Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)

Vol.13. No.1, Februari 2020, pp. 82~87

P-ISSN : 1978-6603

E-ISSN : 2615-3475

Strategi Pengamanan Pesan Rahasia Menggunakan Teknik Steganografi Pada Citra Digital Dengan Metode Least Significant Bit

***Faisal Taufik, Kamil Erwansyah, Dicky Nofriansyah**

Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:

Received Jun 12th, 2020

Revised Aug 20th, 2020

Accepted Aug 26th, 2020

Keyword:

Steganografi

Least Significant Bit

Citra Digital

ABSTRACT

Keamanan dari sebuah pesan yang bersifat personal atau rahasia merupakan salah satu aspek terpenting yang harus dilakukan oleh pembuat atau pemberi pesan, yang biasanya informasi yang dianggap rahasia tersebut akan diamankan dengan cara merubahnya menjadi kode-kode rahasia menggunakan teknik kriptografi namun dapat diketahui bahwasanya kode-kode itu merupakan sebuah pesan. Berbeda dengan teknik kriptografi, steganografi merupakan sebuah teknik untuk menyembunyikan pesan yang bersifat rahasia ke dalam pesan dengan tujuan agar tidak diketahui akan keberadaan dari pesan rahasia tersebut karena disembunyikan di dalam pesan. Penyembunyian pesan tersebut dilakukan dengan cara menyisipkannya ke dalam sebuah citra digital (image) dengan menggunakan metode least significant bit dengan harapan agar citra digital yang dihasilkan setelah dilakukan proses penyembunyian pesan tidak mengalami perubahan dari segi gambarnya, atau citra digital yang digunakan sebelum dan sesudah disisipkan sebuah pesan tetap sama jika dilihat. Dari hasil uji coba yang telah dilakukan metode least significant bit dapat menyembunyikan pesan ke dalam citra digital dengan cara menyisipkan bit-bit pesan ke dalam byte dari citra digital tanpa merubah citra digital itu sendiri sehingga tidak akan diketahui akan keberadaan pesan yang telah disembunyikan didalamnya.

Corresponding Author: *First Author

Faisal Taufik

Sistem Informasi

STMIK Triguna Dharma

faisal.taufik04@gmail.com

1. PENDAHULUAN

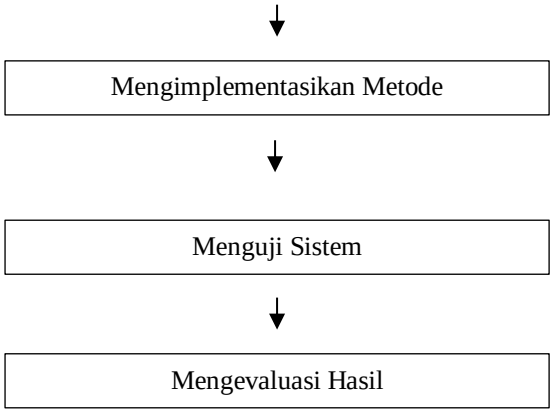
Keamanan dari sebuah pesan yang bersifat rahasia merupakan salah satu aspek terpenting [1] yang harus dilakukan oleh pembuat pesan itu sendiri sebelum pesan itu ditransmisikan, yang biasanya berbagai upaya dilakukan untuk melindungi pesan rahasia tersebut dari orang-orang yang dirasa tidak berhak untuk mengetahui isi pesannya. Salah satu upaya yang dilakukan adalah dengan menyamarkan isi pesan tersebut menggunakan teknik kriptografi yang menghasilkan kode-kode yang sulit untuk dipahami [2], namun cara tersebut bisa dianggap belum cukup dalam mengamankan suatu pesan dikarenakan masih terlihatnya pesan tersebut walaupun dalam bentuk kode-kode yang sulit untuk dimengerti sehingga bagi orang yang memiliki kemampuan dalam teknik kriptografi bisa mencoba untuk memecahkan isi pesan tersebut.

Berbeda halnya dengan teknik kriptografi, teknik steganografi merupakan sebuah ilmu dan seni yang digunakan untuk menyembunyikan sebuah pesan yang bersifat rahasia ke dalam pesan (ada pesan di dalam pesan) dengan tujuan agar tidak diketahui akan keberadaan dari pesan rahasia tersebut karena disembunyikan di dalam sebuah pesan [3]. Penyembunyian pesan tersebut dilakukan dengan cara menyisipkannya ke dalam sebuah wadah penampung seperti teks, citra digital (gambar), suara (audio), dan video [4], yang dalam penelitian ini menggunakan wadah penampung berupa citra digita (gambar). Dengan hal tersebut maka isi pesan rahasia yang telah disembunyikan tidak akan terlihat sehingga tidak diketahui keberadaan pesan tersebut.

Dalam penerapan teknik steganografi terdapat beberapa metode yang dapat digunakan, diantaranya adalan dengan menggunakan metode least significant bit [5]. Metode least significant bit bekerja dengan cara mengganti bit-bit data yang rendah atau paling kanan [6] dengan harapan agar citra digital yang dihasilkan setelah dilakukan proses penyembunyian pesan tidak mengalami perubahan dari segi gambarnya, atau citra digital yang digunakan sebelum dan sesudah disisipkan sebuah pesan tetap sama jika dilihat.

2. METODE PENELITIAN

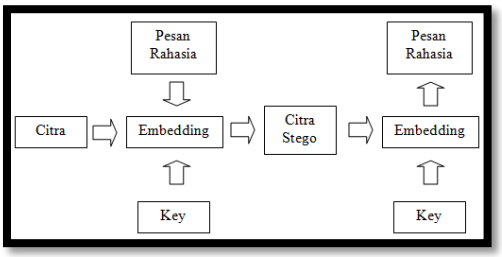
Sebuah kerangka kerja penelitian dibuat untuk dijadikan sebagai pedoman dalam melaksanakan penelitian dan disusun ke dalam bentuk kerangka kerja (*framework*), dimana pada kerangka kerja yang dibuat dapat dilihat kegiatan-kegiatan dalam melakukan penelitian ini.



Gambar 1. Kerangka Kerja Penelitian

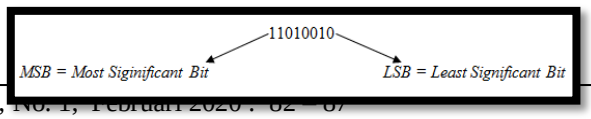
3. ANALISA DAN HASIL

Agar suatu kerahasiaan dari sebuah pesan yang dianggap personal ataupun rahasia yang tersimpan di dalam sebuah gambar tetap terjaga, maka dibutuhkan suatu kunci yang dapat digunakan untuk mengambil pesan rahasia yang telah disisipkan ke dalam objek citra penampung tersebut yang disebut dengan istilah *key*. Dengan adanya kunci (*key*) yang digunakan maka hanya yang mengetahui kuncinya saja yang bisa mengambil pesan rahasia yang telah disisipkan ke dalam objek citra penampung. Untuk lebih jelasnya proses dari Steganografi dapat dilihat pada gambar berikut.



Gambar 2. Gambaran Proses Steganografi

Penyembunyian sebuah pesan dilakukan dengan cara mengganti tiap bit-bit data yang tidak terlalu berpengaruh dalam segmen citra dengan bit-bit pesan yang akan disisipkan ke dalam citra tersebut, Pada susunan bit yang terdapat dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti yaitu *most significant bit* (*MSB*) dan bit yang kurang berarti yaitu *least significant bit* (*LSB*). Untuk lebih jelasnya sebuah susunan bit pada sebuah *byte* dapat dilihat pada gambar berikut:



Gambar 3. Gambaran Susunan bit

Proses analisa metode LSB yang dilakukan dengan mencoba untuk menyisipkan sebuah pesan “saya” ke dalam sebuah gambar yang berukuran 350 x 350 pixel dengan total *byte* yang dimiliki adalah 367500 *byte*.

Gambar 4. Gambar Yang Digunakan

Sebelum isi pesan dapat disisipkan ke dalam sebuah gambar, isi pesan tersebut harus direpresentasikan ke dalam 8 bit kode biner.

Tabel 1. Kode Biner Isi Pesan

Karakter	Bilangan ASCII	Kode Biner
s	115	01110011
a	97	01100001
y	121	01111001
a	97	01100001

Untuk selanjutnya, tiap bit kode biner pesan rahasia digunakan untuk menggantikan bit terakhir dari kode biner citra yang digunakan. Proses penggantian dilakukan dengan memilih *byte* tertentu secara acak. Proses pengacakan tersebut bergantung pada kata kunci (*password*) yang menjadi *random seed* atau titik awal dilakukannya pengacakan. Kata kunci yang coba dimasukkan adalah “DIA”

Tabel 2. Kode Biner Kunci (*Key*)

Karakter	Bilangan ASCII	Kode Biner
D	68	01000100
I	65	01000001
A	73	01001001

Untuk menentukan lokasi penyisipan pesan pada gambar menggunakan persamaan:

$X_{n+1} = (aX_0 + c) \bmod p$

- Dimana X_{n+1} adalah bilangan acak yang dihasilkan.
- *p* adalah jumlah *pixel* dikali 3 (tiga), dimana tiap *pixel* citra 24 bit memiliki tiga komponen warna yaitu *red*, *green* dan *blue* masing-masing 1 *byte* (8 bit).
- *a* adalah nilai karakter kata kunci kedua sebagai pengali *(multiplier).*
- *c* adalah nilai karakter kata kunci ketiga penambah *(increment).*
  X_0 adalah nilai karakter kata kunci pertama nilai awal *(seed or start value).*

Maka :

$X_1 = (65 (68) + 73) \bmod 367500$

$X_1 = 4493$

$X_2 = (4493 (68) + 73) \bmod 367500$

$X_2 = 305597$

$X_3 = (305597 (68) + 73) \bmod 367500$

$X_3 = 200669$

$X_4 = (200669 (68) + 73) \bmod 367500$

$X_4 = 48065$

$X_5 = (48065 (68) + 73) \bmod 367500$

$X_5 = 328493$

$X_6 = (328493 (68) + 73) \bmod 367500$

$X_6 = 287597$

$X_7 = (287597 (68) + 73) \bmod 367500$

$X_7 = 79169$

$X_8 = (79169 (68) + 73) \bmod 367500$

$X_8 = 238565$

$X_9 = (238565 (68) + 73) \bmod 367500$

$X_9 = 52493$

$X_{10} = (52493 (68) + 73) \bmod 367500$

X_{10} = 262097

X_{11} = (262097 (68) + 73) mod 367500

X_{11} = 182669

X_{12} = (182669 (68) + 73) mod 367500

X_{12} = 294065

X_{13} = (294065 (68) + 73) mod 367500

X_{13} = 151493

X_{14} = (151493 (68) + 73) mod 367500

X_{14} = 11597

X_{15} = (11597 (68) + 73) mod 367500

X_{15} = 53669

X_{16} = (53669 (68) + 73) mod 367500

X_{16} = 342065

X_{17} = (342065 (68) + 73) mod 367500

X_{17} = 107993

X_{18} = (107993 (68) + 73) mod 367500

X_{18} = 361097

X_{19} = (361097 (68) + 73) mod 367500

X_{19} = 299669

X_{20} = (299669 (68) + 73) mod 367500

X_{20} = 165065

X_{21} = (165065 (68) + 73) mod 367500

X_{21} = 199493

X_{22} = (199493 (68) + 73) mod 367500

X_{22} = 335597

X_{23} = (335597 (68) + 73) mod 367500

X_{23} = 35669

X_{24} = (35669 (68) + 73) mod 367500

X_{24} = 220565

X_{25} = (220565 (68) + 73) mod 367500

X_{25} = 298493

X_{26} = (298493 (68) + 73) mod 367500

X_{26} = 85097

X_{27} = (85097 (68) + 73) mod 367500

X_{27} = 274169

X_{28} = (274169 (68) + 73) mod 367500

X_{28} = 268565

X_{29} = (268565 (68) + 73) mod 367500

X_{29} = 254993

X_{30} = (254993 (68) + 73) mod 367500

X_{30} = 67097

X_{31} = (67097 (68) + 73) mod 367500

X_{31} = 152669

X_{32} = (152669 (68) + 73) mod 367500

X_{32} = 91565

Berikut ini merupakan tabel pengalokasian penyisipan pesan pada *byte* citra digital yang digunakan sebagai penampung pesan.

Tabel 3. Lokasi Penyisipan Pesan

***Byte* "saya"**	**Kode Biner**
0	4493
1	305597
1	200669
1	48065
0	328493
0	287597
1	79169
1	238565
0	52493
1	262097
1	182669
0	294065
0	151493
0	11597
0	53699

1	342065
0	107993
1	361097
1	299669
1	165065
1	199493
0	335597
0	35669
1	220565
0	298493
1	85097
1	274169
0	268565
0	254993
0	67097
0	152669
1	91665

Adapun tampilan *user interface* dari aplikasi yang telah dirancang dapat dilihat pada gambar berikut.

Gambar 5. Tampilan User Interface Aplikasi

Gambar 5. Penyisipan Pesan

4. KESIMPULAN

Berdasarkan dari hasil analisa dan pembahasan sebelumnya dapat ditarik beberapa kesimpulan bahwa :

1. Pengamanan sebuah pesan rahasia menggunakan media citra digital dapat dilakukan dengan cara menyisipkan pesan tersebut ke dalam sebuah citra digital tanpa diketahui keberadaan pesan itu.
2. Metode Least Significant Bit dapat menyembunyikan pesan ke dalam media citra digital dengan cara menyisipkan bit-bit pesan ke dalam *byte* dari sebuah citra digital.
3. Aplikasi Steganografi yang dirancang memiliki *user interface* yang mudah untuk di mengerti sehingga akan memberikan kemudahan bagi penggunanya dalam proses penyembunyian pesan rahasia.

UCAPAN TERIMA KASIH

Terima kasih yang sebesar-besarnya penulis ucapkan kepada keluarga dan rekan-rekan sejawat yang telah memberikan dukungan dalam penyelesaian tulisan ini.

REFERENSI

[1] D. Darwis, “Implementasi Teknik Steganografi Least Significant Bit (LSB) Dan Kompresi Untuk Pengamanan Data Pengiriman Surat Elektronik,” *J. Teknoinfo,* vol. 10, no. 2, p. 32, 2016.

[2] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016.

[3] R. Tullah, R. Agusli, M. I. Dzulhaq, and I. Halim, "Perancangan Steganografi Dengan Media Gambar Pada Aplikasi Berbasis Android," *J. Sisfotek Glob.*, vol. 1, no. 1, pp. 1–7, 2014.

[4] A. Saefullah, Himawan, and N. Agani, "Aplikasi Steganografi Untuk Menyembunyikan Teks Dalam Media Image Dengan Menggunakan Metode LSB," *Semin. Nas. Teknol. Inf. Komun. Terap. 2012 (Semantik 2012)*, vol. 2012, no. Semantik, pp. 151–157, 2012.

[5] S. Lutfi and Rosihan, "Perbandingan Metode Steganografi LSB (Least Significant Bit) Dan MSB (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia Kedalam Citra Digital," *JIKO (Jurnal Inform. dan Komputer) UNKHAIR*, vol. 02, no. 1, pp. 34–42, 2018.

[6] D. Nugroho, "Penerapan Steganografi Pada File Gambar (Jpg)," vol. 1, no. 1, pp. 53–58, 2016.