IMPLEMENTASI *IMAGE TILLING* PADA PENYEMBUNYIAN PESAN MENGGUNAKAN LSB

Rihartanto[1], Didi Susilo Budi Utomo[2], Ansar Rizal[3]
[1,2,3]Jurusan Teknologi Informasi, Politeknik Negeri Samarinda
e-mail: [1]rihart.c@gmail.com, [2]dsbudiutomo10@gmail.com, [3]anrisal@yahoo.com

ABSTRAK

Dalam era digital saat ini, informasi merupakan aset penting yang dapat digunakan untuk tujuan positif atau tujuan negatif. Karenanya informasi perlu dilindungi. Tidak hanya untuk melindungi informasi yang bersifat rahasia, namun dapat juga untuk tujuan memilah informasi yang sebenarnya dari informasi yang mirip atau bahkan hoax. Dalam penelitian ini, perlindungan informasi dilakukan dengan cara menyembunyikan informasi tersebut ke dalam citra RGB. Metoda yang digunakan adalah LSB dengan mengimplementasikan image tilling atau citra berstruktur ubin. Implementasi citra berstruktur ubin ini mengakibatkan posisi piksel yang digunakan untuk penyembunyian informasi tersebar mengikuti pola tertentu, sesuai dengan jumlah segmen ubin yang ada pada citra. Kriteria steganografi yang dinilai adalah imperceptible, fidelity dan recovery. Pengujian menggunakan ukuran data yang berbeda, mulai 20% sampai dengan mendekati 100% berhasil memenuhi ketiga kriteria tesebut. Hal ini ditunjukkan dengan nilai PSNR sebesar 50.2885 dB untuk kapasitas mendekati 85%, dan yang terendah adalah 49.5947 dB untuk kapasitas mendekati 100%, namun secara visual citra hasil steganografi tidak menunjukkan perbedaan dari citra aslinya.

***Kata Kunci**: Image tilling, LSB, imperceptible, fidelity, recovery*

1. PENDAHULUAN

Informasi merupakan asset berharga yang menjadi komponen utama dalam dunia digital. Karena itu informasi perlu dilindungi, baik dari pengguna yang tidak berhak maupun dari informasi lain yang bersifat hoax. Teknik yang sering kali digunakan untuk melindungi informasi adalah kriptografi dan stenografi. Kriptografi merupakan proses pengubahan pesan asli *(plaintext)* menjadi bentuk lain yang bersifat rahasia *(ciphertext)*. Sedangkan stenografi merupakan proses penyembunyian pesan ke dalam bentuk informasi lainnya.

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan dengan cara tertentu sehingga keberadaan pesan menjadi tersamarkan. Pesan tersebut hanya diketahui oleh pengirim atau penerima pesan saja. Pada umumnya, pesan disembunyikan dalam bentuk yang berbeda dari bentuk pesan aslinya, misalkan dalam gambar, audio, artikel, atau bentuk-bentuk lainnya yang sering disebut sebagai *cover*. *Cover* ini merupakan bentuk yang menyelubungi atau menutupi pesan asli yang dikirim.

Metode yang paling umum diimplementasikan pada steganografi adalah *Least Significant Bit* (LSB) [1]. Teknik atau metoda lainnya diantaranya adalah *Spread Spectrum* [2], *low bit coding* [3], algoritma transformasi, dan *Redundant Pattern Encoding*. Metode LSB paling banyak digunakan karena LSB tidak memerlukan komputasi yang rumit dalam penyembuyian pesan [4]. LSB bekerja dengan cara mengubah atau mengganti nilai bit-bit terakhir data pada *cover* dengan bit-bit pesan yang disembunyikan. Sehingga jika bit-bit terakhir pada *cover* diambil kembali, maka pesan yang disembunyikan dapat dengan mudah diketahui.

Meskipun tidak ada keharusan bahwa *cover* dan pesan yang disembunyikan memiliki bentuk atau format yang berbeda, namun seringkali *cover* bentuk yang berbeda dari pesan yang disembunyikan. Misalkan yang disembunyikan adalah pesan teks, maka *cover* yang digunakan dapat berupa citra atau audio. Jika yang ingin disembunyikan adalah citra, maka *cover* yang digunakan dapat berupa audio atau video. Dalam hal ini, ukuran *cover* selalu lebih besar dari pesan yang disembunyikan, tujuannya tentu saja agar *cover* dapat menampung seluruh isi pesan tersebut.

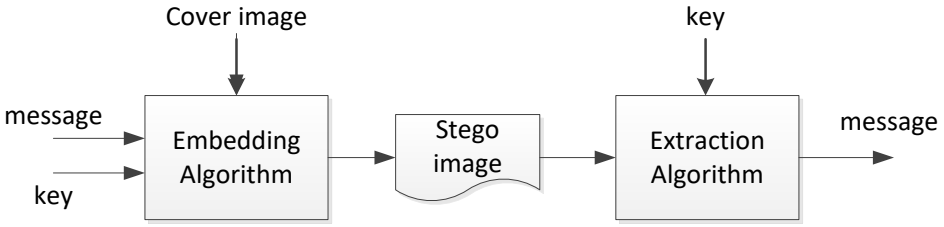
Karena sifat LSB yang sederhana, diperlukan metode tambahan agar pesan yang disembunyikan tidak dengan mudah diketahui. Diantaranya dengan menambahkan proses enkripsi, proses kompresi atau dengan cara peletakan pesan mengikuti pola tertentu ke dalam citra. Pada penelitian ini, penempatan bit-bit pesan dilakukan dengan cara mengubah cover menjadi citra berstruktur ubin sebelum dilakukan penyembunyian pesan. Setelah itu, cover dikembalikan menjadi bentuk semula.

2. METODE PENELITIAN

2.1 Steganografi

Dalam bidang keamanan data, steganografi digunakan untuk menyembunyikan pesan rahasia ke dalam cover-media. Pesan disamarkan sedemikian rupa sehingga tidak diketahui oleh pihak lain. Steganografi dapat diimplementasikan pada berbagai macam bentuk data seperti teks, citra, audio, dan video. Terdapat sejumlah kriteria utama dalam menghasilkan stego-media yang baik, yaitu imperceptible, fidelity dan recovery. Imperceptible yaitu keberadaan pesan rahasia tidak dapat dipersepsikan secara inderawi, dalam arti stego-media yang berisi pesan, secara visual atau audio visual sulit dibedakan dari cover-media. Fidelity berarti kualitas media penampung tidak mengalami banyak perubahan setelah penyembunyian pesan dilakukan, dan recovery yang berarti pesan rahasia yang disembunyikan dapat dimunculkan kembali.

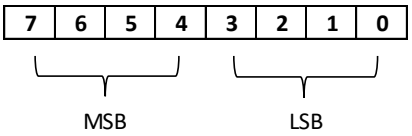
Secara umum, proses steganografi ditunjukkan pada Gambar 1. Pada gambar tersebut diasumsikan bahwa pesan yang akan disembunyikan adalah teks dan yang digunakan sebagai cover adalah citra. Proses embedding untuk menghasilkan stego-media memerlukan masukan berupa pesan yang akan disembunyikan dan cover untuk menampung pesan. Sedangkan pada proses ekstraksi, sebagai masukan adalah stego-media yang dihasilkan pada proses sebelumnya. Kunci bersifat opsional, tergantung teknik atau metoda apa saja yang terlibat pada proses steganografi tersebut.



Gambar 1. Model Steganografi

LSB adalah salah satu algoritma yang banyak digunakan untuk menyembunyikan suatu pesan ke dalam cover. Steganografi dengan LSB dilakukan dengan cara memodifikasi bit-bit pada kelompok bit LSB pada setiap piksel yang terdapat pada cover-image. Bit-bit LSB ini dimodifikasi dengan menggantikannya dengan bit-bit pesan yang ingin disembunyikan.

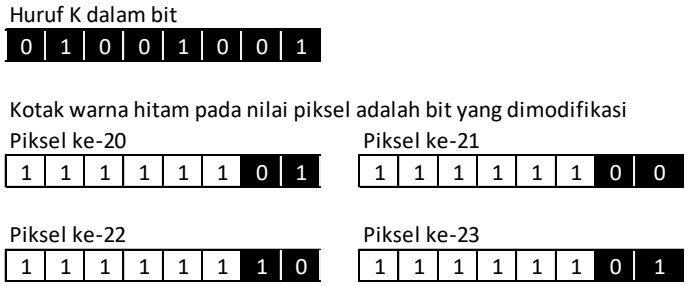
Posisi bit-bit MSB dan LSB diilustrasikan pada Gambar 2, yang menunjukkan tingkat signifikansi posisi bit dalam satu byte. Posisi paling kanan (posisi 0) disebut sebagai least significant atau paling kurang penting, dan yang paling kiri (posisi 7) adalah most significant atau yang paling penting. Setiap satu byte pesan yang akan disembunyikan akan membutuhkan ruang sebanyak delapan byte pada cover-image, jika modifikasi hanya dilakukan pada bit terakhir saja. Namun jika modifikasi dilakukan pada dua bit LSB maka satu byte pesan akan memerlukan empat byte pada cover. Perubahan nilai pada LSB relatif tidak memberikan perubahan yang berarti pada citra secara keseluruhan.



Gambar 2. Posisi bit-bit MSB dan LSB

Sebagai contoh, misalkan huruf K yang memiliki nilai ASCII 75 akan disisipkan pada piksel-piksel berwarna putih mulai piksel ke-20 sampai piksel ke-27. Modifikasi hanya dilakukan pada satu bit terakhir setiap piksel, Gambar 3 mengilustrasikan penempatan setiap bit huruf K ke dalam 8 piksel pada citra cover.

Penggunaan LSB dengan memodifikasi bit-bit terakhir pada citra, secara visual tidak menunjukkan perbedaan yang signifikan dengan citra aslinya. Namun metoda ini memiliki kekurangan diantaranya dari sisi keandalannya. Metoda LSB ini sangat sensitif terhadap proses *filtering*, *scalling*, rotasi atau *cropping* yang dapat mengakibatkan kerusakan pada pesan yang telah disembunyikan.



Gambar 3. Penyembunyian huruf K ke dalam 4 piksel berwarna putih

Pengukuran kualitas citra hasil steganografi dilakukan menggunakan peak signal to noise ratio (PNSR), dimana untuk mendapatkan nilai PNSR tersebut terlebih dulu dihitung nilai MSE-nya. MSE dihitung menggunakan Persamaan (1) dan PNSR dihitung menggunakan Persamaan (2).

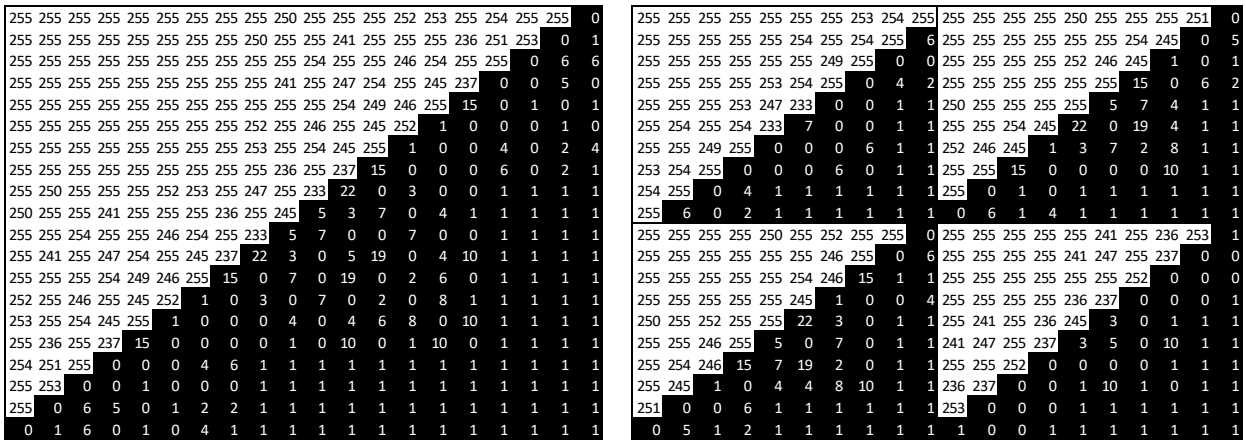
$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m} \sum_{j=0}^{n} \left(X_{ij} - X'_{ij} \right)^2 \quad (1)$$

$$PNSR = 10 \log_{10} \frac{I^2}{MSE} \quad (2)$$

X_{ij} adalah intensitas piksel baris ke *i* dan kolom ke *j* dari *cover-image*, X'_{ij} adalah intensitas piksel baris ke *i* dan kolom ke *j* dari *stego-image*, *m* dan *n* adalah ukuran baris dan kolom *cover-image*, dan *I* adalah intensitas piksel maksimum. Untuk citra 8 bit maka *I* = 255. Semakin besar PSNR (semakin kecil MSE) maka kualitas *stego image* akan semakin baik. Nilai PSNR yang diharapkan adalah di atas 50dB lebih tinggi dibanding dengan penelitian yang sudah ada sebelumnya [5], [6].

2.2 Image tilling

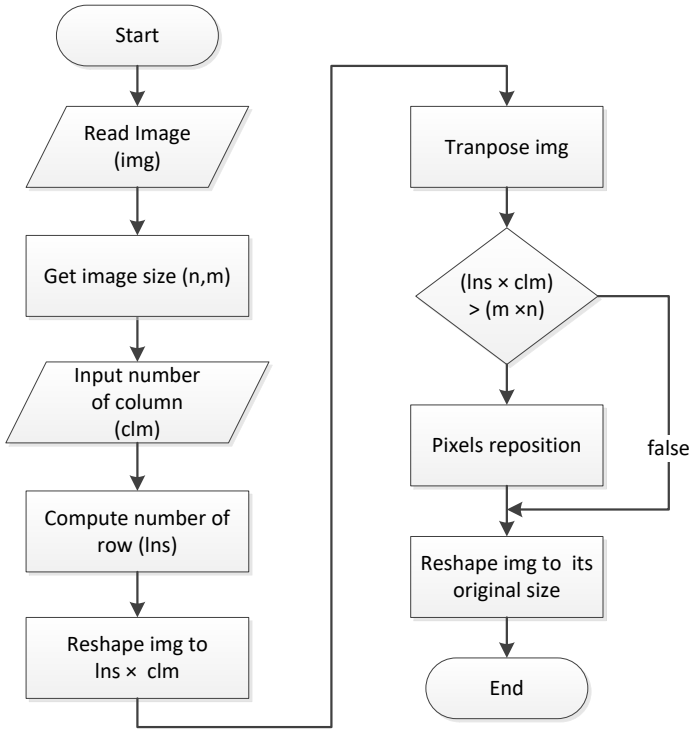
Image tilling merupakan pembentukan citra berstruktur ubin dengan cara mengimplementasikan transposisi kolumnar [7]. Yang dimaksud dengan citra berstruktur ubin disini adalah citra yang terdiri dari segmen citra yang berukuran sama atau mirip. Setiap segmen ubin secara visual merupakan miniatur dari citra aslinya seperti ditunjukkan pada Gambar 4. Proses transposisi tidak mengubah nilai piksel dari citra, namun mengubah posisi dari piksel-piksel tersebut sehingga menghasilkan citra yang berbeda. Dalam hal ini adalah citra berstruktur ubin. Piksel bernilai mendekati nol akan cenderung berwarna hitam sementara piksel bernilai mendekati 255 akan cenderung berwarna putih.



Gambar 4. Citra asli (kiri) dan citra berstruktur ubin (kanan)

Proses pembentukan citra berstruktur ubin ini mengikuti tahapan pada flowchart yang ditunjukkan pada Gambar 5. Dimulai dengan membaca citra, ukuran citra yang diambil adalah jumlah baris dan jumlah kolom yang menyatakan resolusi citra. Jumlah kolom merupakan kolom matriks tujuan yang digunakan sebelum dilakukan operasi transposisi. Jumlah baris matriks tujuan dihitung berdasarkan jumlah kolom yang dimasukkan, dengan syarat bahwa tidak ada data dari citra asal yang hilang. Jumlah kolom matrik yang dimasukkan ini akan menentukan jumlah segmen ubin yang dihasilkan nantinya.

Proses transposisi dilakukan setelah citra asli diubah bentuk menjadi berukuran kolom dan baris yang baru. Setelah transposisi dilakukan selanjutnya matriks tersebut dikembalikan ke ukuran aslinya, untuk menghasilkan citra berstruktur ubin yang memiliki ukuran yang sama dengan citra aslinya. Jumlah kolom sebelum dilakukan transposisi akan menentukan jumlah segmen ubin yang dihasilkan. Jumlah segmen adalah pangkat dua dari jumlah kolom yang digunakan sebelum transposisi.



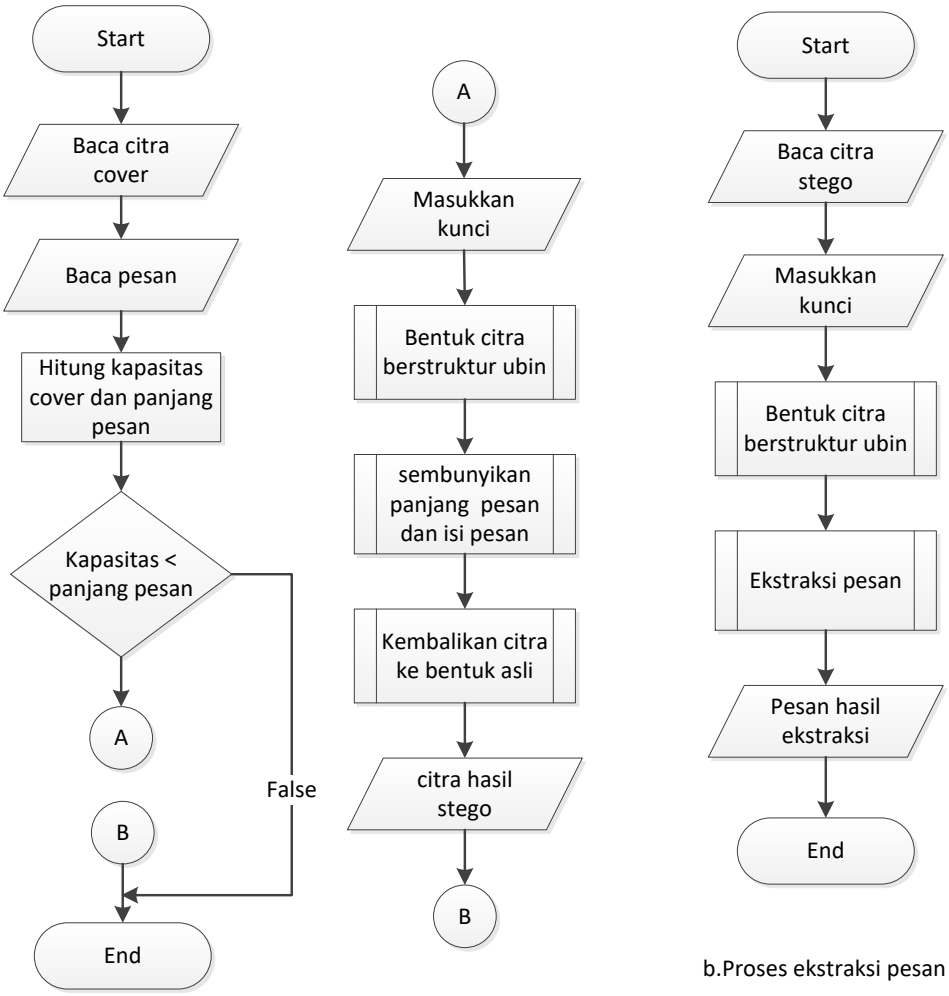
Gambar 5. Implementasi transposisi kolumnar untuk pembentukan citra berstruktur ubin [7].

2.3 Implementasi LSB memanfaatkan citra berstruktur ubin

Penyembunyian pesan dilakukan dengan cara mengganti dua bit terakhir dari nilai piksel pada cover dengan dua bit pesan yang disembunyikan. Pesan dapat berbentuk teks atau data biner lainnya. Data dari pesan yang disembunyikan dibedakan menjadi dua macam, yaitu jumlah atau ukuran pesan serta isi pesan itu sendiri. Dari tiga komponen citra RGB, komponen R dan komponen B digunakan sebagai tempat penyembunyian isi pesan, sementara komponen G digunakan untuk penyembunyian panjang pesan.

Komponen R dan B digunakan untuk tempat penyembunyian isi pesan dikarenakan perubahan nilai pada kedua komponen ini memberi dampak visual yang relatif rendah dibandingkan dengan perubahan yang terjadi pada komponen G. Panjang pesan disimpan dalam bentuk integer 24 bit, sehingga jumlah piksel maksimal yang mengalami perubahan nilai pada komponen G hanya 12 piksel saja.

Sebelum panjang pesan dan isi pesan disembunyikan ke dalam citra, terlebih dahulu citra yang digunakan sebagai cover diubah menjadi citra berstruktur ubin. Setelah itu panjang pesan dan isi disembunyikan ke dalam cover pada piksel yang berurutan. Modifikasi pada komponen B hanya dilakukan pada baris genap sementara pada komponen R pada baris ganjil. Setelah seluruh data disembunyikan, citra berstruktur ubin dikembalikan ke bentuk aslinya, sehingga secara visual citra hasil steganografi adalah citra yang mirip dengan citra aslinya. Alur proses penyembunyian pesan ke dalam citra dengan metoda LSB yang memanfaatkan citra berstruktur ubin ditunjukkan pada Gambar 6.



Gambar 6. Tahapan proses penyembunyian dan ekstraksi pesan mengimplementasikan citra berstruktur ubin

Penyembunyian pesan hanya dapat dilakukan selama kapasitas daya tampung mencukupi untuk seluruh isi pesan. Setelah persyaratan ini terpenuhi, kemudian dimasukkan kunci yang berupa angka yang lebih besar dari satu dan lebih kecil dari setengah lebar citra. Misalkan citra yang digunakan memiliki lebar 100 piksel maka kunci yang dapat digunakan adalah dua sampai 49. Semakin besar angka yang digunakan maka akan semakin banyak segmen ubin yang dihasilkan. Isi pesan dan panjang disembunyikan pada citra berstruktur ubin. Setelah semua data disembunyikan, citra berstruktur ubin dikembalikan ke bentuk aslinya untuk mendapatkan citra hasil steganografi.

3. HASIL DAN PEMBAHASAN

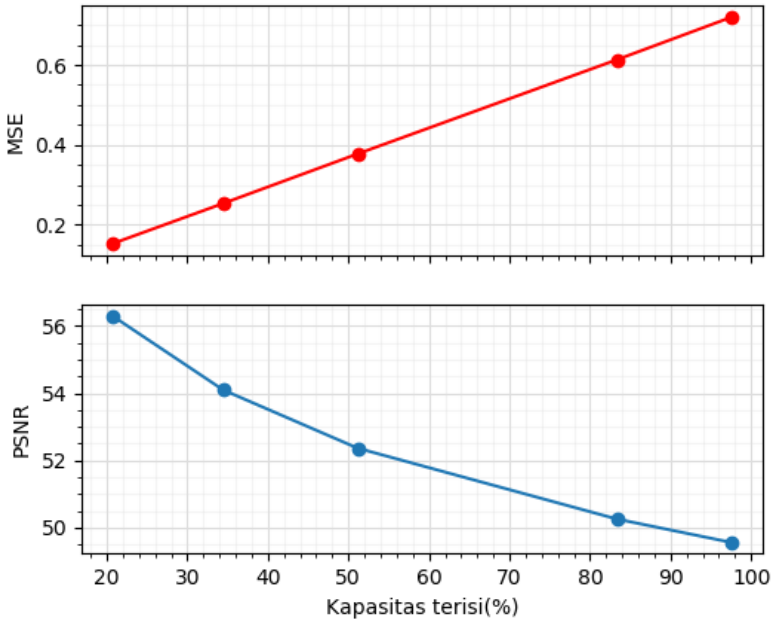
Citra yang digunakan sebagai cover adalah citra lena yang berukuran 225x225 piksel. Citra ini mampu menampung isi pesan maksimal sebesar 12656 byte. Sedangkan teks uji diambil dari bagian pendahuluan sampai paragraf ketiga bagian hasil dan pembahasan dari artikel ini dengan menghilangkan seluruh gambar, rumus, tabel dan baris kosong. Secara keseluruhan teks uji ini terdiri dari 1694 kata dan 12345 karakter. Untuk tujuan pengujian, teks uji dibedakan menjadi empat file teks yang berisi jumlah karakter yang berbeda. Hal ini dilakukan untuk mengetahui penurunan kualitas citra hasil steganografi terhadap penambahan jumlah data yang disembunyikan.

Gambar 7. Citra asli (kiri), citra berstruktur ubin (tengah) dan citra hasil steganografi (kanan)

Citra asli, citra berstruktur ubin yang setelah penyembunyian pesan dan citra hasil steganografi ditunjukkan pada Gambar 7, sementara hasil pengujian kualitas citra ditunjukkan pada Tabel 1. Meskipun ukuran pesan yang disembunyikan mendekati 100% dari kapasitas maksimal, secara visual tidak terlihat perbedaan yang signifikan antara citra hasil steganografi dibandingkan dengan citra aslinya. Dapat diasumsikan bahwa kika pesan yang disembunyikan lebih sedikit, maka keberadaan pesan akan menjadi semakin sulit untuk dikenali. Hal ini menunjukkan bahwa *imperceptible* yaitu keberadaan pesan pada covermedia tidak mudah dikenali menggunakan indera visual, yang merupakan salah satu kriteria steganografi yang baik telah terpenuhi.

Tabel 1. Hasil pengujian penyembunyian pesan teks

File teks	Jumlah Karakter	kapasitas (%)	MSE	PSNR
teksuji1.txt	2623	20.73	0.1510	56.3411
teksuji2.txt	4361	34.46	0.2526	54.1072
teksuji3.txt	6474	51.15	0.3728	52.4160
teksuji4.txt	10548	83.34	0.6085	50.2885
teksuji5.txt	12345	97.54	0.7139	49.5947



Gambar 8. Pengaruh ukuran pesan terhadap nilai MSE dan PSNR

Nilai PSNR digunakan untuk mengukur kualitas citra hasil steganografi. Asumsi yang digunakan dalam penelitian ini adalah citra dianggap memiliki kualitas yang baik jika nilainya lebih besar dari 50 dB. Dari

Tabel 1 dapat dilihat bahwa meningkatnya kapasitas pesan yang disembunyikan berpengaruh secara langsung pada kenaikan nilai MSE, yang selanjutnya berdampak pada penurunan nilai PSNR.

Pengujian dilakukan menggunakan data berukuran mulai dari 20% sampai mendekati 100% kapasitas yang dapat ditampung. Jika satu halaman teks A4 yang diketik menggunakan font times new roman 12 dengan jarak satu spasi rata-rata terdiri dari 2800 sampai 2900 karakter, maka teksuji5 berukuran lebih dari 4 halaman teks tersebut. Penggunaan data yang relatif besar ini bertujuan untuk melihat seberapa signifikan penurunan kualitas citra, secara visual maupun menurut hasil pengukuran menggunakan PNSR.Hasil pengujian pada Tabel 1 menunjukkan bahwa peningkatan ukuran pesan yang disembunyikan linier terhadap peningkatan nilai MSE. Kenaikan nilai MSE ini berakibat pada penurunan nilai PSNR secara logaritmik seperti ditunjukkan pada Gambar 8. Namun meskipun nilai PSNR mengalami penurunan, bahkan sampai sedikit lebih rendah dari nilai yang diharapkan untuk ukuran pesan mendekati 100% dari kapasitas maksimum, citra yang dihasilkan masih dapat dikatakan berkualitas baik. Sehingga kriteria steganografi berikutnya, yaitu fidelity juga terpenuhi.

Pesan yang disembunyikan harus dapat diambil kembali atau diekstraksi. Ini merupakan kriteria steganografi yang ketiga yaitu *recovery* juga terpenuhi. Dalam penelitian ini, merujuk pada flowchart pada Gambar 6, agar pesan yang disembuntikan dapat diambil, terlebih dahulu citra hasil steganografi diubah bentuk menjadi citra berstruktur ubin. Setelah itu barulah pesan dapat diekstraksi. Pemanfaatan citra berstruktur ubin pada penyembunyian pesan ini secara tidak langsung juga meningkatkan keamanan dari pesan itu sendiri. Karena penggunaan citra berstruktur ubin ini mengakibatkan urutan piksel yang digunakan untuk penyembunyian bit-bit pesan menjadi tersebar mengikuti pola tertentu. Dalam hal ini adalah sesuai dengan jumlah segmen ubin yang ada pada citra. Jumlah segmen ubin ini mengikuti nilai kunci yang digunakan, karena jumlah segmen adalah nilai pangkat dua dari nilai kunci. Sebagai contoh, jumlah segmen ubin pada Gambar 7 adalah sembilan buah yang merupakan pangkat dua dari nilai kunci, yaitu tiga. Semakin besar besar angka yang digunakan sebagai kunci, maka akan semakin banyak segmen ubin yang dihasilkan.

4. KESIMPULAN

Penelitian ini menunjukkan penggunaan citra bersegmen ubin dalam steganografi secara tidak langsung berguna untuk meningkatkan keamaan dari pesan yang disembunyikan. Hal ini dikarenakan jika jumlah segmen ubin yang digunakan pada saat ekstraksi berbeda dengan yang digunakan pada saat penyembunyian data, maka pesan hasil ekstraksi akan sangat berbeda dengan pesan aslinya. Penelitian ini juga membuktikan bahwa tiga kriteria kripografi yang baik dapat dipenuhi dalam penyembunyian pesan menggunakan metode LSB. Citra hasil steganografi masih tergolong baik yang ditunjukkan dengan nilai PNSR yang lebih besar dari 50dB untuk ukuran pesan mendekati 85% dari kapasitas maksimum. Sementara untuk ukuran pesan mendekati kapasitas maksimum nilai PNSR adalah sebesar 49.5947. Nilai ini sedikit lebih rendah dibanding nilai PNSR yang diharapkan. Namun secara visual, citra hasil steganografi tidak berbeda nyata dibandingkan citra aslinya.

UCAPAN TERIMA KASIH

Terimakasih penulis sampaikan atas dukungnya kepada P3M Politeknik Negeri Samarinda dan Direktorat Jendral Penguatan Riset dan Pengembangan Kementerian Riset, Teknologi dan Pendidikan Tinggi sesuai dengan kontrak nomor 1207/PL7/LK/2019 dan 151/SP2H/LT/DRPM/2019.

DAFTAR PUSTAKA

[1]. Champakamala, B. S., Padmini, K. and Radhika, D. K., 2014, Least Significant Bit algorithm for image steganography Overview of Steganography, *International Journal of Advanced Computer Technology (IJACT)*, Vol. 3 No. 4, hal. 34–38.

[2]. Assyahid, M. M., Rihartanto, R. and Utomo, D. S. B., 2018, Implementasi Steganografi Pesan Text ke Dalam Audio Dengan Metode Spread Spectrum, *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi (SAKTI)*, Samarinda, hal. 27–34.

[3]. Wakiyama, M., Hidaka, Y. and Nozaki, K., 2010, An audio steganography by a low-bit coding method with wave files, *Proceedings of 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2010*, hal. 530–533. Darmstadt, October, doi: 10.1109/IIHMSP.2010.135

[4]. Patil, S. A. and Adhiya, K. P., 2012, Hiding Text in Audio Using LSB Based Steganography', *Information and Knowledge Management*, Vol. 2 No. 3, hal. 8–15. Available at: www.iiste.org.

[5]. Li, P. and Lu, A., 2018, LSB-based Steganography Using Reflected Gray Code for Color Quantum Images, *International Journal of Theoretical Physics*. Vol. 57 No. 5, hal. 1516–1548.

[6]. Pandian, N., 2014, An Image Steganography Algorithm Using Huffman and Interpixel Difference Encoding, *International Journal of Computer Science & Security*, Vol. 8 No. 6, hal. 202–215.

[7]. Rihartanto, R., Supriadi, S. and Utomo, D. S. B., 2018, Image Tiling Using Columnar Transposition, *Proceedings of International Conference on Applied Information Technology and Innovation (ICAITI)*. Padang: IEEE, September, hal. 118–123. doi: 10.1109/ICAITI.2018.8686758.