Penyisipan Pesan Teks pada Citra Menggunakan Metode LSB dan 2-Wrap Length

Mulyanto*[1], Royke Vincentius Febriyana[2], Arief Bramanto Wicaksono Putra[3]
[1,3]Jurusan Teknologi Informasi, Politeknik Negeri Samarinda
[2]Jurusan Desain, Politeknik Negeri Samarinda;
Jl. Dr. Cipto Mangunkusumo, Samarinda, Indonesia
e-mail: *[1]yanto1294@gmail.com, [2]rvincentius@gmail.com, [3]ariefbram@gmail.com

Abstrak

Steganografi merupakan teknik penyembunyian pesan yang dianggap penting ke dalam file lain dengan cara menyamarkan isi pesan. Proses steganografi membutuhkan pesan dan cover. Cover adalah media yang digunakan untuk penyisipan atau penyembunyian pesan. Penelitian ini bertujuan untuk menyisipkan pesan teks ke dalam citra cover bertipe PNG. Pada penelitian ini menggunakan metode least significant bit sebagai metode penyisipan dan metode 2-wrap length dalam menentukan posisi pesan yang akan disisipkan. Hasil penelitian menunjukkan bahwa penggabungan kedua metode ini membuat posisi pesan yang disisipkan lebih acak pada media cover. Banyaknya pesan yang dapat disisipkan tergantung pada ukuran media cover.

Kata kunci—steganografi, LSB, reshape, 2-wrap length, re-wraping

Abstract

Steganography is a technique to hide messages that are considered necessary in other files by disguising the contents of the message. The steganography process requires a message and cover. The cover is a medium used for message insertion or message hiding. This study aims to insert text messages into PNG images cover. This research uses the least significant bit method as the insertion method and the 2-wrap length method to determining the position of the message to be inserted. The results showed that the combination of these two methods made the position of the message inserted more randomly on the media cover. The number of messages that can be inserted depends on the size of the media cover.

Keywords— steganography, LSB, reshape, 2-wrap length, re-wraping

1. PENDAHULUAN

Komunikasi merupakan aktivitas yang sangat mendasar dan menjadi bagian penting bagi kehidupan manusia. Seiring perkembangan teknologi informasi, komunikasi tidak hanya dilakukan secara verbal, tetapi menggunakan teknologi seperti: *email*, sosial media, *instant messaging*, dan lain-lain. Kadang informasi yang ingin dikirimkan bersifat rahasia dan tidak ingin diketahui pihak lain. Beberapa contoh informasi yang bersifat rahasia, antara lain: *password*, rencana bisnis, informasi kartu kredit, strategi militer, data pasien, dan lain-lain. Beberapa usaha yang umum digunakan untuk menjaga kerahasiaan informasi, antara lain: kriptografi (penyandian pesan), steganografi, dan peningkatan kepedulian pengguna terhadap keamanan informasi. Pada teknik steganografi, pesan yang dirahasiakan dikirimkan dengan cara menyisipkan pesan tersebut melalui sebuah media, bisa berupa citra, audio, maupun video [1].

Salah satu cara menyembunyikan pesan yang dikirimkan menggunakan steganografi. Teknik ini telah digunakan sejak berabad-abad silam untuk menyembunyikan pesan. Orang Mesir kuno menggunakan karakter dalam bentuk gambar untuk menyampaikan pesan (*hieroglyph*). Pada bangsa Yunani, pesan rahasia dikirimkan dengan cara menuliskan pesan tersebut pada kulit kepala budak. Ketika rambut budak tersebut telah tumbuh dan menutup pesan yang dituliskan, kemudian budak tersebut dikirimkan untuk menyampaikan pesan yang ada di kulit kepalanya [2][3].

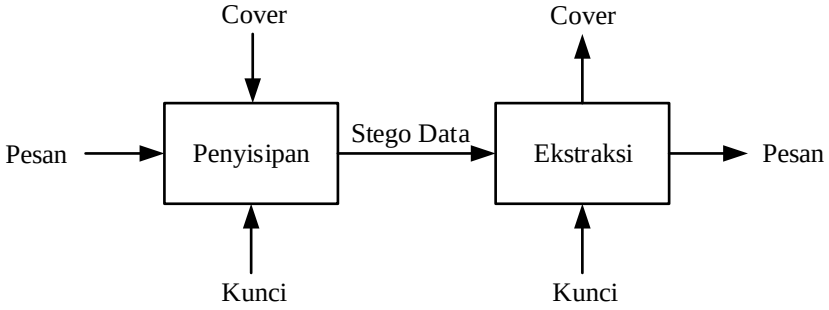
Melalui media internet, data yang dipertukarkan dalam komunikasi, bisa berbentuk teks, *image*, audio dan video. Berbagai teknik steganografi dikembangkan untuk menjaga keberadaan pesan rahasia [4]. Untuk mengamankan pengiriman pesan rahasia, obyek multimedia seperti citra, audio dan video digunakan sebagai *cover* untuk menyembunyikan data. Beberapa teknik steganografi yang umum digunakan untuk menyembunyikan pesan pada media digital, diantaranya menyisipkan pesan pada bit yang paling tidak signifikan (*least significance bit*, LSB) yang menyusun media cover [5]. Cara lain penyisipan pesan dapat menggunakan teknik *mask and filtering*, teknik distorsi, algoritma dan transformasi (fourier, DCT, wavelet), dan ada juga yang menggunakan gabungan teknik steganogafi dan kriptografi [1][2][4][6].

Penelitian-penelitian sebelumnya terkait pengamanan informasi sudah banyak dilakukan. Indriyono menggabungkan teknik kriptografi Rijndael untuk mengacak pesan dengan metode LSB untuk menyisipkan pesan [1]. Pandikumar dan Gebreslassie menggunakan metode LSB dengan teknik peletakan acak pada tepi citra. Pesan yang akan disisipkan diacak terlebih dahulu dengan menggunakan teknik kriptografi *Advanced Encryption Standard* (AES) untuk memberikan keamanan yang lebih [3].

Pada penelitian ini, sama seperti penelitian sebelumnya, menggunakan teknik LSB untuk menyisipkan pesan teks ke citra. Untuk meningkatkan kemampuan LSB dalam menyisipkan pesan, ditambahkan algoritma peletakan pada bagian mana dari citra pesan akan disisipkan. Semakin acak posisi pesan maka semakin tidak mudah terbaca informasi yang dirahasiakan pada pesan teserbut. Untuk menentukan posisi piksel yang akan disisipkan pesan, peneliti mengusulkan penggunaan metode *2-wrap length*. Metode ini didasari oleh konsep seperti melipat pita menjadi dua bagian yang sama panjang, kemudian setelah pita dibuka maka posisi piksel tersebar.

2. METODE PENELITIAN

Penelitian yang dilakukan menggunakan citra sebagai media pesan yang terdapat 3 komponen di dalamnya yaitu R, G, B.penelitian ini hanya menggunakan komponen R sebagai bahan penelitian yang akan disisipi pesan berupa data teks. Pada penelitian ini terdiri dari 2 tahapan utama, yaitu penyisipan (*embed*) dan ekstraksi. Tahapan penyisipan adalah proses penyisipan pesan ke dalam media cover, sedangkan tahapan ekstraksi adalah proses pengambilan kembali pesan teks dari media cover [7][8]. Gambar 2 menunjukkan proses penyisipan dan ekstraksi pesan dari cover.

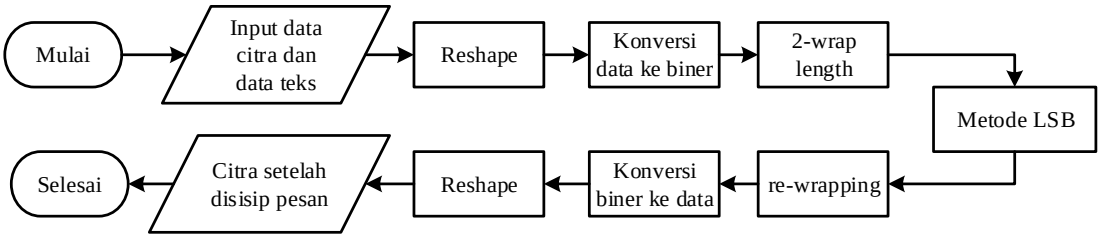


Gambar 1 Proses penyisipan dan ekstraksi pesan

2.1 Proses Penyisipan

Proses penyisipan dilakukan melalui beberapa tahap. Pertama citra dua dimensi diubah menjadi 1 dimensi yang disusun memanjang melalui proses yang disebut *reshape*. Selanjutnya pesan yang akan disisipkan dikonversi dan ditampilkan ke dalam bentuk biner. Citra hasil *reshape* kemudian dilipat menjadi 2 bagian melalui teknik yang disebut *2-wrap length*. Pesan disisipkan pada citra yang sudah dilipat menggunakan teknik LSB. Untuk mengembalikan pesan

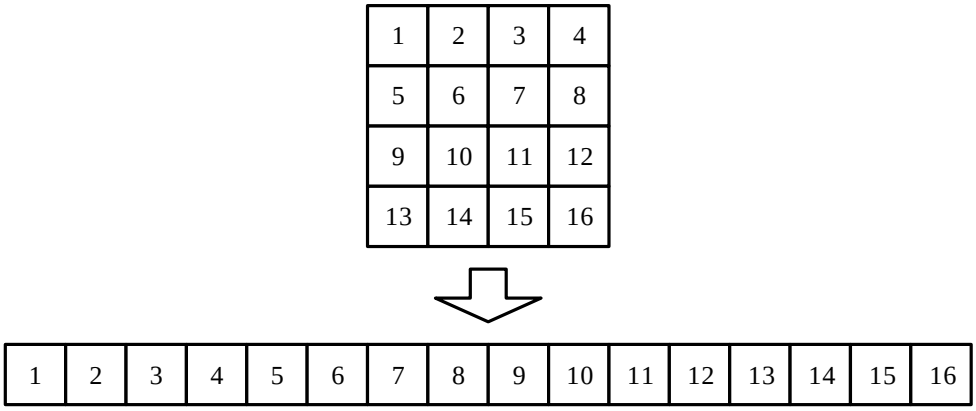
Teknik *2-wrap length* untuk menentukan posisi pesan yang akan disisipkan dan menggunakan metode *least significant bit (LSB)* untuk proses penyisipannya, agar pesan menjadi lebih acak maka akan digunakan teknik *reshape* dan *re-wrapping* pesan untuk mengembalikan dimensi citra menjadi seperti semula.



Gambar 2 Diagram alir proses penyisipan pesan

2.1.1 Reshape

Proses *reshape* bertujuan mengubah citra 2 dimensi menjadi vektor 1 dimensi. Gambar 3 menunjukkan proses *reshape* pada citra ukuran 4×4 menjadi vektor berukuran 1×16.



Gambar 3 Dimensi citra sebelum dan setelah *reshaping*

2.1.2 Teknik 2-wrap length

Teknik *2-wrap length* digunakan untuk menentukan di bagian mana dari citra pesan teks akan disisipkan. Pertama, menentukan panjang piksel citra hasil *reshape*. Selanjutnya citra vektor akan dilipat menjadi 2 bagian yang sama besar dari arah kiri ke kanan, sebagaimana ditunjukkan pada Gambar 4. Untuk teks pada posisi ganjil akan diletakkan pada Lipatan ke-1 sedangkan teks pada posisi genap akan diletakkan pada Lipatan ke-2.

Lipatan 1	9	10	11	12	13	14	15	16
Lipatan 2	8	7	6	5	4	3	2	1

Gambar 3 Data setelah proses *2-wrap length*

2.1.3 Konversi tipe data teks ke biner

Pesan teks yang akan disisipkan dan data citra dikonversi menjadi bilangan biner dengan pengkodean ASCII. Sebagai contoh, karakter teks "BISA" dikonversikan menjadi bilangan biner, sehingga diperoleh hasil seperti di bawah ini.

Karakter	Kode ASCII	Biner
B	66	01000010
I	73	01001001

Karakter	Kode ASCII	Biner
S	83	01010011
A	65	01000001

2.1.4 Proses LSB

Pesan disisipkan ke dalam citra cover menggunakan metode LSB [7, 8]. LSB adalah bit yang nilainya paling kecil pada data bilangan biner, umumnya terletak pada bit paling kanan. Proses penyisipan dilakukan dengan mengganti bit paling kanan dengan bit pesan. Berikut adalah contoh proses penyisipan hurus "S" pada citra menggunakan metode LSB.

Citra : (10100011 11101001 10101000)
(00100111 01001000 10101001)
(01010000 10110111 01001011)

Pesan : S = 83 = **01010011**

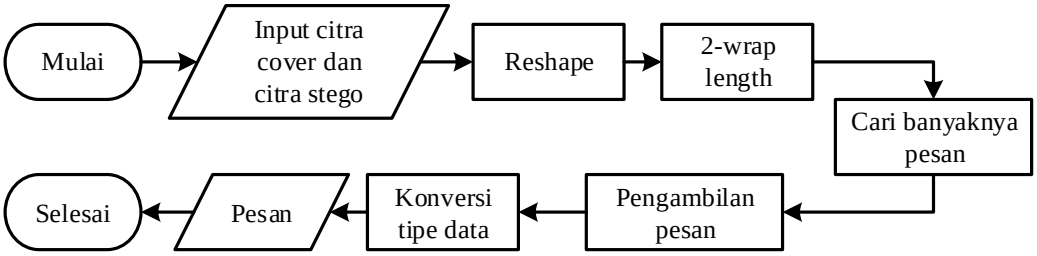
Hasil dari penyisipan pesan :
(1010001**0** 1110100**1** 1010100**0**)
(0010011**1** 0100100**0** 1010100**0**)
(0101000**1** 1011011**1** 01001011)

2.1.5 Re-wrapping

Setelah pesan disisipkan, selanjutnya vektor citra yang dilipat dikembalikan seperti semula, tanpa lipatan. Proses ini disebut dengan *re-wrapping*.

2.2 Proses Ekstraksi

Untuk melakukan pengambilan kembali pesan yang telah disisipkan ke dalam citra dilakukan proses ekstraksi. Proses ekstraksi merupakan kebalikan dari proses penyisipan, sebagaimana ditunjukkan pada Gambar 4. Proses *reshape* mengubah dimensi citra 2 dimensi menjadi vektor. Proses 2-*wrap length* data citra untuk mengetahui posisi pesan yang disisipkan. Selanjutnya mencari banyaknya pesan dengan membandingkan data L1 dan L2 pada citra cover dan citra stego. Jika nilai citra cover tidak sama dengan citra stego, maka data pada citra stego akan diambil.



Gambar 4 Diagram alir proses ekstraksi

2.3 Pengujian performansi

Pengujian kualitas citra setelah dimanipulasi dengan menyisipkan pesan diukur menggunakan *means square error* (MSE) dan *peak signal to noise ratio* (PSNR). MSE merupakan rata-rata dari selisih kuadrat citra asli dengan citra yang telah disisipkan pesan (citra hasil manipulasi) [8].

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left[S(i,j) - C(i,j) \right]^2 \quad (1)$$

Dimana *i* dan *j* adalah koordinat dari citra, *m* dan *n* ukuran citra, *S(i, j)* menyatakan citra stego dan *C(i, j)* menyatakan citra cover. Nilai MSE semakin rendah semakin baik. Rasio kualitas citra sebelum dan setelah penyisipan pesan menggunakan PSNR. Semakin tinggi nilai PSNR, semakin mirip citra manipulasi dengan citra asalnya [8].

$$PSNR = 10 \log_{10} \left(\frac{C_{\max}^2}{MSE} \right) \quad (2)$$

3. HASIL DAN PEMBAHASAN

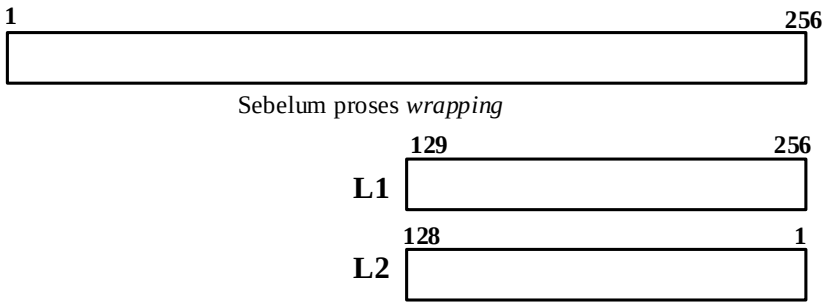
3.1 Data Penelitian

Pada penelitian ini, pesan yang disisipkan berupa data teks, dan cover menggunakan citra. Citra yang digunakan bertipe PNG, ditunjukkan pada Gambar 5. Pada penelitian ini, penyisipan pesan hanya dilakukan pada komponen R (*red*) citra.

Gambar 5 Citra cover

3.2 Proses Penyisipan

Proses penyisipan diawali dengan melakukan perubahan dimensi citra media cover yang berukuran 16 x 16 menjadi vektor berukuran 1 x 256 melalui proses *reshape*. Selanjutnya pesan teks disajikan dalam bentuk bilangan biner, karena proses penyisipan dilakukan pada data biner. Tahapan berikutnya dilakukan proses *2-wrap length* pada vektor berukuran 1 x 256 menjadi 2 bagian dengan cara melakukan pelipatan ke kanan, ditunjukkan pada Gambar 5.



Gambar 5 Bentuk vektor sebelum dan setelah proses *wrapping*

Tahap selanjutnya adalah melakukan proses penyisipan pesan teks ke dalam citra cover menggunakan metode LSB, dengan mengganti bit yang paling kanan pada citra. Huruf pertama pada pesan diletakkan pada L1, huruf kedua diletakkan pada L2. Demikian seterusnya, peletakkan huruf pesan diletakkan bergantian antara L1 dengan L2. Contoh penyisipan pesan pada citra menggunakan metode LSB ditunjukkan pada Gambar 6.

Sebelum penyisipan		Setelah penyisipan
01100100		0110010**0**
01010001		0101000**1**
00011011		0001101**0**
00011011	Disisipkan **ASCII "P" = 80 = 01010000**	0001101**1**
11001000		1100100**0**
01100010		0110001**0**
00110111		0011011**0**
00100010		0010001**0**

Gambar 6 Data citra sebelum dan setelah penyisipan pesan teks

3.3 Pengukuran Performansi

Pengukuran performansi untuk mengetahui perubahan yang terjadi pada citra sebelum dan sesudah proses penyisipan pesan, menggunakan nilai MSE dan PSNR, sebagaimana terlihat pada Tabel 1.

Tabel 1 Pengujian Performansi Image Stego

Dimensi Citra R	**Pengujian Performansi**		
	Panjang Pesan	***Nilai MSE***	***Nilai PSNR***
16x16	10 Karakter	6,78E-06	229,8381
	20 Karakter	2,86E-04	192,4021
	34 Karakter	8,96E-04	180,9912
32x32	10 Karakter	1,06E-07	271,427
	20 Karakter	2,64E-06	239,2382
	34 Karakter	1,05E-07	271,4270
64x64	10 Karakter	1,66E-07	266,9641
	20 Karakter	5,96E-08	277,1806
	34 Karakter	3,24E-07	260,2346

Berdasarkan hasil pengujian pada Tabel 1, semakin pendek pesan disisipkan, nilai MSE cenderung lebih kecil. Semakin besar dimensi citra yang akan disisip pesan, nilai MSE cenderung semakin kecil dan nilai PSNR cenderung lebih besar dibandingkan pada citra yang berukuran lebih kecil.

4. KESIMPULAN

Penelitian ini menerapkan konsep steganografi untuk menyembunyikan pesan teks pada data citra. Metode LSB digunakan untuk menyisipkan pesan, sedangkan teknik *2-wrap length* digunakan untuk menentukan posisi penyisipan pesan teks ke dalam citra untuk menghasilkan penyisipan yang lebih acak sehingga isi pesan tidak mudah diketahui. Penelitian ini menggunakan sampel data citra sebanyak 3 buah dengan ukuran yang berbeda. Hasil penelitian menunjukkan semakin besar citra cover, nilai MSE yang dihasilkan cenderung lebih kecil, dan nilai PSNR cenderung lebih besar. Kualitas citra hasil penyisipan lebih bagus pada citra yang berukuran lebih besar dibandingkan pada citra yang berukuran lebih kecil. Semakin besar dimensi citra yang digunakan sebagai media cover akan dapat menampung banyak pesan yang dapat disisipkan. Semakin sedikit karakter yang disisipkan maka semakin tinggi tingkat keberhasilan kembalinya pesan.

5. SARAN

Studi lebih lanjut adalah bagaimana bisa meningkatkan kinerja citra stego dengan bisa dikembangkan menjadi *4-wrap length,* atau bahkan menjadi *n-wrap length* sehingga tingkat keacakan posisi penyisipannya lebih tinggi. Pesan yang disisipkan juga bisa dilakukan pengacakan terlebih dahulu dengan menggunakan metode kriptografi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih atas dukungan finansial dari Direktorat Riset dan Pengabdian Masyarakat Kemenristekdikti, dan terima kasih kepada Jurusan Teknologi Informasi Politeknik Negeri Samarinda yang telah menyediakan dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] B. V. Indriyono, "Penerapan Keamanan Penyampaian Informasi Melalui Citra dengan Kriptografi Rijndael dan Steganografi LSB," *Creative Information Technology Journal (CITEC),* vol. 3, no. 3, pp. 228–241, 2016.

[2] I. Maurya dan S. K. Gupta, "Understandable Steganography," *International Journal of Engineering & Technology.*, vol. 7, no. 3, pp. 1024–1033, 2018.

[3] P. Thangasamy dan T. Gebreslassie, "Information Security Using Image Based Steganography," *International Research Journal of Engineering and Technology*, vol. 3, no. 6, pp. 2839–2844, 2016.

[4] A. Singh dan S. J. Singh, "An Overview of Image Steganography Techniques," *International Journal of Engineering and Computer Science*, vol. 3, no. 7, pp. 7341–7345, 2014.

[5] Kavita, K. Kadam, A. Koshti, dan P. Dunghav, "Steganography Using Least Significant Bit Algorithm," *International Journal Engineering Research and Applications*, vol. 2, no. 3, pp. 338–341, 2012.

[6] C. P. Sumathi, T. Santanam, dan G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *International Journal of Computer Science & Engineering Survey*, vol. 4, no. 6, pp. 9–25, 2013.

[7] S. Rohayah, G. W. Sasmito, dan O. Somantri, "Aplikasi Steganografi untuk Penyisipan Pesan," *Jurnal Informatika*, vol. 9, no. 1, pp. 975–981, 2015.

[8] E. R. Djuwitaningrum dan M. Apriyani, "Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator," *JUITA*, vol. 4, no. 2, pp. 79–85, 2016.