *stego image* sebesar nilai desimal dari setiap karakter *stego key* yang digunakan. Nilai *parity coding* yang diperoleh dari frame tersebut disimpan sebagai bit pesan. Proses ini dilakukan sampai dengan ditemukan karakter penanda yang sama pada bit *stego image*. Apabila karakter penanda ditemukan dalam beberapa byte berikutnya yang menandakan seluruh pesan telah berhasil diekstrak, bit pesan yang telah diperoleh dari proses sebelumnya dibentuk kembali menjadi file teks berisi *printable* 8 bit ASCII karakter sesuai dengan bit hasil ekstraksi. Flowchrart proses ekstraksi pesan dengan metode *Dynamic Parity Bit* Steganografi dapat dilihat pada Gambar 5.

Proses ekstraksi pesan yang disisipkan denga metode LSB membutuhkan dua data *input*, yaitu *stego image* berupa citra bitmap yang mengandung pesan rahasia di dalamnya, dan karakter penanda untuk dicocokkan dengan tanda yang ada di dalam *stego image* sebagai penanda bahwa pesan di dalamnya telah berakhir. Proses ekstraksi pesan dimulai dari byte ke-33 pada *stego image*. Bit terakhir dari setiap byte *stego image* disimpan sebagai bit pesan sampai dengan bit yang sama dengan karakter penanda ditemukan. Setelah bit yang sesuai dengan karakter penanda ditemukan, bit pesan yang telah diperoleh dari proses sebelumnya dibentuk kembali menjadi file teks berisi *printable* 8 bit ASCII karakter sesuai dengan bit hasil ekstraksi. Flowchart proses ekstraksi pesan dengan metode LSB dapat dilihat pada Gambar 6.



Gambar 5. Flowchart proses ekstraksi pesan dengan metode *Dynamic Parity Bit* Steganografi



Gambar 6. Flowchart proses ekstraksi pesan dengan metode LSB

2.3 Analisis Kapasitas Penyimpanan Pesan

Metode *Dynamic Parity Bit* steganografi menyisipkan *bit* pesan ke dalam suatu set *parity* dalam LSB suatu *cover image*. Set *parity* tersebut memiliki besar yang berbeda-beda satu sama lainnya berkisar antara 32-255 tergantung pada tiap karakter *stego key* yang dimasukkan dalam proses penyisipan pesan. Karakter pertama dalam *stego key* digunakan untuk melewati sejumlah *byte* dalam *cover* image agar proses penyisipan pesan

tidak dimulai dari *byte* pertama *cover image*, melainkan berubah-ubah tergantung pada karakter *stego key* yang digunakan. Masing-masing karakter *stego key* mewakili satu *bit* dari setiap karakter pesan yang disisipkan. Sebuah karakter pesan membutuhkan 8 bit penyimpanan. Persamaan untuk mengetahui jumlah karakter yang dapat ditampung oleh citra dengan suatu *stego key* tertentu dapat dirumuskan menjadi

$$N = C \; div \left(\frac{D}{K}\right) \quad (1)$$

Dimana :
N = Jumlah karakter maksimal yang dapat ditampung citra
C = Besar cover image (*byte*)
D = Jumlah nilai desimal dari kunci
K = Jumlah karakter kunci / 8

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Kapasitas Penyimpanan Pesan

Penyisipan pesan dengan metode LSB dilakukan dengan menyisipkan setiap bit pesan ke dalam setiap bit *cover image* yang digunakan sebagai media penyembunyian pesan. Jumlah karakter yang dapat di tamping oleh suatu citra aabila disisipkan pesan dan karakter penanda dengan metode LSB dapat dihitung dengan cara membagi besar *cover image* dalam byte dengan 8. Hal ini disebabkan karena masing-masing karakter pesan dan penanda terdiri dari 8 bit. Jumlah karakter maksimal yang dapat ditampung suatu citra dapat dilihat pada Tabel 1.

Tabel 1. Kapasitas penyimpanan pesan dengan metode LSB

No	Nama File	Besar File (byte)	Banyak Karakter
1	prambanan kecil.bmp	73.062	9.132
2	candi ijo kecil.bmp	292.086	36.519
3	bintang pinus.bmp	574.710	71.838
4	tangga 20%.bmp	1.168.182	146.022
5	Telaga Warna 25%.bmp	2.250.054	281.256

Selanjutnya, dilakukan pengujian untuk mengetahui kapasitas peyimpanan pesan dengan metode *Dynamic Parity Bit* Steganografi. *Stego key* sangat mempengaruhi kapasitas peyimpanan pesan dengan metode *Dynamic Parity Bit* Steganografi karena besar parity dari setiap bit yang disisipkan ke dalam *cover image* bergantung pada *stego key* yang digunakan. Untuk menghitung banyaknya karakter maksimal yang dapat ditampung oleh suatu citra dapat dihitung dengan persamaan 1.

Dengan persamaan 1, banyak karakter yang dapat ditampung oleh suatu citra dengan menggunakan *stego key* tertentu dapat dihitung. Hasil perhitungan kapasitas penyimpanan pesan dengan metode *Dynamic Parity Bit* Steganografi dapat dilihat pada Tabel 2.

Berdasarkan Tabel 1 dan Tabel 2 dapat dilihat bahwa kapasitas penyimpanan pesan dari metode LSB lebih besar dibandingkan dengan metode *Dynamic Parity Bit* Steganografi. Hal ini terjadi karena metode *Dynamic Parity Bit* Steganografi membutuhkan ruang yang lebih banyak untuk membuat frame parity dalam menyisipkan setiap bit pesan sehingga pesan lebih sulit diekstrak secara paksa.

Tabel 2. Kapasitas penyimpanan pesan dengan metode *Dynamic Parity Bit* Steganografi

No	Nama File	Stego Key	C	D	K	N
1	prambanan kecil.bmp	dialog dini hari	73.062	1.528	2	95
2	prambanan kecil.bmp	!#$%&	73.062	179	5/8	248
3	candi ijo kecil.bmp	dialog dini hari	292.086	1.528	2	382
4	candi ijo kecil.bmp	!#$%&	292.086	179	5/8	1.019
5	bintang pinus.bmp	dialog dini hari	574.710	1.528	2	752
6	bintang pinus.bmp	!#$%&	574.710	179	5/8	2,006
7	tangga 20%.bmp	dialog dini hari	1.16.182	1.528	2	1.529
8	tangga 20%.bmp	!#$%&	1.168.182	179	5/8	4.078
9	Telaga Warna 25%.bmp	dialog dini hari	2.250.054	1.528	2	2.945
10	Telaga Warna 25%.bmp	!#$%&	2.250.054	179	5/8	7.056

3.2 Pengujian Kualitas Citra

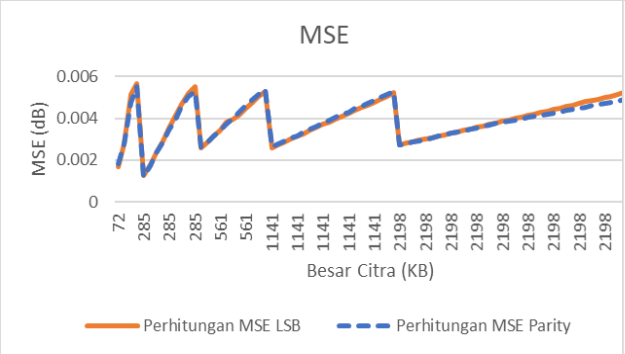
Pengujian kualitas citra dilakukan untuk mengetahui seberapa besar perubahan uang terjadi antara *cover image* dengan *stego image*. Penelitian ini membandingkan kualitas *stego image* yang dihasilkan dari metode LSB dan *Dynamic Parity Bit* Steganografi dengan metode pengujian MSE dan PSNR. Semakin besar nilai MSE, maka perbedaan antara *cover image* dan *stego image* semakin besar. Berbanding terbalik dengan perhitungan MSE, pada perhitungan PSNR perbedaan antara *cover image* dan *stego image* semakin besar apabila nilai yang dihasilkan semakin kecil. Nilai PSNR biasanya dinyatakan dalam skala decibel (dB). Nilai PSNR di bawah 30 dB menunjukkan kualitas citra yang rendah, sedangkan nilai di atas 40 dB menunjukkan kualitas citra yang baik. Semakin tinggi nilai PSNR yang dihasilkan, maka semakin baik pula kualitas citra tersebut (Cheddad, dkk, 2010). Sebagian hasil perhitungan MSE dan PSNR dapat dilihat pada Tabel 3.

Dalam Gambar 7 dan Gambar 8 dapat dilihat bahwa perbandingan nilai MSE dan PSNR dari metode *Dynamic Parity Bit* Steganografi dan metode LSB tidak memiliki perbedaan yang signifikan, sehingga dapat dikatakan bahwa metode tersebut menghasilkan kualitas citra yang sama baiknya.

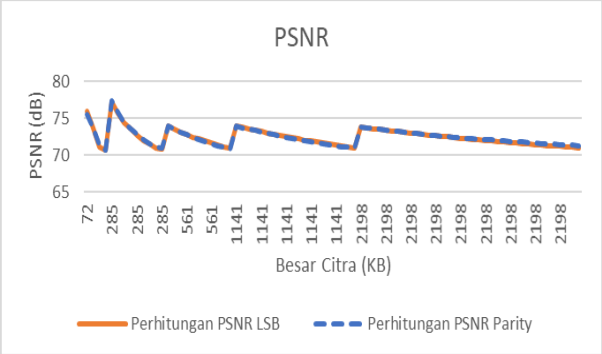
Tabel 3. Perhitungan MSE dan PSNR

No	Besar Citra	Banyak Karakter	Perhitungan MSE		Perhitungan PSNR	
			LSB	Parity	LSB	Parity
1	72 KB	40	0.00279	0.00279	73.705415	73.70541
2	72 KB	95	0.00565	0.00552	70.64221	70.74866
3	285 KB	200	0.00292	0.00286	73.51551	73.60304
4	285 KB	382	0.00549	0.00528	70.76515	70.93624
5	561 KB	480	0.00342	0.00343	72.82124	72.81462
6	561 KB	752	0.00526	0.00537	70.95481	70.86814
7	1141 KB	1200	0.00411	0.00419	72.00329	71.94681
8	1141 KB	1528	0.00522	0.00529	70.98447	70.92931
9	2198 KB	1980	0.00351	0.00348	72.71871	72.74633
10	2198 KB	2660	0.00471	0.00447	71.43367	71.65686
11	2198 KB	2944	0.00522	0.00488	70.99152	71.27793

Berdasarkan perhitungan MSE dan PSNR yang telah dilakukan, dapat dibangun grafik perbandingan nilai MSE dan PSNR seperti pada Gambar 7 dan Gambar 8



Gambar 7. Perbandingan nila MSE



Gambar 8. Perbandingan nilai PSNR

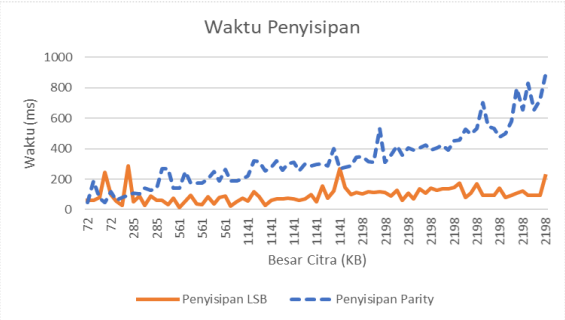
3.3. Pengujian Waktu Penyisipan dan Ekstraksi Pesan

LSB merupakan salah satu metode steganografi yang memiliki kecepatan penyisipan dan ekstraksi pesan yang relative cepat. Tabel 4 menunjukkan waktu penyisipan dan ekstraksi pesan antara metode LSB dan *Dynamic Parity Bit* Steganografi.

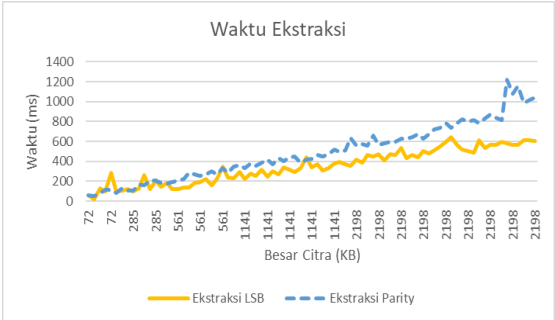
Tabel 4. Perbandingan waktu penyisipan dan ekstraksi pesan

No	Besar Citra (KB)	Banyak Karakter	Penyisipan		Ekstraksi	
			LSB (ms)	Parity (ms)	LSB (ms)	Parity (ms)
1	72	40	63	187	16	47
2	72	95	100	118	285	113
3	285	200	53	109	100	109
4	285	382	60	266	148	187
5	561	480	56	250	134	219
6	561	752	89	265	350	330
7	1141	1200	70	311	313	439
8	1141	1528	266	267	381	518
9	2198	1980	106	406	536	625
10	2198	2660	79	499	562	837
11	2198	2944	221	881	606	1039

Berdasarkan pengujian waktu penyisipan dan ekstraksi pesan dari Tabel 4, dapat dibangun grafik perbandingan waktu penyisipan dan ekstraksi pesan seperti pada Gambar 9 dan Gambar 10



Gambar 9 Perbandingan waktu penyisipan



Gambar 10. Perbandingan waktu ekstraksi

Pada Gambar 9 dan Gambar 10 dapat dilihat bahwa rata-rata waktu yang dibutuhkan dalam penyisipan dan ekstraksi pesan dengan metode *Dynamic Parity Bit* Steganografi lebih banyak dibandingkan dengan metode LSB.Hal ini disebabkan oleh kompleksitas yang dimiliki oleh metode *Dynamic Parity Bit* Steganografi lebih tinggi dibandingkan dengan metode LSB.

3.4. Kompleksitas Algoritma

Dalam penyisipan dengan metode *Dynamic Parity Bit* Steganografi terdapat perulangan bersarang (*nested loop*) dengan banyak perulangan berbeda. Pada perulangan luar (*outer loop*), perulangan dilakukan sebanyak jumlah bit yang akan disisipkan. Sedangkan pada perulangan dalam (*inner loop*), perulangan dilakukan sebanyak nilai decimal dari tiap-tiap karakter *stego key*. persamaan yang dihasilkan adalah

$$g(n) = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} 1 = \sum_{i=0}^{n-1} m = nm \qquad (2)$$

Dari persamaan 2 dapat dikatakan Big-*O* dari algoritma ini adalah *O*(*nm*).

Dalam penyisipan dengan metode LSB terdapat perulangan sebanyak bit pesan yang disisipkan. Persamaan yang dihasilkan adalah

$$g(n) = \sum_{i=0}^{n-1} 1 = n \qquad (3)$$

Dari persamaan 3 dapat dikatakan Big-*O* dari algoritma ini adalah *O*(*n*).

Proses ekstraksi pesan dengan metode *Dynamic Parity Bit* Steganografi, terdapat perulangan *while* dan dua buah perulangan *for* di dalamnya. Salah satu perulangan *for* tersebut berfungsi untuk mengecek apakah terdapat karakter penanda di dalam beberapa byte berikutnya. Sedangkan *for* yang lain bertugas menjalankan perulangan sebanyak nilai desimal dari *stego key* yang digunakan oleh user. Perulangan ini berfungsi untuk menghitung banyanya *bit* 1 yang terdapat dalam suatu parity. Perulangan *while* disini akan berhenti apabila karakter penanda ditemukan. Persamaan yang dihasilkan adalah

$$g(n) = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} 1 + \sum_{k=0}^{o-1} 1 \right) = \sum_{i=0}^{n-1} (m+o) = n(m+o) = nm + no \qquad (4)$$

Dari persamaan 4 dapat dikatakan Big-*O* dari algoritma ekstraksi pesan dengan metode *Dynamic Parity Bit* Steganografi adalah *O*(*nm* + *no*).

Proses ekstraksi pesan dengan metode LSB menggunakan sebuah perulangan *while* dan sebuah perulangan *for* di dalamnya. Perulangan *while* disini akan berhenti apabila karakter penanda ditemukan dalam beberapa *byte* berikutnya yang dicari dengan menggunakan perulangan *for* tersebut. Persamaan yang dihasilkan adalah

$$g(n) = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} 1 = \sum_{i=0}^{n-1} m = nm \qquad (5)$$

Dari persamaan 5 dapat dikatakan Big-*O* dari algoritma ekstraksi pesan dengan metode LSB adalah *O*(*nm*).

Berdasarkan kompleksitas algoritma penyisipan dan ekstraksi pesan antara metode LSB dan *Dynamic Parity Bit* Steganografi tersebut dapat dilihat bahwa kompleksitas yang dimiliki oleh metode *Dynamic Parity Bit* Steganografi lebih tinggi dibandingkan dengan metode LSB.

3.5 Pengujian Keamanan Pesan

Ekstraksi pesan yang disisipkan dengan metode LSB dapat dilakukan dengan melakukan (n*8) kali percobaan karena data yang tersimpan dalam *stego image* dalam kondisi berurutan pada setiap byte citra. Sedangkan apabila mengekstrak pesan yang disisipkan dengan metode *Dynamic Parity Bit* Steganografi secara *brute force* tanpa menggunakan *stego key* membutuhkan $223^{(n*8)}$ kali percobaan dengan n merupakan jumlah karakter yang disisipkan dalam citra.

Misalkan serangan secara *brute force* dilakukan dengan menggunakan super komputer Sunway Taihu Light buatan *China* pada November 2016 yang memiliki kecepatan 93.01 petaflops atau dengan kata lain dapat melakukan $93.01 * 10^{15}$ perhitungan per detik. Waktu yang dibutuhkan oleh perangkat super komputer ini untuk melakukan ekstraksi pesan secara *brute force* pada pesan yang disisipkan dengan metode *Dynamic Parity Bit* Steganografi adalah $223^{(n*8)} / 93.01 * 10^{15}$ detik. Untuk mengekstrak 2 karakter pesan dalam stego image secara brute force, super komputer ini membutuhkan waktu 4021130469094185899 57.02750112792 detik ($402,113 * 10^{18}$ detik) atau sekitar $12,75 * 10^{12}$ tahun. Sedangkan apabila komputer ini melakukan ekstraksi pada dua karakter pesan yang disisipkan dengan metode LSB akan membutuhkan waktu $(2*8) / 93.01 * 10^{15}$ detik atau $4,1 * 10^{-16}$ detik. Dari contoh perhitungan tersebut dapat dikatakan mengekstrak pesan dengan menggunakan metode *brute force* dari *stego image* yang dihasilkan dari metode *Dynamic Parity Bit* Steganografi membutuhkan waktu yang jauh lebih lama dibandingkan dengan metode LSB.

4. KESIMPULAN

Berdasarkan pada pengujian dan pembahasan hasil yang dihasilkan oleh metode *Dynamic Parity Bit* Steganografi, maka kesimpulan yang diperoleh antara lain sbb:

(i) Dilihat dari segi fungsionalitas, metode *Dynamic Parity Bit* Steganografi dapat menyisipkan dan mengekstrak pesan dengan baik selama pesan yang disisipkan tidak melebihi kapasitas *cover image* yang digunakan. Untuk menghindari penyisipan pesan yang melebihi kapasitas *cover image*, pengguna dapat menghitung jumlah karakter maksimal yang dapat ditampung suatu citra dengan *stego key* tertentu.

(ii) Jumlah karakter pesan maksimal yang dapat ditampung oleh suatu citra *bit*map menggunakan metode *Dynamic Parity Bit* Steganografi lebih sedikit dibandingkan dengan metode LSB. Karakter maksimal yang dapat ditampung dapat dihitung dengan persamaan $N = C\ div\ \left(\frac{D}{K}\right)$. Sedangkan apabila menggunakan metode LSB, karakter maksimal pesan yang dapat ditampung adalah sebanyak *byte* yang dimiliki oleh *cover image* yang digunakan.

(iii) Waktu yang dibutuhkan untuk menyisipkan dan ekstraksi pesan menggunakan metode *Dynamic Parity Bit* Steganografi relatif lebih lama dibandingkan dengan metode LSB. Hal ini disebabkan oleh kompleksitas algoritma *Dynamic Parity Bit* Steganografi yang lebih tinggi dibandingkan dengan metode LSB.

(iv) Perhitungan MSE dan PSNR dari citra hasil penyisipan pesan menggunakan metode *Dynamic Parity Bit* Steganografi menghasilkan nilai yang tidak jauh berbeda dengan citra hasil penyisipan dengan metode LSB.

(v) Keamanan metode *Dynamic Parity Bit* Steganografi lebih tinggi dibandingkan dengan metode LSB karena ekstraksi pesan yang disisipkan dengan metode *Dynamic Parity Bit* Steganografi secara paksa dengan metode brute force membutuhkan waktu yang lebih lama dibandingkan dengan pesan yang disisipkan dengan metode LSB.

5. SARAN

Hasil penelitian ini masih memiliki kekurangan, sehingga dimasa yang akan datang memungkinkan untuk pengembangan penelitian lebih lanjut seperti yang dipaparkan dalam saran-saran berikut ini:

(i) Metode *Dynamic Parity Bit* Steganografi dalam penelitian ini diterapkan untuk menyisipkan teks ke dalam citra *bit*map. Pada penelitian yang akan datang dapat dilakukan penyembunyian informasi dengan jenis dan media penyembunyian yang lain.

(ii) Ketahanan *stego image* yang dihasilkan oleh metode *Dynamic Parity Bit* Steganografi dapat dikatakan rendah karena data tidak dapat diekstrak apabila *stego image* yang dihasilkan dimanipulasi terlebih dahulu. Pada penelitian yang akan datang dapat dilakukan peningkatan ketahanan terhadap *stego image* yang dihasilakan.

DAFTAR PUSTAKA

Cole, E. (2003). Hiding in Plain Sight : Steganography and the Art of Covert Communication. Indiana: Bob Ipsen

Kalita, M., & Tuithung, T. (2016). A Novel Steganographic Method Using 8-Neighboring PVD (8nPVD) and LSB Substitution. *International Conference on System, Signal and Image Processing*, 6-10

Malekmohamadi, H., & Ghaemmaghami, S. (2009). Steganalysis of LSB Based Image Steganography Using Spatial and Frquency Domain Features. *IEEE International Conference on Multimedia and Expo*, 1744-1747

Akhtar, N., Ahamad, V., & Javed, H. (2017). A Compressed LSB Steganography Method. *IEEE International Conference on "Computational Intelligence and Communication technology"*. Aligarh. IEEE

Nurhayati, & Ahmad, S. S. (2016). Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Criptographic Algorithm. *4th International Conference on Cyber and IT Service Management*, 1-6

Arya, R., & Sarahan, R. (2015). Algorithm to Enhance the Robustness and Imperceptibility of LSB. *Second International Converence on Advances in Computing and Communication Engineering (ICACCE)*, 583-587

Bandyopadhyay, P. S., & Banik, B. G. (2012). Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 71-74

Dighe, D. G., & Kapale, N. (2013). Random Insertion Using Data Parity Steganography Technique. *International Journal of Engineering Science and Innovetive Technique*, 364-368

Cheddad, A., Condell, J., Curran, K., & Kevitt, P. M. (2010). Digiral Image Steganography: Survey and Analysis of Current Methods. *Signal Processing 90*, 727-752