Jurnal Riset Komputer (JURIKOM), Vol. 6, No. 5, Oktober 2019
ISSN 2407-389X (Media Cetak)
Hal: 447-452

Stegnografi Menggunakan Metode Least Significant Bit dan Quick Response Code (QR-Code)

Ispandi[1], Ahmad Fauzi[2], Sugiono[2]

[1] STMIK Nusa Mandiri Jakarta, Jakarta Pusat, Indonesia
[2] Magister Ilmu Komputer, STMIK Nusa Mandiri Jakarta, Jakarta Pusat, Indonesia
Email: [1]ispandi.ipd@nusamandiri.ac.id, [2]ahmad.aau@bsi.ac.id, [2]Sugiono.sgx@bsi.ac.id

Abstrak

Trasmisi informaisi melalui internet dapat mencakup data pribadi yang sensitif yang dapat disadap, ada banyak aplikasi dan situs web yang memerlukan keamanan yang baik guna menghindari kejahatan yang terjadi pencurian dokumen dan informasi rahasia. Stegnografi adalah seni dan sains untuk menulis pesan tersembunyi sedemikian rupa sehingga tidak ada yang terpisah dari pengiriman dan penerima yang dimaksudpun mengetahui ada pesan tersembunyi, image sebagai salah satu dari sekian banyak media digital yang bisa digunakan sebagai object untuk menyisipkan sebuah pesan atau kode rahasia yang dengan menggunakan metode Least Significant Bit (LBS) Metode ini menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam cover dengan bit-bit data rahasia. Dari meode ini penulis akan mengkombinasikan dengan Quick Response Code (QR),guna menghasilkan sebuah enkripsi yang memiliki keamanan yang lebih prima,hasil dari embedding cover image menjadi stgno image, akan dienkripsi kembali kedalam Quick Response Code (QR).

Kata Kunci: Stegnografi, Quick Response Code (QR), metode Least Significant Bit (LBS)

Abstract

Transmission of information through the internet can involve sensitive personal data that can be tapped, there are many applications and websites that require good security to avoid the safety of theft of documents and confidential information. Stegnography is the art and science of writing stored secret messages that are not separate from the sending and the recipient is asked related to hidden messages, images as one of the many digital media that can be used as objects to insert messages or secret messages using methods Least Significant Bit (LBS) This method determines data by replacing the bits of data that at least means that it is closed with bits of confidential data. From this meode the author will combine with the Quick Response Code (QR), in order to produce encryption that has higher security, the result of embedding the cover image into a stgno image, will be encrypted again to Quick Response Code (QR).

Keywords: Stegnography, Quick Response Code (QR), Least Significant Bit (LBS) method

1. PENDAHULUAN

Secara teori penyisipan informasi pada data digital dengan menggunakan teknik steganografi dapat dilakukan pada semua format data digital yang ada dalam komputer sebagai media covernya seperti format teks, format gambar, bahkan untuk format audio dan sebagainya asalkan file-file tersebut mempunyai bit-bit data redundan yang dapat dimodifikasi. Steganograf membuat data satu informasi yang dikirimkan menjadi lebih aman dengan berbagai cara. Salah satu metode steganografi adalah Least Significant Bit, teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia.

Tujuan dari makalah ini untuk menujukan keamanan yang lebih baik. stegnografi menggunakan LBS, embedding pesan rahasia menjadi gambar digital, diwakili perlindungan kemungkinan informasi rahasia. Metode steganografi gambar meliputi prinsip- prinsip ini dari embedding rahasia.pertama didasarkan pada modifikasi Least Significant Bit (LSB) [1]. LSB metode steganalytic memiliki keuntungan dari encode sederhana dan dijamin decoding sukses jika gambar tidak berubah oleh kebisingan atau serangan. Penambhan, dari beberapa proses enkripsi yang sudah dilakukan akan dipadukan dengan Quick Response Code (QR), sehingga menghasilkan keamanan yang lebih prima dari sebelumnya dan mampu merikan enkripsi yang cepat.

2. METODE PENELITIAN

2.1 Steganografi

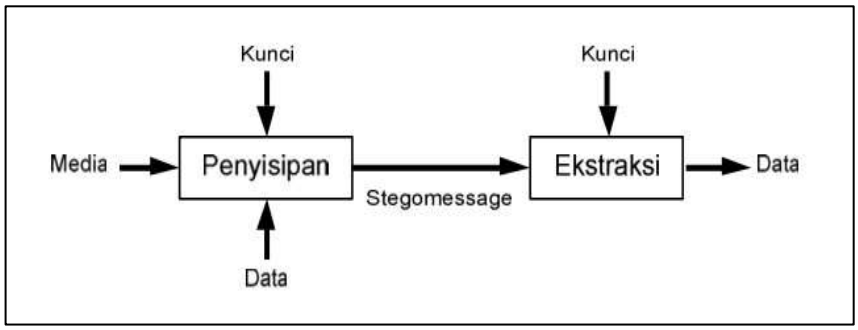
Stegnografi adalah ilmu dan seni menulis atau menyembunyikan pesan kedalam sebuah media. Stegnografi merupakan salah satu benuk komunikasi trsembunyi yang secara harfiah berarti ”tulisan tertutup” pesannya terbuka ,selalu terlihat tetapi tidak terditeksi adanya pesan rahasia deskripsi lain untuk stegnografi adalah *Hidden in Plain sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi tempat pesan acak tidak dapat dibaca dan keberadaan pesan sering dikenal[8].

Salah satu esensial yang menjadi kelebihan stegnografi adalah kemampuannya untuk menipu persepsi seseorang untuk mencurigai adanya pesan tersembunyi didalamnya. Namun begitu terbentuk pula suatu teknik yang dikenal dengan steganalysis, yaitu suatu teknik yang digunakan untuk mendeteksi penggunaan steganografi pada suatu pesan yang terdapat didalam media yang dijadikan sebagai media menyembunyikan sebuah pesan, seorang steganalyst tidak berusaha untuk melakukan dekripsi terhadap informasi yang tersembunyi, yang dilakukan adalah berusaha untuk menemukannya. Terdapat beberapa cara yang dapat digunakan untuk mendeteksi steganografi seperti melakukan pengamatan terhadap suatu dokumen atau suatu object yang telah di modifikasi dan membandingkannya dengan salinan dokumen yang dianggap belum direkayasa, atau berusaha mendengarkan dan melihat dan membandingkan perbedaannya dengan arsip lain bila arsip tersebut adalah dalam bentuk audio atau video [2]. Ada tiga hal yang harus diperhatikan dalam menggunakn stegnografi yaitu :

1. *Impercepbility*

Keberadaan penyisipan pesan rahasia dalam media penampung tidak dapat dideteksi, jika covertext berupa citra digital, maka pesan membuat citra stegotext sukar dibedakan oleh mata dengan covertext-nya

2. *Fidelity*
   Mutu media penampung tidak berubah banyak akibat penyisipan. Misalnya, jika covertext berupa citra, maka penyisipan pesan dapat membuat citra stegotext sukar dibedakan. Jika covertext berupa audio, maka audio stegotext tidak rusak dan indera telinga tidak dapat mendeteksi perubahan pada filestegotext-nya.
3. *Recovery*
   Pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah data hidding, maka sewaktu-waktu pesan rahasia di dalam stegotext dapat diambil kembali untuk digunakan **lebih lanjut.**

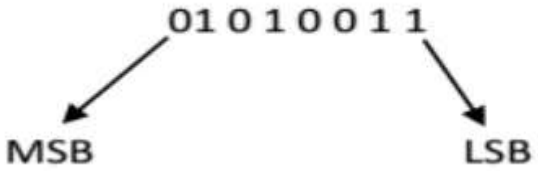


Gambar 1. Proses Steganografi [7]

2.2 Format Tampilan Dokumen

Least Significant Bit (LSB) metode pendekatan yang paling sederhana untuk menyisipkan informasi dalam satu citra digital [3] Metode ini menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam cover dengan bit-bit data rahasia. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti Most Significant Bit (MSB) dan bit yang paling kurang berarti Least Significant Bit (LSB)[9].

Pada susunan bit di dalam sebuah byte, ada bit yang paling berarti most significant bit atau MSB dan bit yang paling kurang berarti least significant bit atau LSB. Gambar 2 menjelaskan posisi MSB dan LSB dalam susunan bilangan biner pada 1 byte atau 8 bit.



Gambar 2. Posisi MSB dan LSB pada bilangan biner 8 bit

(00100111 11101001 11001000) (00100111 11001000 11101001)

Untuk menyisipkan sebuah karakter “C” dengan bilangan biner 01000011 (kode ASCII 67) kedalam 2 pixel citra warna tersebut, setiap 2 bit dari pesan yang dimulai dari MSB disisipkan kedalam 2 bit LSB dari setiap byte citra warna. Hasil penyisipannya memberikan nilai pixel baru sebagai berikut:

(00100**01** 11101**00** 11001**00**) (00100**11** 11001000 11101001)

2.3 Citra Digital

Secara harafiah, citra (image) adalah gambar pada bidang dua dimensi Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (continue) dari intensitas cahaya pada bidang dwimatra [8] Ada beberapa format citra digital, antara lain: bmp, png, jpg, gif, pxc, dan sebagainya. Masing-masing format mempunyai perbedaan satu dengan yang lain terutama pada header file-nya. Namun ada beberapa yang memiliki kesamaan yaitu penggunaan pallete untuk penentuan warna pixel[10].

2.4 Embedding

Data embedded, yang tersembunyi dalam suatu gambar membutuhkan dua file. Pertama adalah gambar asli yang belum modifikasi yang akan menangani informasi tersembunyi, yang disebut cover image. File kedua adalah informasi pesan yang disembunyikan. Suatu pesan dapat berupa plaintext, chipertext, gambar lain, atau apapun yang dapat ditempelkan ke dalam bit-stream Ketika dikombinasikan [6].

2.5 Kriptografi

Kata Kriptografi berasal dari bahasa yunani "crypto" yang berarti rahasia dan "graphien" yang berarti tulisan, Menurut terminologinya, kriptografi adalah seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain

1. Kerahasiaan Menjaga isi dari suatu pesan dari siapapun kecuali kepada orang yang memiliki otoritas terhadap data yang disandikan dalam bentuk kunci dekripsi.
2. Integritas Data Dalam kriptografi akan dilakukan proses pengecekan apakah data yang sampai di penerima merupakan benar data yang pertama kali dikirim oleh pengirim.
3. Autentikasi Pada proses autentikasi ini data akan dicek apakah mengalami manipulasi dalam isinya seperti penyisipan, penghapusan dan penggantian data.

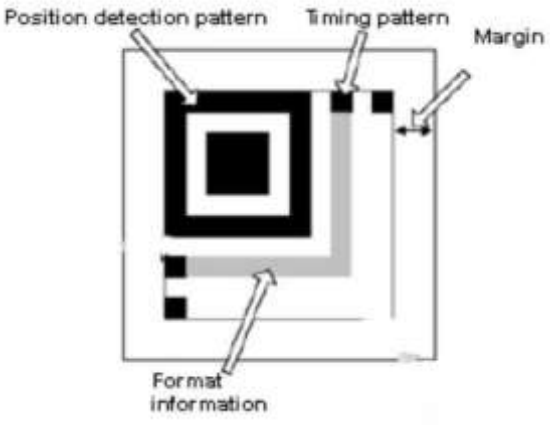
Non-Repudiasi Jika seseorang sudah mengirimkan pesan, maka orang tersebut tidak dapat membantah/ menyangkal pengiriman pesan tersebut.

2.6 *Quick Response Code* (QR-Code)

QR-Code merupakan teknik yang mengubah data tertulis menjadi kode-kode 2-dimensi yang tercetak kedalam suatu media yang lebih ringkas.[2], Jumlah data yang dapat disimpan dalam simbol QR code tergantung pada datatype (mode, atau karakter masukan set), versi (1, 2, ..., 40, yang menunjukkan keseluruhan dimensi simbol), dan tingkat koreksi kesalahan.Ada empat tingkat koreksi kesalahan (tingkat L - 7%, M - 15%, Q - 25% dan H - 30% dari codeword dapat dikembalikan) menunjukkan ukuran [1]

Gambar 3. *Quick Response Code*

Penjelasan rinci dari gambar *QR-Code* adalah sebagai berikut:



Gambar 4. *Quick Response Code*

1. *Position detection patterns*:
   Posisi pola deteksi diatur pada tiga sudut kode QR, Posisi dari kode QR terdeteksi dengan pola deteksi posisi yang memungkinkan kecepatan tinggi membaca dan dapat dibaca dari segala arah.
2. *Margin*
   Ini adalah area kosong di sekitar kode QR dan membutuhkan margin sebesar empat modul.
3. *Timing pattern*
   Modul putih dan modul hitam diatur secara bergantian untuk menentukan koordinat, Pola waktu ditempatkan di antara dua pola deteksi posisi dalam kode QR.
4. *Format Information*:
   Informasi Format dibaca pertama ketika kode tersebut diterjemahkan.

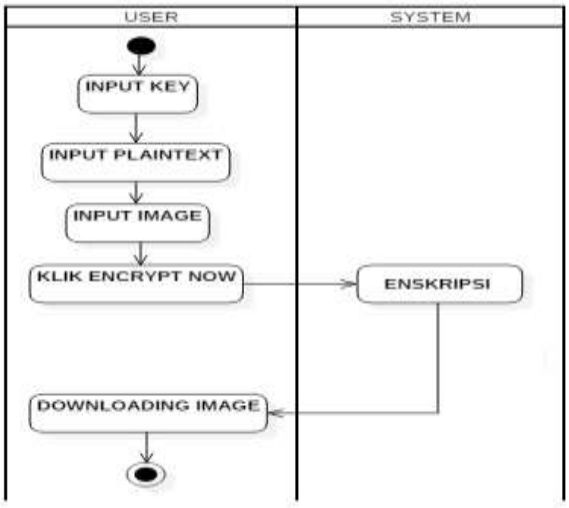
QR *Code* mampu menyimpan semua jenis data, seperti data angka/numerik, alpanumerik, biner, kanji/kana. Selain itu QR *Code* memiliki tampilan yang lebih kecil daripada *barcode*. Hal ini dikarenakan QR *Code* mampu menampung data secara horizontal dan vertikal, jadi secara otomatis ukuran dari tampilannya gambar QR *Code* bisa hanya sepersepuluh dari ukuran sebuah *barcode*. Tidak hanya itu, QR *Code* juga tahan terhadap kerusakan, sebab QR *Code* mampu memperbaiki kesalahan sampai dengan 30% tergantung dengan ukuran atau versinya[2]

3. ANALISA DAN PEMBAHASAN

Pada proses steganografi terdapat dua proses. Proses pertama adalah menyembunyikan pesan ke dalam media penampung pesan (*encode*). Dimana pesan yang disembunyikan ke dalam media dienkripsi terlebih dahulu. Proses kedua adalah pendeteksian pesan rahasia dari media penampung pesan (*decode*). Pada penelitian ini proses tersebut dipaparkan sebagai berikut :

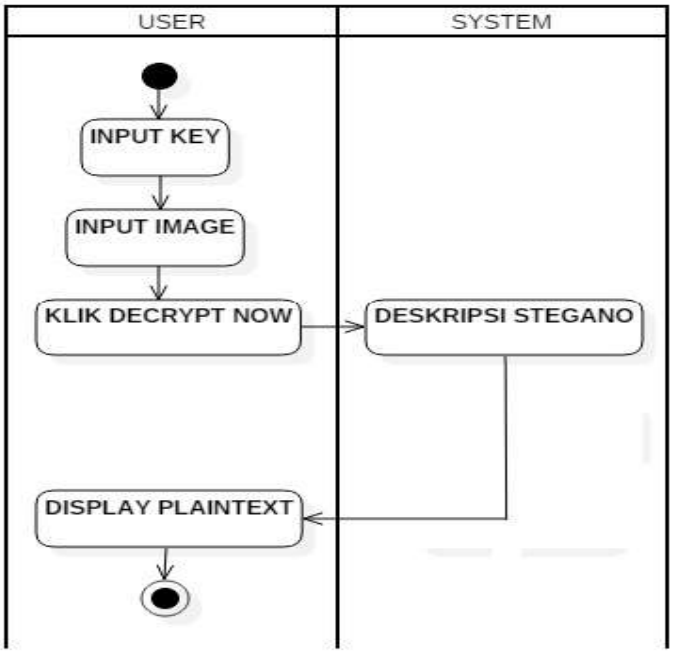
Misal pesan yang akan disisipkan 5 bit = 11010, maka jumlah byte yang digunakan = 5 byte
10010110 11001001 11111001 10001000 10100011 (byte yang digunakan untuk penyisipan pesan)
Proses penyisipan pesan **11010**hasil penyisipan menjadi **1001011**1 **1100100**1 **1111100**0 **1000100**1 **1010001**0

Jadi metode Least Significant Bit ini hanya menggantikan bit pertama, jika diimplementasikan kedalam rancangan program maka penulis bisa menjelaskan melalui aktivity diagram, guna memberikan gambaran secra jelas mengenai proses enkripsi menggunakan stegnografi,namun pada tahapan ini media yang di gunakan hanya gambar unuk menyembunyikan pesan.



Gambar 5. Aktiviti Diagram Enkripsi

Ketika informasi rahasia tersebut ingin kembali dibuka, maka bit-bit LSB yang sekarang ada, diambil satu per satu kemudian disatukan kembali menjadi sebuah informasi yang utuh seperti semula. Penentuan bit-bit LSB dilakukan secara berurutan, mulai dari byte awal sampai byte terakhir sesuai panjang dari data rahasia yang akan disembunyikan.Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya tidak berpengaruh terhadap persepsi visual/auditori. Bisa dilihat pada **Gambar 1**



Gambar 6. Aktiviti Diagram Deskripsi

Data gambar digunakan sebagai media penutup dalam metode yang sebelumnya.

Gambar 7. Hasil Enkripsi

Pada usulan kali ini penulis mencoba memberikan didefinisikan pesan rahasia dengan *Quick Response Code*. kode berbagai jenis data input (numerik, alfanumerik dan biner). Dalam metode yang diusulkan, kode QR dapat dikompresi dengan gambar yang dihasilakan oleh enkripsi stegnografi menggunakan Least Significant Bit (LSB) karena ukuran yang berbeda dari modul.Ukuran yang lebih tinggi dari modul ini penting agar *Quick Response Code*. dapat dibaca dari jarak yang lebih tinggi. Di sisi lain, ada beberapa bit berlebihan dalam setiap modul yang dapat secara efektif dikurangi tanpa kehilangan informasi sebelum pesan rahasia dalam bentuk gambar stego oleh algoritma ekstraksi metode steganografi masih memiliki bebrapa kekurangan jika gambar yang sudah dienkripsi, namun dimodifikasi maka pesan yang ada di dalamnya akan hialng atau rusak, sehingga pada tahap ini penulis memberikan usuan untuk menambahkan keamanan dari hasil ekstraksi steganografi. *Quick Response Code*, dapat menjadi kaeaman kedua dari hasil enkripsi steganografi diperoleh dari yang diusulkan Akhirnya, diperoleh QR code dapat dibaca oleh perangkat imaging (yaitu smartphone), di mana pesan rahasia dalam teks atau data formulir diperoleh.

Metode yang diusulkan *Quick Response Code* menjadi keamanan tambahan dan mudah digunakan, bisa menggunakan *Quick Response Code generator*, dan dapat mencari *Library* jika ingin membuat aplikasi secara pribadi atau tim dan dapat di gunakan sebagai bukti dari hasil teransaksi, Jumlah karakter dikodekan dengan *Quick Response Code generator* tergantung tidak hanya pada versi *Quick Response Code generator*, tetapi juga pada jenis data. Kapasitas penyimpanan maksimum untuk jenis data yang berbeda dan untuk tingkat tertinggi *Quick Response Code generator*

Gambar 8. Enkripsi Usulan

Keuntungan menggunakan *Quick Response Code* gambar yang sudah di enkripsi aman dari manipulasi yang menyebabkan pesan yang terdapat di dalam gambar tidak terbaca atau bahkan rusak, proses deskripsi pada bagian ini membutuhkan beberapa tahap

Gambar 9. Dekripsi

1. Deskrispi dari *Quick Response Code* kedalam bentuk gambar.(bias menggunakan aplikasi yang di *smartphone*)
2. Setelah bentuk gambar yang di deskripsikan oleh *Quick Response Code* berhasil
3. Deskripsi gambar kedalam bentuk aslinya sehingga diketahui isi pesan yang terdapat di dalamnya

4. KESIMPULAN

Dari pembahasan yang penulis kemukakan masih jauh dari kata sempurna namun penulis berusaha untuk memberikan yang paling baik dari penelitian yang di lakukan kali ini, stegnografi merupakan pesan rahasia atau penyembunyian pesan ddalam sebuah media digital berpa video,audio,gambar,dokumen dll, penulis memberikan keamanan yang lebih perima menambahkan double *enkripsi* dan deskripsi pada pembahasan ini yaitu hasil dari enkripsi stegnografi menggunakan gambar kembali di enkripsi kedalam bentuk *Quick Response Code*,sehingga pesan tidak mudah di rusak dan di pecahkan.

REFERENCES

[1] Vladimír Hajduk1, Martin Broda1, Ondrej Ková 2, Dušan Levický1, “Image steganography with using QR code and cryptography,” IEEE Vol 4:1 : Slovak Republic., 2016.
[2] Anita Rahmawati, Arif Rahman, " Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64," JUSI , vol. 9: 1, no. september, 2011.
[3] Pricilia Yulianingsih, Hamdani, Septya Maharani, " APLIKASI CHATTING RAHASIA MENGGUNAKAN ALGORITMA VIGENERE CIPHER," JUSI , vol. 9: 1, no. september, 2011.
[4] Muhamad Prof.Hamka, " Penyembunyian Informasi (steganography) Gambar Menggunakan Metode LSB(Least Significant Bit)," Rekayasa Teknologi , vol. 5: 1, no. 2013.
[5] Syaiful Anwar, " Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES," Rekayasa Teknologi , vol. 5: 1, no. 2013.
[6] Za’Imatun Niswati, " stegnografi menggunakan Least Significant Bit untuk menyispkan gambar kedalam citra gambar," faktor extra , vol. 5: 2, no. 2013.
[7] Rahmat nur ibrohim,ilham ms, " perancangan stegnografi dengan metode lbs dan algoritma RAS berbasis web ,”jurnal computech & bisnis , vol. 11: 1, no.desember, 2017.
[8] imamah, " enkripsi data menggunakan stegnografi untuk keamanan data pada cloud ,”jurnal computech & bisnis , vol. 11: 1, no.desember, 2017.
[9] Mesran, M. (2012). APLIKASI PENGAMANAN DATA TEKS PADA CITRA BITMAP DENGAN MENERAPKAN METODE LEAST SIGNIFICANT BIT (LSB). *Pelita Informatika: Informasi Dan Informatika*, *2*(1). Retrieved from http://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/111/80
[10] Shinta puspita sari, winarno, dodick z sudirman, " Implementasi menggunakan metode Least Significant Bit dan kriptografi advenced encription standard ,”ultimatices , vol. IV: 1, no.juni, 2012.