PENYEMBUNYIAN TEKS TERENKRIPSI PADA CITRA RGB MENGGUNAKAN METODA LSB DENGAN POLA ZIG-ZAG

HIDING ENCRYPTED TEXT IN RGB IMAGE USING THE LSB METHOD WITH ZIG-ZAG PATTERNS

Didi Susilo Budi Utomo[1], Jems[2], Hari Purwadi[3], Rihartanto[4*]
[1,2,3,4]Politeknik Negeri Samarinda
Jurusan Teknologi Informasi
Jl. Cipto Mangunkusumo, Kampus Gn. Lipan, Samarinda Seberang, Samarinda, 75131
E-mail: dsbudiutomo10@gmail.com, j16615043@gmail.com, al1fzharfan@yahoo.co.id, rihart.c@gmail.com

Naskah diterima tanggal 24/9/ 2019, direvisi tanggal 3/12/ 2019, disetujui pada tanggal 6/12/2019

Abstract

The widespread use of digital media currently tends to increase public awareness about the importance of information security. Not only to protect confidential and personal information, but also for the purpose of sorting out real information from hoaxes. Securing Information can be done using techniques in encryption and steganography. In this study, the LSB method with a zig-zag pattern is used to hide messages that are encrypted using a rail-fence cipher. The steganography attributes assessed are imperceptible, fidelity and recovery. The implementation of steganography using LSB method with zig-zag pattern using message sizes ranging from 10% up to 100% succeeded in fulfilling the three good steganographic attributes. This is indicated by a PSNR value of 52.5564 dB for capacities close to 100% where visually the results of steganography do not show differences from the original image.

***Keywords** : LSB, Zig-zag pattern, Rail-fence cipher, PSNR*

Abstrak

Maraknya penggunaan media digital saat ini cenderung meningkatkan kesadaran masyarakat tentang pentingnya arti perlindungan informasi. Tidak hanya untuk melindungi informasi rahasia dan pribadi, namun juga untuk tujuan memilah informasi sebenarnya dari yang bersifat hoax. Perlindungan informasi dapat dilakukan menggunakan teknik-teknik dalam enkripsi dan steganografi. Pada penelitian ini, metode LSB dengan pola zig-zag digunakan untuk menyembunyikan pesan yang dienkripsi menggunakan rail-fence cipher. Atribut steganografi yang dinilai adalah imperceptible, fidelity dan recovery. Implementasi steganografi menggunakan metoda LSB dengan pola zig-zag menggunakan ukuran pesan mulai dari 10% sampai dengan mendekati 100% berhasil memenuhi ketiga atribut steganografi yang baik tesebut. Hal ini ditunjukkan dengan nilai PSNR sebesar 52.5564 dB untuk kapasitas mendekati 100% dimana secara visual citra hasil steganografi tidak menunjukkan perbedaan dari citra aslinya.

Kata Kunci : LSB, Pola zig-zag, Rail-fence cipher, PSNR

PENDAHULUAN

Kerahasiaan informasi merupakan hal penting yang menjadi semakin krusial seiring dengan maraknya penggunaan media digital. Media sosial (medsos) adalah contoh konkrit penggunaan data digital dalam berbagai bentuk, dengan tujuan yang sangat beragam. Mulai dari sekedar obrolan hingga masalah yang sangat serius dan sensitif. Informasi yang ada juga seringkali tidak dapat begitu saja dapat diangap benar, karena kandungan informasi yang bersifat 'hoax' cenderung tinggi (Ginting, Manongga, & Sembiring, 2018). Demikian pula, medsos dapat dikatakan sebagai saluran komunikasi yang terbuka dan relatif tidak aman karena dapat diakses oleh semua orang. Sehingga perlu langkah

pengamanan pada pengiriman informasi penting agar informasi tersebut terlindungi dan tidak dapat disusupi oleh konten hoax.

Berbagai usaha dilakukan untuk menjamin agar data penting tidak bisa diakses oleh sembarang orang. Teknik yang umum digunakan untuk mengamankan pesan penting dan rahasia dari orang-orang yang tidak berhak adalah kriptografi. Teknik ini merupakan proses pengubahan pesan dari teks asli *(plaintext)* menjadi bentuk lainnya yang bersifat rahasia *(ciphertext)*. Namun penerapan teknik kriptografi masih memiliki kelemahan, diantaranya adalah munculnya kecurigaan dari pihak lain bahwa informasi tersebut bersifat rahasia, sehingga menimbulkan niat untuk mengetahui informasi yang sebenarnya.

Selain kriptografi teknik yang dapat digunakan untuk mengamankan informasi adalah teknik steganografi. Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan dengan cara tertentu sehingga keberadaan pesan tersebut tidak disadari selain oleh pengirim atau penerima pesan. Pada umumnya, pesan steganografi muncul dalam bentuk lain seperti gambar, audio, artikel, daftar belanjaan, atau bentuk-bentuk lainnya yang sering disebut sebagai *cover*. *Cover* ini merupakan bentuk yang menyelubungi atau menutupi pesan asli yang dikirim.

Steganografi dapat dilakukan dengan berbagai macam metode, diantaranya adalah *Least Significant Bit* (LSB), *Spread Spectrum* (Assyahid, Rihartanto, & Utomo, 2018), *low bit coding* (Wakiyama, Hidaka, & Nozaki, 2010), algoritma transformasi, dan *Redundant Pattern Encoding*. Metode LSB termasuk metode yang paling umum (Champakamala, Padmini, & Radhika, 2014) digunakan dalam penyembunyian pesan. Salah satu alasannya adalah karena LSB tidak memerlukan komputasi yang rumit dalam penyembuyian pesan (Patil & Adhiya, 2012). LSB bekerja dengan cara mengubah nilai bit terakhir data pada *cover* dengan bit-bit pesan yang disembunyikan. Sehingga secara sederhana, jika setiap bit terakhir pada *cover* diambil kembali, maka pesan yang disembunyikan dapat segera diketahui.

Karena sifat LSB yang sederhana, diperlukan metode tambahan agar pesan yang disembunyikan tidak dengan mudah diketahui. Dalam penelitian ini, teknik yang digunakan adalah dengan cara melakukan enkripsi sebelum pesan disembunyikan, dan menerapkan pola zig-zag saat proses penyembunyiannya. Dengan cara ini kekurangan dari enkripsi yang mudah menimbulkan kecurigaan tentang adanya data rahasia dapat dikaburkan dengan steganografi karena pesan tersebut menjadi tersembunyi dan tidak mudah menarik perhatian. Sementara penggunaan pola zig-zag merupakan pengamanan tambahan agar pesan yang disembunyikan tidak dapat diekstraksi dengan mudah.

Rail-fence cipher merupakan salah satu teknik enkripsi untuk menyandikan pesan teks dengan cara mengubah posisi karakter secara diagonal atau zig zag (Annalakshmi & Padmapriya, 2013; Siahaan, 2016). Rail-fence cipher termasuk algoritma enkripsi sederhana sehingga tidak memerlukan kemampuan komputasi yang tinggi. Meskipun algoritma ini relatif mudah untuk dipecahkan (Dar, 2014), namun ketika dikombinasikan penggunaannya dengan metoda LSB (Centina, 2017), diharapkan kedua metode sederhana ini mampu saling menutupi kelemahannya masing-masing.

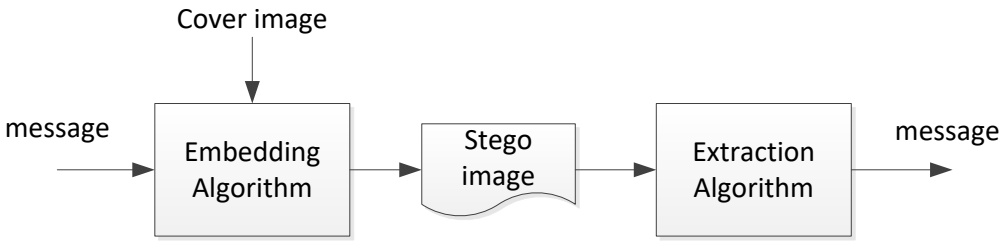
METODA DAN MATERIAL

a. 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. Ada tiga 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 sudah disisipi pesan, secara visual atau audio visual tidak berbeda dengan cover aslinya. *Fidelity*

berarti kualitas media penampung tidak mengalami banyak perubahan setelah penyisipan pesan dilakukan, dan *recovery* yang berarti pesan rahasia yang disembunyikan dapat dimunculkan kembali.

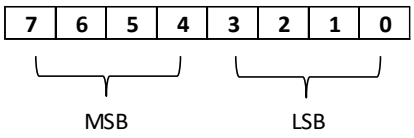
Secara umum, proses steganografi ditunjukkan pada Gambar 1. Pada gambar tersebut diasumsikan bahwa pesan yang akan disembunyikan adalah teks dan yang digunakan sebagai cover adalah citra. Proses embedding untuk menghasilkan stego-media memerlukan masukan berupa pesan yang akan disembunyikan dan cover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



Gambar 1. Model Steganografi

LSB adalah salah satu algoritma yang dapat digunakan untuk menyisipkan suatu pesan ke dalam cover image. Steganografi dengan LSB dilakukan dengan memodifikasi bit-bit yang termasuk bit LSB pada setiap byte warna pada sebuah pixel yang terdapat pada cover-image. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada pada cover image 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. Jika modifikasi hanya dilakukan pada bit terakhir saja, maka setiap satu byte pesan yang akan membutuhkan ruang sebanyak delapan byte pada cover-image. 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 huruh 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 cover image.

Gambar 3. Penyembunyian huruf K ke dalam 8 piksel berwarna putih pada cover image

Penggunaan LSB dengan memodifikasi bit terakhir pada citra, secara visual tidak menunjukkan perbedaan 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 disisipkan.

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).

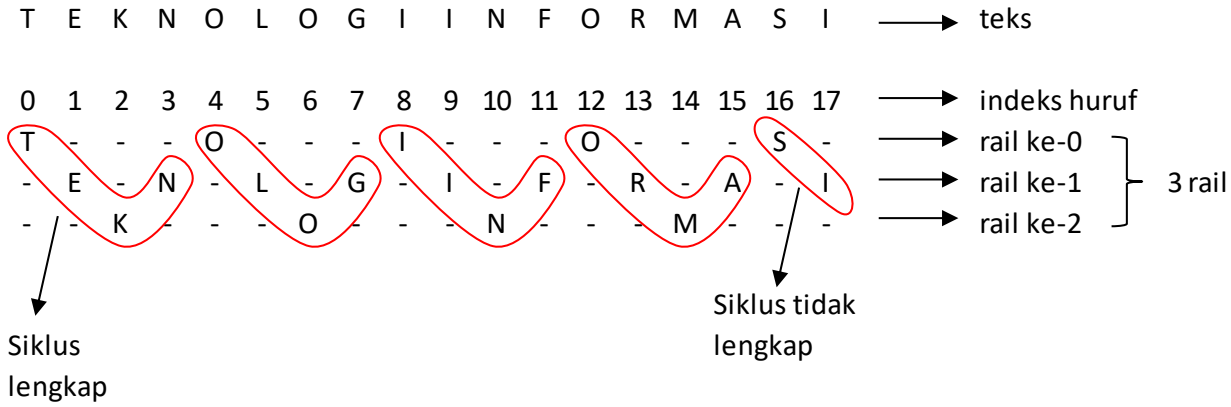
$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m} \sum_{j=0}^{n} \left(X_{ij} - X'_{ij}\right)^2 \quad (1)$$

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

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 (Li & Lu, 2018; Pandian, 2014).

b. Rail-fence Cipher

Rail-fence Cipher adalah salah bentuk cipher transposisi yang namanya diambil dari cara teks disandikan. Cipher transposisi adalah metode enkripsi dimana posisi yang merujuk setiap karakter plaintext digeser atau diubah dengan cara tertentu sehingga ciphertext yang dihasilkan merupakan permutasi dari plaintext. Pada rail-fence cipher, teks ditulis ke bawah pada rel berurutan secara zig-zag sehingga membentuk pagar imajiner. Pesan kemudian dibaca secara horizontal menurut relnya masing-masing. Misalkan teks "`JURUSAN TEKNOLOGI INFORMASI`" ditulis pada tiga buah rail, dengan asumsi spasi dan tanda baca diabaikan sehingga jumlah hurufnya menjadi 18. Ilustrasi penulisan rail-fence ditunjukkan pada Gambar 4.



Gambar 4. Ilustrasi pembentukan fence dengan tiga rail

Setiap huruf diletakkan secara berurutan mulai dari rel ke-0 sampai rel ke-2 dengan arah diagonal. Setelah mencapai rel ke-2, peletakannya pada rel dilakukan dengan arah yang berlawanan menuju rel ke-0 kembali. Jika peletakan ini dilakukan pada semua huruf yang ada, maka akan dihasilkan sebuah bentuk pagar dengan pola zig-zag. Satu siklus lengkap adalah jumlah huruf yang diperlukan untuk membentuk pola zig-zag yang dimulai dari rel ke-0 sampai mendekati rel ke-0 kembali, dalam hal ini sampai rel ke-1. Jika jumlah rel yang digunakan adalah tiga, maka satu siklus lengkap akan terdiri dari empat

huruf. Jumlah huruf siklus lengkap ini dapat dihitung menggunakan Persamaan (3).

$$cycle = (2 \times rail) - 2 \qquad (3)$$

Memanfaatkan Persamaan (1) ini juga dapat diketahui jumlah huruf yang ada pada siklus tidak lengkap, yaitu dengan cara melakukan operasi modulus terhadap jumlah huruf pada teks dengan jumlah huruf pada siklus lengkap. Untuk ilustrasi pada Gambar 4, jumlah huruf pada siklus tidak lengkap adalah dua, yang diperoleh dari hasil modulus 18 dengan 4.

Untuk mengetahui pada rel keberapa sebuah huruf akan diletakkan dapat dihitung menggunakan Persamaan (4). i adalah posisi atau indeks dari huruf yang akan diletakkan pada rail.

$$rpos = \begin{cases} mod(i, cycle) & : K1 \\ mod(-(mod(i, cycle), cycle) & : K2 \end{cases} \quad (4)$$

K1 adalah jika *mod(i, cycle)* < *cycle/2*, sementara *K2* adalah jika *mod(i, cycle)* ≥ *cycle/2*.

Zig-zag pertama dimulai dari baris ke-0 kolom ke-0 hingga kolom terakhir. Dilanjutkan dengan zig-zag kedua yang dimulai dari baris ke-2 kolom ke-0 hingga baris terakhir, dan seterusnya sampai akhir baris dimana masih dapat dihasilkan pola zig-zag lengkap. Pemberian jarak satu piksel antar baris zig-zag bertujuan untuk memastikan bahwa terdapat cukup banyak pixel yang tidak mengalami perubahan nilai untuk menjaga kualitas hasil steganografi agar tetap mendekati citra aslinya.

Jumlah rel adalah jumlah baris yang digunakan untuk membentuk pola zig-zag. Jumlah rel yang digunakan berpengaruh terhadap banyaknya piksel yang dapat digunakan untuk penyembunyian pesan. Semakin besar nilai rel yang digunakan maka akan semakin sedikit jumlah pola zig-zag yang dapat dihasilkan, yang pada akhirnya menurunkan jumlah piksel yang dapat digunakan untuk penyembunyian pesan. Jumlah zig-zag dan jumlah piksel ini dapat

Hasil enkripsi diperoleh dengan cara membaca setiap huruf pada rel secara horizontal dari kiri ke kanan, dimulai dari rel ke-0 sampai rel terakhir. Untuk contoh pada Gambar 4, hasil enkripsinya adalah `TOIOS ENLGIFRAI KONM`. Proses dekripsi dilakukan dengan cara meletakkan kembali setiap huruf pada posisi yang sesuai pada rail-nya masing-masing. Setelah itu dibaca menurut arah zig-zag mulai huruf pertama pada rel ke-0 sampai huruf terakhir.

c. Implementasi LSB dengan Pola Ziz-Zag

Penyembunyian pesan dilakukan dengan cara mengganti dua bit terakhir dari nilai piksel dengan dua bit pesan yang disembunyikan. Pesan yang disembunyikan adalah hasil enkripsi menggunakan rail-fence cipher. Pola zig-zag dilakukan mengikuti karakteristik dari rail-fence cipher. Ilustrasi pola posisi pixel yang digunakan untuk menyembunyikan pesan pada citra berukuran 20×20, ditunjukkan pada Gambar 5.

dihitung menggunakan Persamaan (5) dan Persamaan (6).

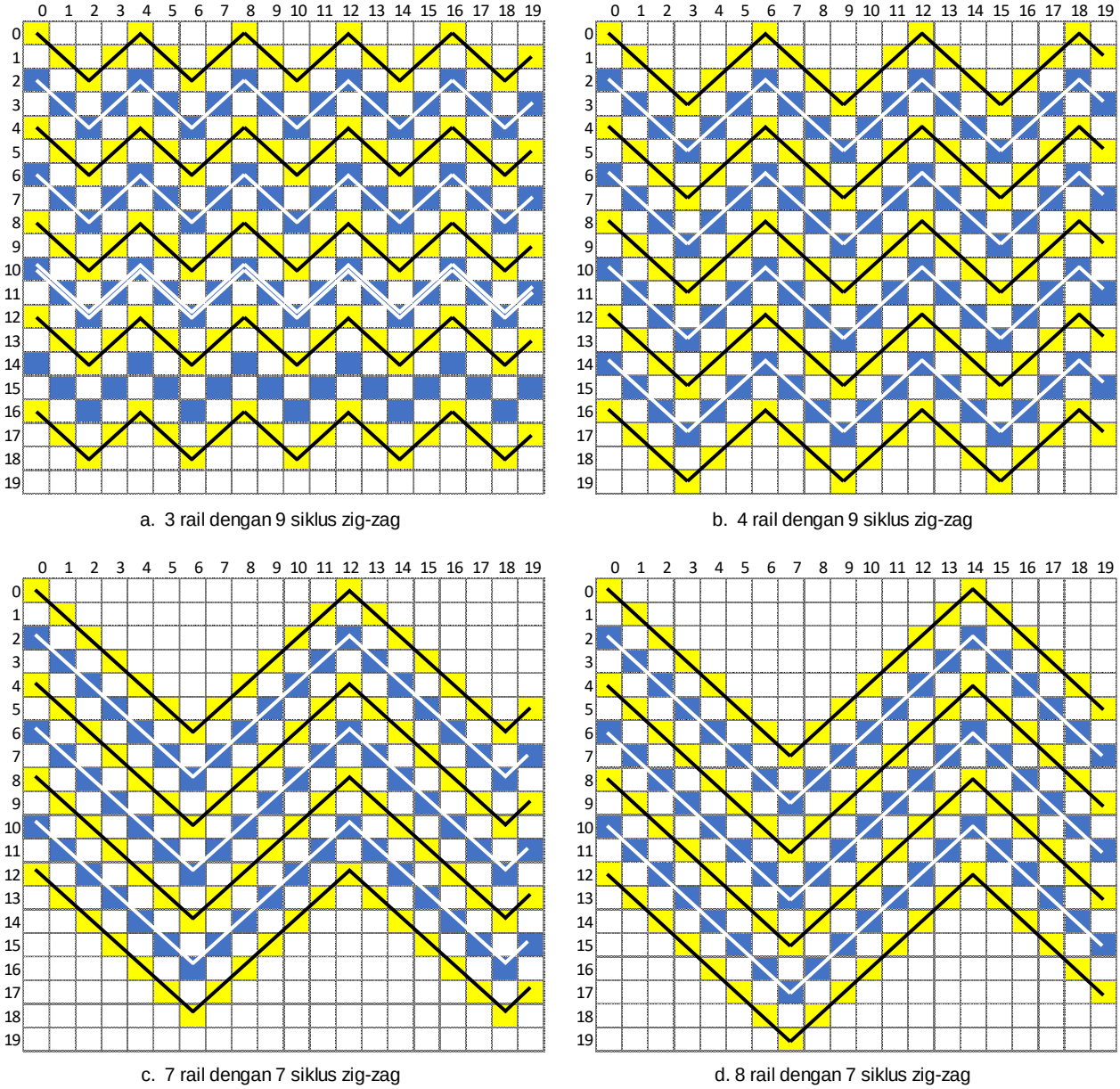
$$zigzag = int\left(\frac{sumrow - rail}{2}\right) + 1 \quad (5)$$

$$sumpixel = zigzag \times sumcol \quad (6)$$

Diasumsikan bahwa pesan hanya disembunyikan pada salah satu komponen warna saja dari citra RGB. Pada Persamaan (5) dan (6), zigzag adalah jumlah zig-zag lengkap yang dapat dibentuk, sumpixel adalah jumlah piksel yang dapat digunakan untuk penyembunyian pesan sementara sumrow dan sumcol adalah jumlah baris dan jumlah kolom pada citra. Sebagai contoh, rel adalah 3 dan masing-masing jumlah baris dan jumlah kolom pada citra adalah 20 maka jumlah zig-zag adalah 9, sehingga jumlah piksel yang dapat digunakan untuk penyembunyian pesan adalah 180.

Data yang disembunyikan adalah jumlah karakter pesan dan isi pesan. Jumlah karakter pesan disimpan sebagai data biner 16 bit dan setiap karakter pesan disimpan sebagai data biner 8 bit. Jumlah karakter pesan disembunyikan pada komponen R, sementara isi pesan disembunyikan di komponen B. Komponen R dan B dipilih karena perubahan nilai pada kedua komponen ini memberi dampak kecerahan atau intensitas cahaya yang relatif rendah secara visual dibandingkan dengan perubahan nilai yang terjadi pada komponen G. Tingkat kecerahan ini biasanya diukur dalam derajat keabu-abuan yang dihitung menggunakan Persamaan (7).

$$Y' = 0.299 \cdot R + 0.587 \cdot G + 0.114 \cdot B$$



a. 3 rail dengan 9 siklus zig-zag

b. 4 rail dengan 9 siklus zig-zag

c. 7 rail dengan 7 siklus zig-zag

d. 8 rail dengan 7 siklus zig-zag

Gambar 5. Pola posisi piksel tempat peyembunyian pesan

Citra yang digunakan sebagai cover adalah adalah lena.jpg yang berukuran 225x225 yang ditunjukkan pada Gambar 7. Diasumsikan jumlah rel yang digunakan

adalah 3, baik untuk tujuan enkripsi dan untuk melakukan penyembunyian data pesan. Dari sini dapat dihitung menggunakan Persamaan (5) dan (6) bahwa jumlah piksel yang dapat digunakan untuk penyembunyian pesan adalah 25200 piksel. Jika pada setiap piksel jumlah data yang disembunyikan sebanyak dua bit, maka ukuran pesan maksimal yang dapat disembunyikan adalah 6300 karakter pada setiap komponen warna.

penyembunyian data. Penyembunyian data hanya dapat dilakukan jika kapasitas cover lebih besar dari pesan. Setelah syarat ini terpenuhi, maka dapat dilakukan proses enkripsi dan penyembunyian pesan ke dalam cover. Jumlah rel digunakan sebagai kunci untuk melakukan enkripsi ataupun penyembunyian pesan secara zigzag. Pesan teks asli merupakan masukan bagi proses enkripsi. Pesan terenkripsi (cipher text) sebagai luaran dari proses enkripsi selanjutnya menjadi masukan bagi proses penyembunyian pesan untuk menghasilkan citra hasil steganografi (stegoimage).

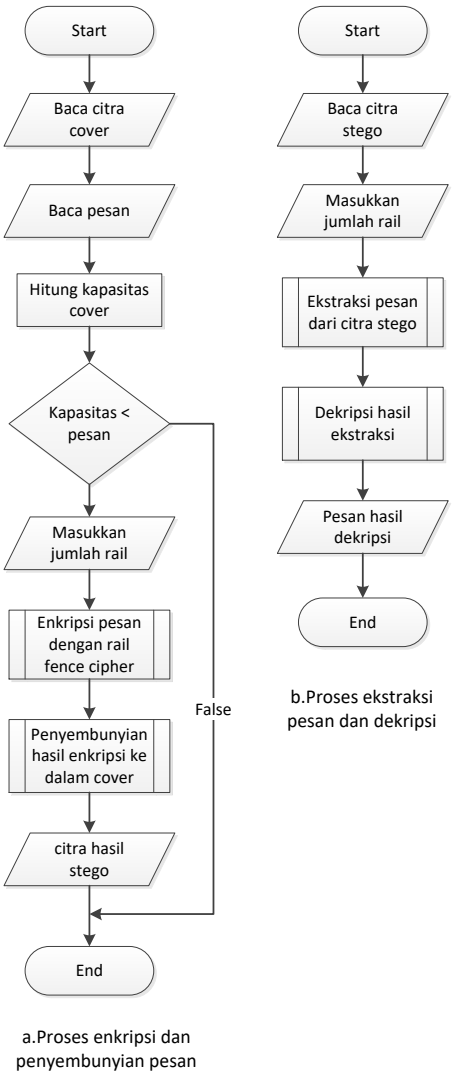
Untuk mendapatkan pesan yang disembunyikan, sebagai masukan adalah citra hasil steganografi. Jumlah rel yang dimasukkan dianggap sebagai kunci enkripsi dan digunakan untuk membentuk pola zig-zag untuk pengambilan pesan. Informasi pertama yang diambil dari *stegoimage* adalah jumlah karakter yang disembunyikan. Informasi ini disimpan dalam 16 bit pada 8 piksel pada komponen R. Setelah jumlah karakter ketahui, isi pesan diambil dari komponen B sebanyak jumlah karakter tersebut. Hasil ekstraksi adalah pesan teks terenkripsi menggunakan rail-fence cipher. Jumlah rel untuk membentuk pola zig-zag juga digunakan sebagai kunci untuk melakukan dekripsi. Hasil ekstraksi ini selanjutnya dijadikan masukan pada proses dekripsi untuk mendapatkan pesan aslinya.

Pesan yang dienkripsi untuk selanjutnya disembunyikan ke dalam *coverimage* diambil dari bagian latar belakang serta metode dan material pada artikel ini. Pesan tersebut disimpan dalam tujuh file teks yang diberi

HASIL DAN PEMBAHASAN

Proses enkripsi dan penyembunyian data dilakukan mengikuti alur yang ditunjukkan dalam Gambar 6. Pada proses penyembunyian pesan, sebagai masukkan adalah citra cover dan pesan yang akan disembunyikan. Kapasitas cover adalah jumlah piksel yang dapat digunakan untuk

nama teksuji1 sampai teksuji7. Seluruh teks uji diambil dari bagian pendahuluan dan metoda dari artikel ini, dengan memperhatikan peningkatan jumlah karakter pada setiap teksnya.



Gambar 6. Proses penyembunyian dan ekstraksi pesan

Contoh citra sebelum dan sesudah dilakukan penyembunyian pesan ditunjukkan

ditunjukkan pada Tabel 1. Setiap file pesan mewakili ukuran yang berbeda, mulai dari yang berukuran mendekati 10% sampai mendekati 100% dari kapasitas maksimal yang dapat disembunyikan, yaitu 6300 karakter.

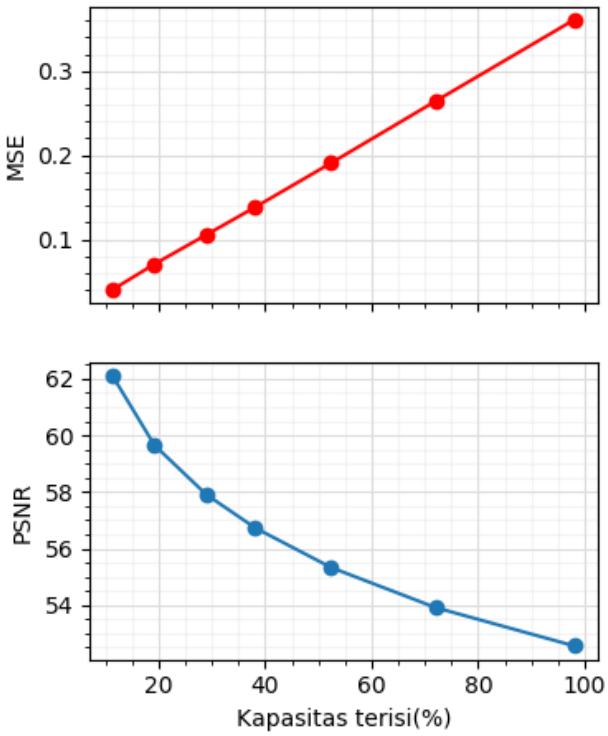
Pada Gambar 7 secara visual tidak terlihat perbedaan yang signifikan antara citra hasil steganografi dibandingkan dengan citra aslinya, meski jumlah data yang pada Gambar 7, sementara hasil pengujian menggunkaan ukuran data yang berbeda disembunyikan ke dalam citra tersebut mendekati 100% dari kapasitas yang dapat ditampung. Apalagi jika jumlah pesan yang disembunyikan lebih seditik, tentunya akan semakin sulit untuk dikenali. Artinya kriteria pertama dari steganografi yang baik yaitu *imperceptible* dimana keberadaan pesan pada cover media tidak mudah dikenali menggunakan indera visual, dapat dianggap sudah terpenuhi.

Gambar 7. Citra cover media (kiri) dan hasil steganografi dengan teksuji7 (kanan)

Tabel 1. Hasil pengujian penyembunyian pesan terenkripsi

File teks	Jumlah karakter	Jml. pola zigzag lengkap	Kapasitas (%)		MSE		PSNR (dB)	
			Terisi	Selisih	Nilai	Selisih	Nilai	Selisih
teksuji1.txt	713	12	11.32	-	0.0402	-	62.0938	-
teksuji2.txt	1209	21	19.19	7.87	0.0705	0.0304	59.6478	2.4460
teksuji3.txt	1822	32	28.92	9.73	0.1053	0.0348	57.9069	1.7409
teksuji4.txt	2402	42	38.13	9.21	0.1382	0.0329	56.7260	1.1810
teksuji5.txt	3300	58	52.38	14.25	0.1906	0.0525	55.3286	1.3974
teksuji6.txt	4537	80	72.02	19.63	0.2641	0.0735	53.9125	1.4161
teksuji7.txt	6180	109	98.10	26.08	0.3609	0.0968	52.5564	1.3561

Nilai selisih pada hasil pengujian pada Tabel 1 merupakan nilai absolut dari pengurangaan hasil pengukuran data pertama dengan kedua, data kedua dengan ketiga dan seterusnya. Selisih kapasitas menunjukkan perubahan dalam hal peningkatan jumlah karakter pada teksuji. Demikian pula dengan masih dikatakan baik jika nilainya lebih besar dari 50 dB. Terlihat pada Tabel 1 bahwa peningkatan kapasitas pesan yang disembunyikan berpengaruh secara langsung pada peningkatan nilai MSE yang pada gilirannya mempengaruhi nilai PSNR.



Gambar 8. Perubahan nilai MSE dan PSNR karena perubahan kapasitas terisi

Seperti ditunjukkan pada Gambar 8, peningkatan kapasitas pesan yang disembunyikan ke dalam *coverimage* linier dengan peningkatan nilai MSE. Peningkatan nilai MSE ini menurunkan nilai PSNR secara logaritmik. Namun, meskipun terjadi penurunan nilai PSNR yang menandakan terjadinya penurunan kualitas citra hasil steganografi, penurunan ini masih menghasilkan citra yang berkualitas baik. Karena untuk penyembunyian pesan dengan kapasitas mendekati 100% masih menghasilkan nilai PSNR yang lebih besar dari 50 dB. Dari sini dapat diartikan bahwa kriteria steganografi yang kedua yaitu *fidelity* juga terpenuhi.

Kriteria steganografi yang ketiga yaitu *recovery* juga terpenuhi. Recovery berarti pesan yang disembunyikan dapat diambil kembali atau diekstraksi dari *stegoimage*. Dalam penelitian ini, merujuk pada flowchart pada Gambar 6, hasil ekstraksi masih dalam bentuk pesan terenkripsi. Sehingga untuk mengetahui pesan aslinya, terlebih dahulu perlu dilakukan proses dekripsi menggunakan algoritma rail-fence cipher. Algoritma ini menggunakan kunci simetris berupa jumlah rel yang digunakan untuk melakukan enkripsi sama dengan jumlah rel yang digunakan untuk melakukan dekripsi.

Pola zig-zag pada penyembunyian pesan bertujuan untuk meningkatkan keacakan data, karena secara alaminya metoda LSB diterapkan dengan cara penulisan pada piksel yang berurutan. Penggunaan pola zig-zag ini dimaksudkan sebagai pengamanan tambahan pada pesan yang disembunyikan, meskipun pesan sudah dalam bentuk terenkripsi. Sehingga dapat dikatakan bahwa pesan dimaksud, mendapatkan dua tingkat pengamanan.

Dalam kondisi nyata, cara ini dapat digunakan untuk mengirimkan informasi digital dalam satu kemasan, sehingga bermanfaat juga untuk menurunkan penggunaan bandwith yang diperlukan untuk transmisi data. Misalkan pada sebuah foto yang dikirim, dapat sekaligus disematkan informasi lengkap tentang foto tersebut, dimana informasi hanya dapat diekstraksi oleh pihak-pihak yang berkepentingan saja.

Namun seperti banyak teknologi lainnya yang pada awalnya dibuat untuk tujuan positif, teknik ini juga dapat disalahgunakan untuk tujuan negatif. Tujuan negatif yang dimaksud disini adalah penggunaan untuk tujuan-tujuan yang illegal dan melanggar hukum seperti pornografi, sumber-sumber yang sejak awal memang sudah dicurigai, guna mendeteksi dan mencegah kegiatan berbahaya seperti intimidasi (*bullying*), perencanaan serangan teroris, dan penyebaran informasi yang bersifat menipu (Liu & Chawla, 2017).

PENUTUP

Simpulan

Penelitian ini menunjukkan bahwa salah satu kelemahan enkripsi yang mudah menimbulkan dugaan tentang adanya pesan rahasia berhasil ditutupi dengan steganografi. Penelitian ini juga menunjukkan bahwa tiga kriteria steganografi yang baik yakni impercetability, fidelity dan recovery dapat dipenuhi dalam penyembunyian pesan menggunakan metode LSB dengan pola zig-zag. Citra hasil steganografi masih tergolong baik yang ditunjukkan dengan nilai PNSR yang besar dari 50dB dan secara visual tidak mudah dibedakan dari citra aslinya. Peyembunyian pesan terenkripsi dilakukan menggunakan pesan pada kisaran 10% hingga mendekati 100% dari kapasitas maksimum yang dapat ditampung oleh *coverimage.* PNSR tertinggi adalah 62.0938 utk kapasitas 11.32% dan yang terendah sebesar 52.5564 dB untuk kapasitas mendekati 100%.

Penelitian selanjutnya akan mengkaji pengaruh posisi dan jumlah bit LSB yang digunakan serta penggunaan komponen warna lainnya untuk peyembunyian pesan dengan tujuan untuk peningkatan kapasitas jumlah pesan yang dapat disembunyikan.

terorisme dan kejahatan seperti penggunaan ransomware. Hal ini semestinya juga menjadi perhatian pihak yang berwenang untuk dapat meningkatkan kewaspadaan dalam hal lalu lintas komunikasi data yang terjadi. Khususnya yang berasal dari

Saran

Implementasi stenografi pada penelitian ini berhasil digunakan untuk menutupi salah satu kelemahan dari enkripsi, namun kelemahan steganografi atas operasi konversi, kompresi, *cropping*, *filtering* masih belum dikaji dan diuji. Untuk itu, selain upaya peningkatan kapasitas penyembunyian data juga perlu dilakukan kajian untuk mengurangi kelemahan dari steganografi tersebut agar pesan yang disembunyikan tidak hilang karena adanya proses pada citra hasil steganografi.

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

Annalakshmi, M., & Padmapriya, A. (2013). Zigzag Ciphers : A Novel Transposition Method. In *International Conference on Computing and information Technology (IC2IT-2013)* (pp. 8–12).

Assyahid, M. M., Rihartanto, R., & Utomo, D. S. B. (2018). Implementasi Steganografi Pesan Text ke Dalam Audio Dengan Metode Spread Spectrum. In *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi (SAKTI)* (Vol. 3, pp. 27–34).

Centina, E. A. C. (2017). Image Steganography of Multiple File Types with Encryption and Compression Algorithms. *Asia Pacific Journal of Multidisciplinary Research*, *5*(3), 57–64.

Champakamala, B. S., Padmini, K., & Radhika, D. K. (2014). Least Significant Bit algorithm for image steganography Overview of Steganography. *International Journal of Advanced Computer Technology (IJACT)*, *3*(4), 34–38.

Dar, J. A. (2014). Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques. *International Journal of Science and Research (IJSR)*, *3*(9), 1787–1791. Retrieved from https://www.ijsr.net/archive/v3i9/U0VQMTQxMTQ=.pdf

Ginting, J. A., Manongga, D., & Sembiring, I. (2018). The spread path of hoax news in social media (facebook) using social network analysis (SNA). In *2018 International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2018* (pp. 405–409). IEEE. https://doi.org/10.1109/ISRITI.2018.8864444

Li, P., & Lu, A. (2018). LSB-based Steganography Using Reflected Gray Code for Color Quantum Images. *International Journal of Theoretical Physics*, *57*(5), 1516–1548.

Liu, Y., & Chawla, S. (2017). Social Media Anomaly Detection : Challenges and Solutions. In *The 1st International Workshop on Search and Mining Terrorist Online Content & Advances in Data Science for Cyber Security and Risk on the Web* (pp. 817–818).

Pandian, N. (2014). An Image Steganography Algorithm Using Huffman and Interpixel Difference Encoding. *International Journal of Computer Science & Security*, *8*(6), 202–215.

Patil, S. A., & Adhiya, K. P. (2012). Hiding Text in Audio Using LSB Based Steganography. *Information and Knowledge Management*, *2*(3), 8–15. Retrieved from www.iiste.org

Siahaan, A. P. U. (2016). Rail Fence Cryptography in Securing Information. *International Journal of Scientific & Engineering Research*, *7*(7), 535–538.

Wakiyama, M., Hidaka, Y., & Nozaki, K. (2010). An audio steganography by a low-bit coding method with wave files. *Proceedings - 2010 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2010*, 530–533. https://doi.org/10.1109/IIHMSP.2010.135