STEGANOGRAFI BERBASIS CITRA DIGITAL UNTUK MENYEMBUNYIKAN DATA MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* (LSB)

Aliy Hafiz
Manajemen Informatika, AMIK Dian Cipta Cendikia
Jl. Cut Nyak Dien No. 65 Durian Payung (Palapa) Bandar Lampung
e-mail: hafiz@dcc.ac.id.

ABSTRAKS

Kerahasiaan data merupakan hal yang sangat sangat penting dalam suatu organisasi maupun untuk pribadi. Apalagi kalau data tersebut berada dalam suatu sistem komputer, jaringan komputer bahkan dalam jaringan internet.kebutuhan akan keamanan dan kerahasiaan menjadi kebutuhan pokok saat ini. Karena maraknya pembajakan data maupun pencurian data. Steganografi bisa menjadi solusi dalam menjaga kerahasiaan data dan keamanan dari data yang dimiliki. Data yang ada akan disembunyikan sehingga tidak semua orang bisa melihat dan menggunakannya. Dengan metode Least Significant Bit, Steganografi bisa dilakukan dengan menyisipkan data kedalam gambar yang diinginkan. Proses yang terjadi adalah bit-bit data akan disisipkan ke dalam bit citra digital sehingga bit data akan berada di dalam bit wadah citra digital tersebut untuk disembunyikan. Dengan adanya steganografi dan metode Least Significant Bit data bisa disembunyikan kemuian diambil kembali untuk bisa dibaca oleh pemilik data.

Kata Kunci: Steganografi, LSB, Data, Citra Digital

1. PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi informasi, semakin berkembang pula teknik kejahatan yang berupa perusakan maupun pencurian data oleh pihak yang tidak memiliki wewenang atas data tersebut. Dengan berbagai teknik seseorang bisa mengakses informasi secara ilegal, sehingga banyak yang mencoba untuk mengakses informasi yang bukan haknya. Oleh karena itu, pada saat ini telah dilakukan berbagai upaya untuk menjaga keamanan dan kerahasiaan dari data dan informasi.

Berbagai macam teknik digunakan dalam upaya mengamankan suatu data penting. Sebelumnya telah digunakan untuk menjaga keamanan data yang dikenal dengan nama kriptografi. Dengan kriptografi data rahasia terjaga keamanannya, namun bentuk chipertext yang diacak akan mudah terdeteksi dan menyadarkan pihak ketiga akan kerahasiaan data tersebut. Selanjutkanya diterapkan steganografi dalam usaha menjaga kerahasiaan data berupa penyembuat bit-bit data kedalam bit wadah yang berupa citra digital.

Steganografi pada citra digital dapat dijadikan alternatif untuk menyimpan data rahasia kedalam wadah citra digital. Steganografi bisa digunakan juga untuk menyampaikan pesan yang bersifat rahasia, karena sifat dari steganografi yaitu sulit dideteksi keberadaannya karena tersembunyi. Untuk system keamanan komputer, steganografi dapat digunakan untuk menyembunyikan data rahasia pada saat proses enkripsi tidak dapat dilakukan atau bersamaan dengan proses enkripsi itu sendiri (Darwis, 2016).

Metode yang digunakan dalam steganografi ini adalah metode Spread spectrum dalam pengacakan pesan dan menggunakan metode Modifikasi LSB (*Least Significant Bit*) dalam menyisipkan pesan rahasia ke media citra digital. I-2 Modifikasi LSB dilakukan dengan mengganti bit-bit data yang kurang berarti di dalam segmen citra dengan bit-bit pesan rahasia.

1.2 Tinjauan Pustaka

Dasar dan teori-teori dari hasil berbagai penelitian sebelumnya merupakan hal yang dapat dijadikan sebagai data pendukung.Salah satu datapendukung yang dijadikan sebagian acuan adalah penelitian terdahulu yang relevandan permasalahan yang dibahas dalam penelitian tersebut. Dalam penelitiannya Ari Muzakir (2016), Dengan judul penelitian Implementasi Teknik Steganografi Dengan Kriptografi Kunci Private AES Untuk Keamanan File Gambar Berbasis Androiddi Ilmu KomputerUniversitas Bina Darma Palembang mengunakan algoritma aes berhasil membangun aplikasi penyisipan teks gambar menggunakan perangkat mobile android. Kemudian penelitian oleh

Michael Sitorus (2015), dengan judul penelitian Teknik steganografi Dengan Metode *Least Significant Bit (*LSB), agar stegonografi lebih kuat menyembunyikan data maka pesan text terlebih dahulu di enkripsi menggunakan algoritma kriptografi. Pada penelitian ini Metode yang digunakan adalah *Least Significant bit insertion* (LSB).

a. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu kryptos yang memiliki arti tersembunyi atau rahasia dan graphein artinya menulis. Kriptografi adalah ilmu untuk mengenkripsi atau mengacak, dimana data asli atau plaintext diacak menggunakan kunci enkripsi untuk menjadi naskah acak yang sulit dibaca atau yang disebut dengan ciphertext.
Secara umum berdasarkan kesamaan kuncinya algoritma sandi dibedakan menjadi ;
1. Algoritma Kunci Simetris.
2. Algoritma Kunci Asimetris.

Berdasarkan arah implementasi dan pembabakan zamannya dibedakan menjadi ;
1. Algoritma Sandi Klasik.
2. Algoritma Sandi Modern

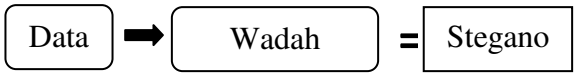
Berdasarkan kerahasiaan kuncinya dibedakan menjadi ;
1. Algoritma Sandi Kunci Rahasia
2. Algoritma Sandi Kunci Publik

Algoritma kriptografi terdiri atas 3 (tiga) fungsi dasar, yaitu :

1. Enkripsi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaanya. Pesan asli disebut plaintext, yang diubah menjadi kode – kode yang tidak dimengerti.
2. Dekripsi, merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya disebut dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
3. Kunci, yang dimaksud disini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi 2 bagian yaitu : kunci rahasia (private key) dan kunci umum (public key).

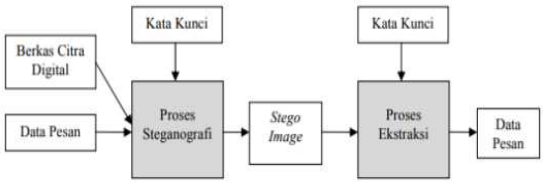
b. Steganografi

Steganografi berasal dari bahasa Yunani yaitu Steganos yang berarti menyembunyikan dan Graptos yang artinya tulisan, sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan.Secara umum steganografi adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia. Steganografi sangat kontras dengan kriptografi (Ukkas, 2017). Kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, sedangkan steganografi menutupi keberadaan pesan.Steganografi dapat dipandang sebagai kelanjutan dari kriptografi.



Gambar 1. Properti Steganografi

Dalam praktiknya, agar data menjadi lebih aman, data diacak terlebih dahulu menggunakan kriptografi, kemudian baru dilakukan proses steganografi agar lebih maksimal dalam mengamankan dan menjaga kerahasiaan. Steganografi membutuhkan dua properti, yaitu data dan wadah penampung data. wadah penampung yang umumnya digunakan berupa teks, suara, gambar, atau video. Sedangkan data yang disembunyikan dapat berupa teks, gambar, atau data yang lainnya.



Gambar 2. Model sistem Steganografi

Keuntungan menggunakan steganografi adalah memungkinkan pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim karena pesan tersembunyi. Ini membuat pihak ketiga tidak menyadari keberadaan pesan. Sebaliknya, penggunaan kriptografi akan menarik kecurigaan pihak ketiga bahwa ada sesuatu yang disembunyikan dalam pesan yang sedang dikirim. Steganografi juga memiliki kelemahan. Akan tetapi steganografi memerlukan banyak ruang untuk dapat menyembunyikan beberapa bit pesan. kelemahan ini terus diatasi dengan perkembangan teknik-teknik dalam melakukan steganografi.

c. Least Significant Bit (LSB)

Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri.

Contohnya adalah bilangan biner dari 255 adalah 11111111 (kadang-kadang diberi huruf b pada akhir bilangan menjadi 1111 1111b). Bilangan tersebut dapat berarti:

$$1*2^7+1*2^6+1*2^5+1*2^4+1*2^3+1*2^2+1*2^1+1*2^0=128+64+32+16+8+4+2+1=255$$

Dari barisan angka 1 di atas, angka 1 paling kanan bernilai 1, dan itu adalah yang paling kecil. Bagian tersebut disebut dengan least significant bit (bit yang paling tidak berarti), sedangkan bagian paling kiri bernilai 128 dan disebut dengan most significant bit (bit yang paling berarti).

Least significant bit sering kali digunakan untuk kepentingan penyisipan data ke dalam suatu media digital lain, salah satu yang memanfaatkan Least significant bit sebagai metode penyembunyian adalah steganografi audio (Rajab, 2017).

d. Citra Digital

Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpunan/ diskrit nilai digital yang disebut pixel/ picture elements. Citra digital dapat dibedakan menjadi dua, yaitu raster dan vektor. Pada umumnya, yang disebut dengan citra digital adalah citra digital dalam bentuk raster atau yang biasa disebut dengan citra bitmap (Al Caruban, 2018).

1.3 Metode Pengembangan Sistem

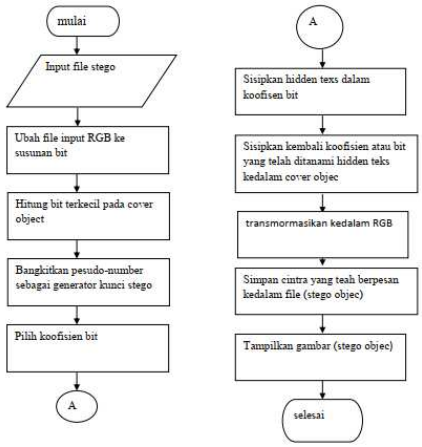
Metode Pengembangan system yang digunakan adalah extreme programming. Secara umum *Extreme Programming* (XP) dapat dijabarkan sebagai sebuah pendekatan pengembangan perangkat lunak yang mencoba meningkatkan efisiensi dan fleksibilitas dari sebuah proyek pengembangan perangkat lunak dengan mengkombinasikan berbagai ide simpel/sederhana tanpa mengurangi kualitas software yang akan dibagun (Firdaus, 2017). Proses pengembangan pada extreme programming dimulai dari perencangaan, perancangan, pengkodean, dan terakhir pengujian.

1.4 Metode Perancangan Sistem

UML adalah sekumpulan alat yang digunakan untuk melakukan abstraksi terhadap sebuah sistem atau perangkat lunak berbasis objek. UML juga menjadi alat bantu yang digunakan untuk *transfer* ilmu tentang sistem atau aplikasi yang akan dikembangkan dari satu *developer* ke *developer* lainya. Tidak hanya antar *developer* , UML bisa digunakan siapapun karena mudah dipahami. Perancangan dimulai dengan use case diagram, class diagram, activity diagram, sequence diagram.

2. PEMBAHASAN

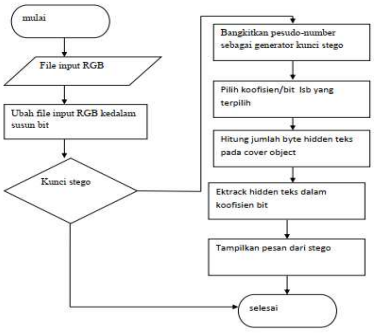
Hasil penelitian ini digambarkan kedalam diagram alir berikut ini;



Gambar 2. Proses Penyisipan (*Embedding*) /Stegano Pesan Ke Citra Digital

Pada gambar 2 di atas merupakan proses penyisipan data ke dalam gambar yang akan menjadi wadah untuk disisipi data. Proses penyisipan ketika data telah dipecah kedalam bit-bit kemudian disisipkan kedalam bit citra yang menjadi wadah menggunakan metode *Least Significant Bit* (LSB). Adapun untuk proses pengembalian gambar yang telah disisipi data untuk diambil data dapat dilihat pada diagram alir di bawah ini.

P-ISSN:0216-9436
E-ISSN:2622-6782



Gambar 3. Proses Ekstaksi Citra Digital yang telah berisi data

Pada gambar 3 di atas merupakan proses dekripsi dari citra yang telah dijadikan wadah dari data setelah steganografi. Adapun proses stegano atau penyisipan data ke dalam gambar dengan menggunakan perubahan data ke dalam bilangan biner. Seperti di bawah ini:

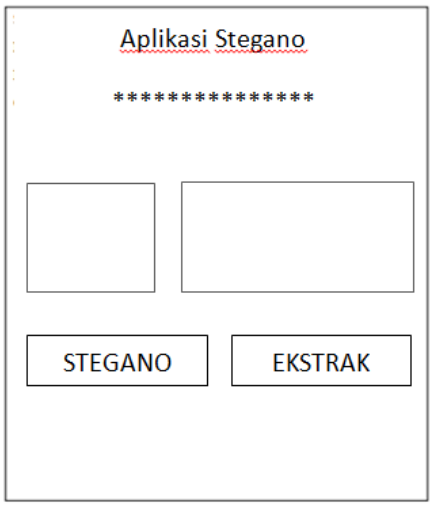
Perubahan citra ke dalam bilangan biner, pada table di bawah ini

(100,50,100)	(70,50,80)	(75,60,75)
(101,43,23)	(10,20,50)	(52,40,35)
(20,10,40)	(54,43,31)	(55,40,65)

Kemudian dikonverisi ke bilangan biner dalam hitungan bit.

00101001, 00100001	00100001, 00001001	00011001, 00001001
00101011, 00111001	00000010, 00000110	00001001, 00001001
00000011, 00001001	00001001, 00001001	00101001, 00010001

Adapun untuk desain interface dari aplikasi steganografi menggunakan metode *Least Significant Bit* (LSB) adalah sebagai berikut:



Gambar 4. Desain interface dari aplikasi steganografi

Gambar 5. Menu utama aplikasi steganografi

Gambar 5. Menu stegano aplikasi steganografi

P-ISSN:0216-9436
E-ISSN:2622-6782

Gambar 6. Menu ekstraksi aplikasi steganografi

3. SIMPULAN

Penyisipan pesan tersembunyi berupa data dapat dilakukan ke dalam wadah citra digital berformat JPEG dan format citra digital lainnya, kemudian dapat mengekstraksi kembali data tersembunyi tersebut dari dalam citra digital. Terjadi perubahan pada ukuran citra digital namun secara kasat mata perbedaan antara gambar sebelum dan sesudah disisipkan pesan tidak terlihat. Selain itu waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dipengaruhi oleh kecepatan komputer yang digunakan dan ukuran citra.

PUSTAKA

Al Caruban, R., Sugiantoro, B., & Prayudi, Y. (2018). Analisis Pendeteksi Kecocokan Objek Pada Citra Digital Dengan Metode Algoritma Sift Dan Histogram Color Rgb. *Cyber Security dan Forensik Digital*, *1*(1), 20-27.

Darwis, D. (2016). Implementasi Teknik Steganografi Least Significant Bit (LSB) Dan Kompresi Untuk Pengamanan Data Pengiriman Surat Elektronik. *Jurnal Teknoinfo*, *10*(2), 32-38.

Firdaus, M. A. (2017). Implementasi Kerangka Kerja Scrum Pada Manajemen Pengembangan Sistem Informasi. *Semnasteknomedia Online*, *5*(1), 1-2.

Muzakir, A. (2016). Implementasi Teknik Steganografi Dengan Kriptografi Kunci Private AES Untuk Keamanan File Gambar Berbasis Android. *SEMNASTEKNOMEDIA ONLINE*, *4*(1), 4-7.

Rajab, A. (2017). *Studi Komparasi Metode Least Significant Bit Dan Metode Echo Hiding Pada Audio Watermarking* (Doctoral dissertation, STMIK AKAKOM Yogyakarta).

Sitorus, M. (2015). Teknik Steganography Dengan Metode Least Significan Bit (LSB). *Faklutas Teknik. Universitas Satya Negara Indonesia*.

Ukkas, M. I., Andrea, R., & Anggen, A. B. P. (2017). Teknik Pengamanan Data Dengan Steganografi Metode End Of File (EOF) Dan Kriptografi Vernam Cipher. *Sebatik*, *17*(1), 20-26.