

Implementasi Steganografi Menggunakan Metode Spread Spectrum Dalam Pengamanan Data Teks Pada Citra Digital

Yusuf Ramadhan Nasution¹, Mhd. Furqan², Meri Sinaga³

^{1,2,3}Prodi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara

Jalan IAIN No. 1 Medan, Sumatera Utara

¹ramadhannst@uinsu.ac.id, ²mfurqan@uinsu.ac.id, ³merisinaga41@gmail.com

Abstract

Various techniques are used to protect digital information, especially information that is kept secret from people who are not entitled to the right of access to information, one of which is the technique of steganography. Steganography technique is a technique used to secure data by inserting or hiding data into an object without changing the shape of the object, one of the objects is a digital image. Steganography technique also has several methods, namely the Spread Spectrum method. Spread Spectrum is a method of communication where information signals are spread across all available frequencies by selecting where to insert data at low frequencies and adding pseudo-noise (PN). This study secures text data with the Spread Spectrum steganography technique on digital image objects by the steps of changing the value of the RGB pixel image and text data into binary, spreading the text data, followed by key generation and the modulation process of spreading text data with the generated key results. So as to produce a stegano image with an RGB pixel value that changes the value of 0 to 1 value that does not affect the color reproduction of the RGB pixel image.

Keywords: Image, Text, Steganography, Spread Spectrum

Abstrak

Berbagai macam teknik digunakan untuk melindungi informasi digital terutama informasi yang dirahasiakan dari orang yang tidak berhak terhadap hak akses informasi tersebut, salah satunya adalah dengan teknik steganografi. Teknik steganografi adalah sebuah teknik yang digunakan untuk mengamankan data dengan cara menyisipkan atau menyembunyikan data kedalam sebuah objek tanpa mengubah bentuk objek tersebut, salah satu objeknya adalah citra digital. Teknik steganografi juga memiliki beberapa metode yaitu metode Spread Spectrum. Spread Spectrum adalah metode komunikasi dimana sinyal informasi disebar diseluruh frekuensi yang tersedia dengan memilih tempat penyisipan data pada frekuensi yang rendah serta menambahkan pseudo-noise (PN). Penelitian ini mengamankan data teks dengan teknik steganografi Spread Spectrum pada objek citra digital dengan tahapan mengubah nilai RGB pixel citra dan data teks kedalam biner, melakukan spreading pada data teks, dilanjutkan dengan pembangkitan kunci serta proses modulasi hasil spreading data teks dengan kunci hasil pembangkitan. Sehingga menghasilkan citra stegano dengan nilai RGB pixel yang mengalami perubahan nilai 0 hingga 1 nilai yang tidak mempengaruhi reproduksi warna RGB pixel citra.

Kata Kunci: Citra, Teks, Steganografi, Spread Spectrum

1. PENDAHULUAN

Saat ini perkembangan teknologi informasi telah memberikan kemudahan dalam menyelesaikan pekerjaan manusia. Pertukaran data dan informasi menjadi lebih mudah dan cepat. Namun disisi lain juga memiliki kekurangan, yaitu informasi yang dikirim dapat dengan mudah dicuri oleh oknum yang tidak bertanggung jawab. Berbagai macam teknik digunakan



untuk melindungi informasi digital terutama informasi yang dirahasiakan dari orang yang tidak berhak terhadap hak akses informasi tersebut, maka diperlukan suatu cara untuk mengamankan data dan informasi. Diantaranya adalah dengan cara menyembunyikan data tersebut kedalam sebuah objek yang tidak dapat dicurigai dengan teknik steganografi.

Berdasarkan pada masalah keamanan data yang dapat merugikan pihak yang memiliki otoritas, solusi yang diberikan adalah dengan memanfaatkan sebuah teknik steganografi. Teknik steganografi adalah sebuah teknik yang digunakan untuk mengamankan data dengan cara menyisipkan atau menyembunyikan data kedalam sebuah objek tanpa mengubah bentuk objek tersebut [1] Sehingga data yang disisipkan kedalam objek tidak dapat dicurigai oleh pihak yang tidak bertanggung jawab.

Proses penyisipan teknik steganografi juga membutuhkan sebuah perhitungan menggunakan metode dan harus memiliki jenis objek yang akan dijadikan wadah penyisipan data teks. Salah satunya adalah teknik steganografi dengan metode *Spread Spectrum*. *Spread Spectrum* adalah metode komunikasi dimana sinyal informasi disebar diseluruh frekuensi yang tersedia dengan memilih tempat penyisipan data pada frekuensi yang rendah serta menambahkan *pseudo-noise* (PN), sehingga algoritma *Spread Spectrum* memiliki kelebihan terhadap serangan *jamming* dan *interferensi* yang akan membuat data penyisipan tetap dapat dipresepsi apabila terjadi kerusakan sinyal[2]. Secara ringkas metode *Spread Spectrum* bekerja dengan menyisipkan dan menyebarkan data kedalam objek dengan melakukan perhitungan modulasi terlebih dahulu.

Jenis objek yang diterapkan pada penelitian adalah objek citra digital. Pemilihan objek citra digital bertujuan untuk mengurangi rasa curiga pihak yang tidak memiliki otoritas dalam mengambil informasi data teks. Hal ini dilandasi berdasarkan komunikasi modern saat ini yang salah satunya adalah komunikasi visual menggunakan citra digital. Sehingga penelitian ini akan menyisipkan pesan data teks kedalam sebuah citra digital menggunakan metode *Spread Spectrum*.

2. METODOLOGI PENELITIAN

Penelitian ini mencoba melakukan pengamanan pesan dengan cara menyisipkan pesan kedalam image yang berbasis JPG, dalam teknik steganografi terdapat sebuah metode yang menyembunyikan pesan tanpa adanya kecurigaan, yaitu metode *spread spectrum*.

a) Observasi

Pada penelitian ini bahan yang digunakan adalah sebuah objek citra digital yang berformat .jpg. Sedangkan alat penelitian meliputi perangkat keras (*hardware*) dan perangkat lunak (*software*).

b) Perancangan

Perencanaan penelitian menggunakan program aplikasi Microsoft Visual Studi Express 2012. Pada pengerjaanya, metode penelitian yang digunakan.

Perancangan sistem dalam suatu penelitian adalah tahap yang dilakukan peneliti setelah mengumpulkan semua kebutuhan sistem yang akan dirancang. Adapun tahap-tahap yang akan dilakukan meliputi dari perancangan desain penelitian, perancangan *flowchart* metode penelitian dan perancangan *interface* aplikasi.

3. HASIL DAN PEMBAHASAN

Berdasarkan dari pengujian steganografi pada aplikasi didapatkan hasil bahwa citra digital yang menjadi objek penyisipan file data teks tidak mengalami perubahan bentuk dan warna. Hal ini tentu membuat data file teks aman didalam citra digital dikarenakan secara visual tidak ada bentuk yang mencurigakan dari gambar hasil setganografi. Sehingga kecil kemungkinan terjadi kebocoran akan kerahasiaan dari file teks yang akan dikirimkan kepada pihak penerima dengan objek citra digital. Berikut nilai RGB dari keseluruhan resolusi citra sampel untuk keperluan hitungan manual:

Tabel 1. Nilai Biner Citra Sampel 8 x 6 *Pixel*

Pixel	Warna	Desimal	Biner
1	R	73	01001001
	G	108	01101100
	B	109	01101101
2	R	117	01110101
	G	109	01101101
	B	112	01110000
3	R	117	01110101
	G	116	01110100
	B	101	01100101
4	R	114	01110010
	G	80	01010000
	B	177	10110001
5	R	169	10101001
	G	180	10110100
	B	133	10000101
6	R	178	10110010
	G	109	01101101
	B	169	10101001
7	R	108	01101100
	G	120	01111000
	B	153	10011001
8	R	161	10100001
	G	123	01111011
	B	167	10100111
9	R	152	10011000
	G	177	10110001
	B	157	10011101
10	R	149	10010101
	G	137	10001001
	B	190	10111110



Berdasarkan pada tabel 1, telah diketahui nilai RGB dari setiap sampel citra resolusi 8 x 6 *pixel* atau 46 *pixel*. Selanjutnya adalah menentukan karakter data teks yang akan disisipkan kedalam objek sampel citra digital. Berikut adalah karakter data teks yang akan disisipkan kedalam citra sampel: Karakter : MERI
Karakter di atas, dikonversikan kedalam bentuk biner seperti pada tabel berikut:

Tabel 2. Nilai Desimal dan Biner Sampel Data Teks

No	Karakter	Nilai Desimal	Biner
1	M	77	01001101
2	E	69	01000101
3	R	82	01010010
4	I	73	01001001

Proses modulasi dapat dilihat di bawah ini :

Segmen data teks 1 = 00100100010000111100100000011100

Segmen *pseudonoise* 1 = 00101011010000110011011100010011
XOR

00001111000000001111111100001111

Segmen data teks 2 = 01000000000001110010010001001100

Segmen *pseudonoise* 2 = 01001111000001110010101101000011
XOR

00001111000000000000111100001111

Segmen data teks 3 = 00111000000111000100111111110111

Segmen *pseudonoise* 3 = 00110111000100110100111100000111
XOR

00001111000011110000000011110000

Segmen data teks 4 = 00100100010000111100011100011100

Segmen *pseudonoise* 4 = 00101011010000110011011100010011
XOR

00001111000000001111000000001111

Hasil dari demodulasi antara biner karakter data teks *spread spectrum* dengan biner *pseudonoise* akan disisipkan ke dalam objek sampel citra digital dengan resolusi 8 x 6 *pixel*. Adapun hasil demodulasi adalah sebagai berikut :

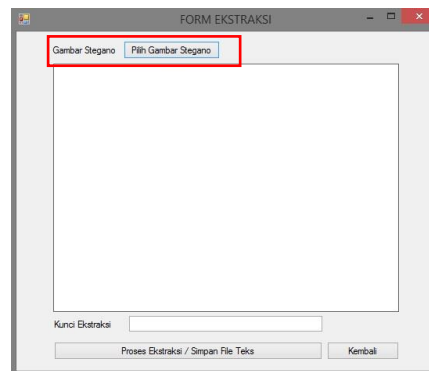
00001111 00000000 11111111 00001111
00001111 00000000 00001111 00001111
00001111 00001111 00000000 11110000
00001111 00000000 11110000 00001111

Adapun hasilnya dapat dilihat pada tabel dibawah ini:

Tabel 3. Nilai Desimal dan Biner Sampel Data Teks Kembali

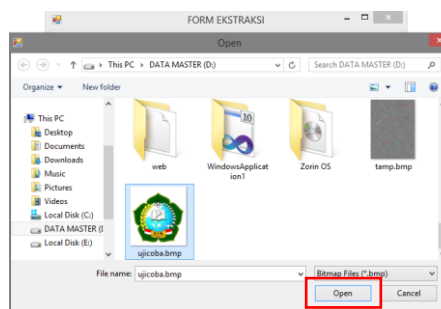
No	Karakter	Nilai Desimal	Biner
1	M	77	01001101
2	E	69	01000101
3	R	82	01010010
4	I	73	01001001

Berdasarkan pada tabel 3.3 karakter awal sebelum disisipkan kembali yaitu karakter “MERI”. Setelah dilakukan proses *embedding* data teks kedalam citra digital, kemudian untuk mengembalikannya file teks dari dalam citra digital maka dilakukan proses ekstraksi dengan menekan menu “Ekstraksi” pada menu utama sehingga muncul menu ekstraksi seperti gambar di bawah ini:



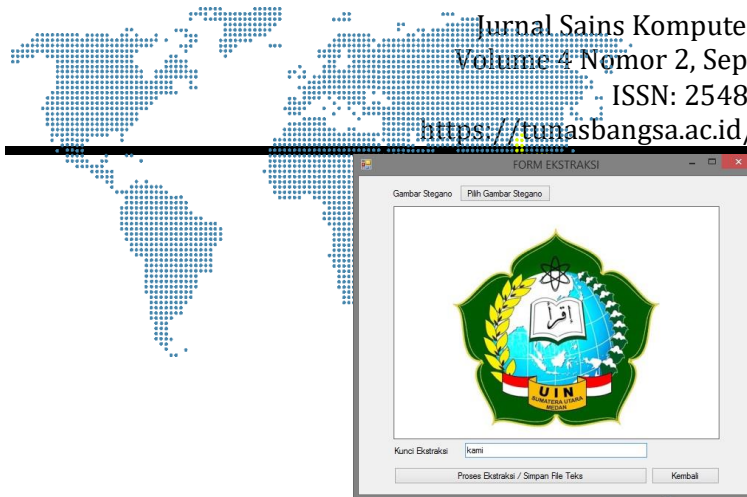
Gambar 1. Tampilan Menu Ekstraksi

Berdasarkan menu ekstraksi data teks didalam citra digital, untuk memulai terlebih dahulu memilih file citra / gambar stegano hasil *embedding* dengan format .bmp dengan cara menekan *button* “Pilih Gambar Stegano” dan menampilkan *pop up* menu pilih citra stegano seperti gambar di bawah ini:



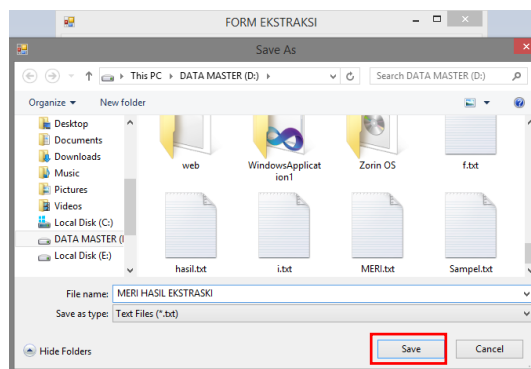
Gambar 2. Pop Up Citra Stegano Pada Menu Ekstraksi

Berdasarkan pada gambar di atas, dipilih gambar stegano hasil proses *embedding* sebelumnya dengan nama file “ujicoba.bmp” kemudian menekan *button* “open” dan menampilkan hasil seperti gambar di bawah ini:



Gambar 3. Citra Stegano Pada Menu Ekstraksi

Berdasarkan pada gambar 3, kemudian memasukan kunci yang sama saat proses *embedding*, sehingga kunci saat ekstraksi adalah karakter “kami”. Proses selanjutnya adalah melakukan ekstraksi dan menyimpan file data teks kedalam direktori penyimpanan dengan cara menekan *button* “Proses Ekstraksi / Simpan File Teks” seperti gambar di bawah ini:



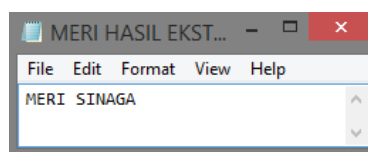
Gambar 4. Pop Up Simpan File Data Teks Pada Menu Ekstraksi

Berdasarkan pada gambar di atas, user menyimpan file teks hasil ekstraksi dengan nama file “MERI HASIL EKSTRAKSI” kemudian untuk memproses ekstraksi dan penyimpanan secara langsung dengan menekan *button* “Save”. Adapun file teks yang disimpan seperti gambar di bawah ini:



Gambar 5. File Data Teks Ekstraksi Pada Menu Ekstraksi

Adapun isi karakter dari file hasil ekstraksi akan kembali seperti semula yang dapat dilihat pada gambar di bawah ini:



Gambar 6. Isi File Data Teks Hasil Ekstraksi Pada Menu Ekstraksi

Berdasarkan dari pengujian steganografi pada aplikasi didapatkan hasil bahwa citra digital yang menjadi objek penyisipan file data teks tidak mengalami perubahan bentuk dan warna. Hal ini tentu membuat data file teks aman didalam citra digital dikarenakan secara visual tidak ada bentuk yang mencurigakan dari gambar hasil setganografi. Sehingga kecil kemungkinan terjadi kebocoran akan kerahasiaan dari file teks yang akan dikirimkan kepada pihak penerima dengan objek citra digital.

4. SIMPULAN

Dari hasil penelitian yang dilakukan terhadap pengamanan pesan teks yang disembunyikan ke dalam file citra digital menggunakan algoritma *spread sprectum*, maka terdapatbeberapa kesimpulan berdasarkan uraian yang telah tercantum pada bab-bab sebelumnya. Adapun kesimpulan dari hasil penelitian ini adalah pesan teks dengan format txt dapat diamankan dengan teknik steganografiyang disembunyikan ke dalam sebuah media berupa citra digital gambar dengan format .jpg

DAFTAR PUSTAKA

- [1] Achmad Noercholis & Yohanes Nugraha, 2016, *Pengamanan Data Tek Menggunakan Teknik Steganografi Spread Spectrum Berbasis Android*. Jurnal Antivirus, Vol.10, No.1, 1 Mei 2016 p-ISSN:1978-5232 e-ISSN:2527337X, 33-34
- [2] Aliy Hafiz, 2019, *Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB)*. Jurnal Cendikia, Vol. XVII Cendikia 2019 P-ISSN:0216-9436 Bandar Lampung, April 2019 E-ISSN:2622-682, 194-195.
- [3] Ari Septayuda, Dr., Ir. Bambang Hidayat, DEA & Hilal Hudan Nuha, MT, 2014, *Analisis Steganografi Citra Digital Menggunakan Metode Spread Spectrum Berbasis Android*. E-Proceeding of Engineering : Vol.1, No.1 Desember 2014 ISSN:2365-9365, 3.
- [4] Asep Saefullah, Himawan, & Nazori Agani. 2012. Aplikasi Steganografi Untuk Menyembunyikan Teks Dalam Media Image Dengan Menggunakan Metode LSB. Seminar Nasional Teknologi Informasi & Komunikasi Terapan. Semarang 23 Juni 2012, ISBN 979-26-0255-0. 152-156.
- [5] Azkar Kumala, Bambang Pramono & Rahmat Ramadhan. 2017. Implementasi Metode Spread Spectrum Dalam Steganografi Pada File MP3 Berbasis Android. SemanTIK. Vol.3 No.2, Jul-Des 2017. Pp.127-132 ISSN:2502-8928. 128-129.
- [6] Edi Winarno ST,M,Eng, Ali Zaki & SmitDev Community, 2015. VB.NET untuk Skripsi. PT. Elex Media Komputindo, Jakarta.
- [7] Fresly Nandar Pabokory, Indah Fitri Astuti & Awang Harsa Kridalaksana. 2015. Implementasi Kriptografi Pengamanan Data

- Pada Pesan Teks, Isi File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Jurnal Informatika Mulawarman. Vol.10 No.1 February 2015, 22.
- [8] Indra Gunawan & Sumarmo. 2018. Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video. Jurnal Sains Komputer & Informatika. Vol.2 No.1 Maret 2018, ISSN:2548-9771/EISSN:2549-7200, 58-60.
- [9] Heri Santoso, Abdul Halim Hasugian & Yusuf Ramadhan Nasution, Aplikasi Deteksi Perubahan Wilayah dengan Menggunakan Post-Classification. Jurnal Arma Informatika. Vol 3, No.1 Juli 2019 ISSN : 2615-6891, 1-14.
- [10] Jane Irma Sari, Sulindawaty & Hengki Tamando Sitohang. 2017, Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggunakan Algoritma Hill Cipher Dan Metode Least Significant Bit. Jurnal Mantik Penusa. Vol.1 No.2 Desember 2017. 2-3
- [11] Mesran & Darmawati, 2012, Aplikasi Pengamanan Data Teks Pada Citra Bitmap Dengan Menerapkan Metode Least Significant Bit (LSB). Pelita Informatika Budi Darma. Vol II, Desember 2012 ISSN : 2301-9425, 7-8.
- [12] Muhammad Iqbal, Taronisokhi Zebua & Ronda Deli Sianturi. 2019. Implementasi Algoritma Sprintz dan Metode Spread Spectrum Untuk Menyembunyikan Pesan Enkripsi Kedalam File Audio MP3. Konferensi Nasional Teknologi Informasi dan Komputer. Vol.3 No.1, Oktober 2019, ISSN:2597-4645, ISSN:2597-4610, 447-448
- [13] Riko Arlando Saragih, 2006, *Metode Parity Coding Versus Metode Spread Spectrum Pada Audio Steganography*. SNATI, ISSN:1907-5022, 72.
- [14] Siti Rohayah, Ginanjar Wiro Sasmito & Oman Somantri, 2015, Aplikasi Steganografi Untuk Penyisipan Pesan. JURNAL INFORMATIKA Vol. 9, No. 1, 976-977.
- [15] Sutoyo, T., Mulyanto, E Suhartono, V., & Nurhayati, O, D., 2009, *Teori Pengolahan Citra Digital*. Yogyakarta dan Semarang: C.V ANDI OFFSET dan ANDINUS Semarang.
- [16] Zaenal Rifai & Solichul Huda, 2013, *Aplikasi Pengamanan Data Email Dengan Teknik Steganografi*. Techno.COM, Vol. 12 No. 2, Mei 2013:73-8173, 75.