ANALISIS KEKUATAN DAN DAYA TAMPUNG PESAN OPTIMAL PADA CITRA STEGANOGRAFI METODE STEGO N BIT LSB DENGAN PENGURUTAN GRADASI WARNA

David Samuel – NIM: 13506081

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16081@students.itb.ac.id

Abstrak

Steganografi merupakan salah satu cara untuk saling bertukar pesan dengan cara menyembunyikan pesan tersebut di dalam sebuah media perantara. Menyembunyikan pesan sedemikian rupa di dalam sebuah media perantara memungkinkan seseorang untuk dapat berkirim pesan dengan orang yang dituju tanpa harus dicurigai jika dilihat oleh seseorang yang tidak berkepentingan. Salah satu media perantara yang dapat digunakan dalam steganorafi adalah citra.

Menyembunyikan pesan di dalam sebuah citra adalah salah satu metode yang sering digunakan dalam steganografi. Ada bermacam-macam metode yang dapat digunakan dalam steganografi menggunakan media perantara citra. Pada kondisi ideal, citra yang telah disisipi oleh pesan harus memiliki tekstur dan terlihat serupa dengan citra awal sebelum disisipi pesan. Akan tetapi, dengan pengamatan detail dan perbandingan dalam tingkat bit, akan terlihat adanya perbedaan antara citra awal dan citra yang telah disisipi oleh pesan. Selain itu, setiap citra juga memiliki daya tampung optimal terhadap pesan yang akan disisipkan. Semakin banyak pesan yang disisipkan dalam sebuah citra, maka citra hasil steganografi akan tampak jauh berbeda dari citra awal, dan dengan mudahnya seseorang yang tidak berkepentingan melakukan steganalisis untuk melakukan serangan terhadap citra yang telah disisipi oleh pesan rahasia.

Makalah ini akan memaparkan analisis hasil percobaan yang telah dilakukan oleh penulis mengenai kekuatan, kelemahan dan daya tampung pesan ideal dalam sebuah citra hasil steganografi dengan menggunakan metoda *STEGO N BIT*. Metode *STEGO N BIT* merupakan metode dasar yang sudah umum digunakan dan dikenal luas dalam steganografi. Analisis terhadap masing-masing jenis metode *STEGO N BIT* akan dilakukan dengan mempergunakan analisis perbandingan gradasi warna (*pallete*) citra awal dan citra hasil steganografi, dan inspeksi visual terhadap citra yang dihasilkan.

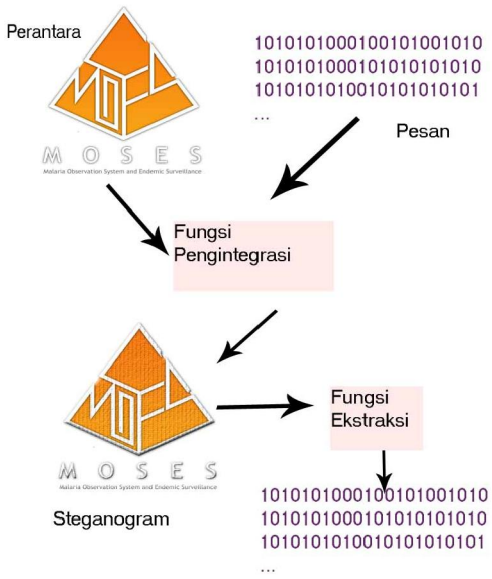
***Kata kunci**: STEGO N BIT, Palette, Visual Inspection, Stego Image, Greyscale,* steganogram, Steganalisis

1. Pendahuluan

Steganografi berasal dari kata “steganos” dan “graphia”, memiliki arti “Terselubung atau tulisan tersembunyi”. Tujuan dari steganografi adalah mengirim pesan kepada seseorang. Seiring dengan kemajuan teknologi, di mana pertukaran data menjadi semakin dinamis, maka diperlukan sebuah cara agar dapat mengirimkan data, namun sulit bahkan tidak dapat diartikan kecuali oleh orang yang dituju.

Steganografi berbeda dengan kriptografi, namun keduanya dipakai untuk dapat saling melengkapi, di mana pesan dalam kriptografi dapat dilihat oleh orang lain, namun dalam bentuk yang telah terenkripsi.

Salah satu perantara yang sering digunakan dalam pengiriman pesan adalah dengan menumpangkannya kepada sebuah citra. Ada banyak teknik dan metode dalam menumpangkan sebuah pesan kepada citra. Namun yang paling umum digunakan adalah metode STEGO N BIT, di mana metode ini memanipulasi informasi warna dari pixel-pixel yang menyusun sebuah citra.



Gambar 1 Skema Umum Proses Integrasi dan Ekstraksi pesan pada steganografi

2. Batasan Masalah

Citra yang digunakan dalam percobaan adalah citra, baik dengan informasi warna RGB, dan juga citra *greyscale* berekstensi .GIF. Penentuan gradasi warna yang akan membantu dalam proses analisis akan dilakukan dengan menggunakan bantuan perangkat lunak yang penulis kembangkan, serta menggunakan bantuan perangkat lunak pemroses citra lain, yaitu *Hide and Seek,* dan *S-Tools.*

Alasan penggunaan citra berekstensi .GIF adalah sifat *lossless compression,* yang memungkinkan reproduksi citra yang tepat sama, sehingga informasi dari susunan bit dalam citra tersebut tepat sama dan dapat dijaga. Selain itu, jumlah maksimal warna yang dapat ditampung adalah 256. Dengan demikian, diperlukan adanya reduksi jumlah warna pada gradasi, agar dapat menampung perubahan gradasi warna citra-stego. Perubahan signifikan dalam gradasi warna citra akan menunjukkan indikasi adanya pesan yang disembunyikan di dalam LSB dari pixel yang ada pada sebuah citra.

3. Metode STEGO N BIT

Metode *STEGO N BIT* menggunakan informasi RGB tiap pixel yang ada pada sebuah citra dalam menyembunyikan pesan rahasia. Pesan rahasia tersebut akan disisipkan pada LSB (*Least Significant Bit*) dari informasi salah satu warna RGB pada pixel sebuah citra. Penggantian LSB dari sebuah informasi warna hanya akan membuat pergantian hasil nilai integer dengan sebanyak satu, sehingga citra hasil penerapan *STEGO N BIT* tidak akan berbeda jauh dari citra hasilnya. Dampak yang dihasilkan sulit ditangkap oleh indra penglihatan manusia.

Nilai N pada *STEGO N BIT* menyatakan jumlah bit yang akan diganti dengan informasi pesan rahasia. Contohnya metode *STEGO ONE BIT* akan mengganti LSB nilai RGB dengan pesan rahasia sebanyak satu bit. Pada contoh kasus sebuah citra 24 bit (Red = 8 bit, Green = 8 bit, Blue = 8 bit), jika menggunakan metode *STEGO ONE BIT*, maka setiap pixel pada citra dapat menyimpan 3 bit informasi. Penggantian LSB dengan bit informasi akan mengakibatkan adanya penambahan jumlah warna pada gradasi warna (*pallete*).

3.1 Daya Tampung Citra Dengan STEGO N-BIT

Apabila kita mengambil asumsi contoh kasus akan menyembunyikan sebuah pesan informasi Sebesar 1000 bit dalam sebuah citra 24 bit, dengan menggunakan metode *STEGO ONE BIT*, maka dibutuhkan setidaknya 334 pixel, atau jika dikonversi ke dalam bentuk bit, maka akan diperlukan sebuah citra berukuran 334 X 3 X 8 = 8016 bit (8X lipat) dari ukuran pesan yang akan ditampung oleh sebuah citra.

4. Metode Pengurutan Gradasi Warna

Sebuah citra yang berkestensi GIF hanya dapat memiliki pembatasan informasi warna sebanyak 256 buah, hal ini akan berpengaruh pada gradasi warna yang akan didapat dari sebuah citra.

Pada percobaan dengan menggunakan citra *Greyscale,* pembatasan jumlah warna sejumlah 256 bit tidak akan memberikan pengaruh yang cukup berarti, karena informasi gradasi warna yang tidak terlalu signifikan. Akan tetapi, pada citra berwarna, maka pembatasan ini mengharuskan citra dengan informasi jumlah warna yang melebihi jumlah batas maksimum akan dipetakan mendekati sebuah warna yang mendekati warna dari citra tersebut.

Apabila menggunakan contoh kasus di atas, maka sebuah citra berwarna yang akan diproses

dengan metode *STEGO ONE BIT* harus memiliki informasi gradasi warna sebesar 128 pixel atau kurang. Sehingga dapat menampung gradasi perubahan warna secara baik. Warna gradasi dari citra awal dan citra-stego akan diurutkan dan dibandingkan untuk menentukan kekuatan kelemahan, serta daya tampung pesan optimal dari metode *STEGO N BIT* dengan nilai n berbeda. Penggunaan *STEGO N BIT* dengan n>1 akan memperbesar daya tampung pesan, namun hal tersebut akan berpengaruh kepada perbedaan citra awal dan citra-stego yang dapat ditangkap oleh indra penglihatan manusia.

Dinamika pemilihan besar n, dan tingkat keterlihatan dengan indra penglihatan manusia akan menjadi variabel yang akan menentukan baik tidaknya sebuah metode steganografi digunakan.

5. Contoh Kasus Steganografi STEGO ONE BIT

Pada analisis ini akan digunakan sebuah pesan berupa berkas HTML yang akan disisipkan dalam sebuah citra GIF. Proses penyisipan menggunakan bantuan kakas S-Tools, dan pada tabel berikut disajikan informasi karakteristik dari berkas dan citra yang digunakan:

Nama file: map.html
Ukuran: 6089 karakter (5,97 KB)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
    <title></title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">

    <script type="text/javascript" src="http://dev.virtualearth.net/mapcontrol/mapcontrol.ashx?v=6.2"></script>

    <script type="text/javascript">
      var map = null;

      var LA = new VELatLong(34.0140, -118.2370);

      var pinToArt = null;
      var pinPixel = null;

      function GetMap()
      {
        map = new VEMap('myMap');
        map.LoadMap(LA, 14, VEMapStyle.Road, false, VEMapMode.Mode2D, true, 1);

        AddPin();
      }

      function getInfo()
      {
```

Gambar 2 Sekilas isi berkas map.html

Citra: Shinta.GIF
Ukuran: 50,7 KB

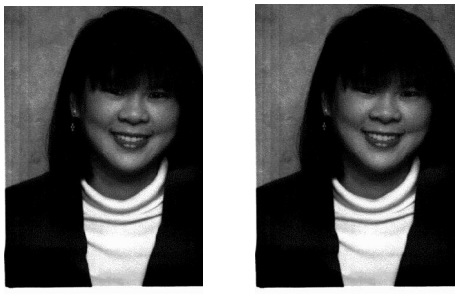
Gambar 3 Berkas Shinta.GIF

Alasan penggunaan berkas dan citra tersebut adalah ukuran dari berkas map.html yang akan disisipkan ke dalam citra Shinta.GIF berukuran hampir 1/8 dari ukuran Shinta.GIF, yaitu daya tampung maksimum dari citra Shinta.GIF, sehingga akan memudahkan tahap analisis, mengingat perbandingan gradasi warna yang akan diperbandingkan.

Pada uji kasus pertama akan dilakukan dengan menggunakan citra *Grey Scale* Shinta.GIF, dan pada uji kasus kedua akan dilakukan dengan menggunakan citra warna Shinta.GIF. Untuk masing-masing uji, digunakan proses perbandingan pengurutan gradien warna yang dihasilkan, serta inspeksi secara visual.

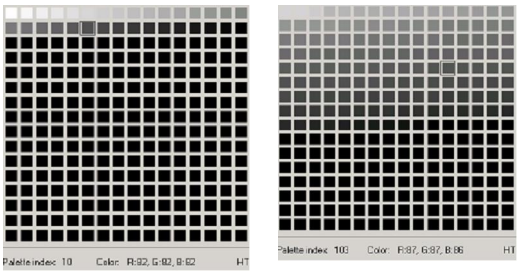
5.1 Analisis Hasil Citra Steganografi dengan mode Grey Scale

Berikut adalah citra yang didapat dengan menggunakan metode STEGO ONE BIT setelah dilakukan penyisipan pesan:



Gambar 4 Citra Awal dan Steganogram

Tampak tidak ada perubahan berarti yang dapat dilihat pada citra hasil awal dan citra hasil steganografi. Namun, apabila kita melakukan ekstraksi warna-warna yang terdapat pada citra awal dan steganogram, akan terlihat terjadi perubahan gradien warna, yang disebabkan oleh adanya penyisipan pesan yang dilakukan.



Gambar 5 *Pallete* Hasil Ekstraksi

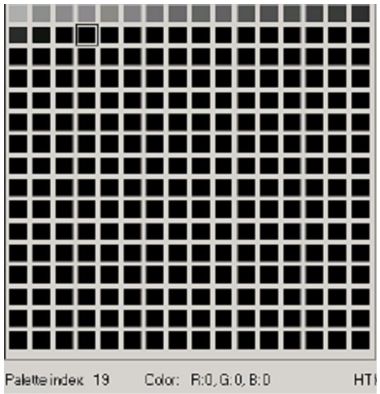
Pada *Pallete* yang telah diurutkan yang diekstraksi dari citra, tampak dengan jelas bahwa Steganogram membentuk warna gradien baru yang lebih halus dibandingkan dengan citra awal. Citra awal diharuskan hanya menggunakan warna maksimal sejumlah 128 warna, sehingga penambahan warna baru memungkinkan untuk diinspeksi visual dengan menggunakan metode gradasi warna.

Warna pada *pallete* index ke-25, nilai R,G, dan B berturut adalah 87,87,86. Perubahan pada nilai *blue* ini dikarenakan adanya bit pesan yang disisipkan pada masing-masing pixel.

Pada uji pertama ini, juga digunakan metode STEGO TWO BITS, yang dapat menghasilkan rentang perubahan nilai *blue* antara 0 sampai 3, dan juga metode metode STEGO THREE BITS yang menghasilkan perubahan nilai *blue* antara 0 sampai 7.

5.2.1 Penambahan Jumlah Pesan Mendekati Daya Tampung Maksimal Citra

Pada sub uji coba dengan menggunakan citra *grey scale* ini, juga dicobakan apabila digunakan berkas yang sama, namun ditambahkan dengan sejumlah karakter sehingga masih bisa diterima oleh citra, sampai mendekati kapasitas maksimum yang dapat diterima oleh citra Shinta.GIF, setelah dilakukan ekstraksi *pallete* warna, didapatkan hasil seperti berikut ini:



Gambar 6 *Pallete* hasil eksktraksi dengan berkas pesan mendekati daya tampung maksimal citra

Hasil yang didapat adalah dengan jumlah pesan mendekati daya tampung maksimal citra, maka hasil ekstraksi *pallete* menunjukkan kemiripan yang lebih besar dengan hasil ekstraksi *pallete* pada citra awal.

Hal ini dapat disebabkan perubahan yang terjadi pada seluruh elemen *pallete* mengakibatkan warna-warna yang menjadi elemen penyusun steganogram hampri menyerupai susunan *pallete* warna yang dibentuk oleh citra awal.

5.2.2 Inspeksi Visual Pada Citra Hasil Perbesaran

Dengan menggunakan perbesaran 15x, dan inspeksi dengan mata, tanpa bantuan apapun, maka hasil perbesaran citra pada lokasi paling kiri atas menghasilkan citra berikut ini:

Gambar 7 Hasil Perbesaran Citra Awal dan Steganogram 15x

Pada inspeksi secara visual, hasil yang didapatkan dengan menggunakan metode STEGO ONE BIT tidak tampak adanya perbedaan besar antara citra awal dan steganogram, kecuali pada pixel ke-2 dari kiri atas, yang memberikan sedikit perbedaan warna. Namun secara umum, tidak terdapat perbedaan berarti dari citra awal dan steganogram.

Perbedaan pada inspeksi visual antara citra awal dengan steganogram, dapat mengindikasikan adanya steganografi, yang juga dapat disimpulkan bahwa citra tersebut telah disisipi oleh suatu pesan.

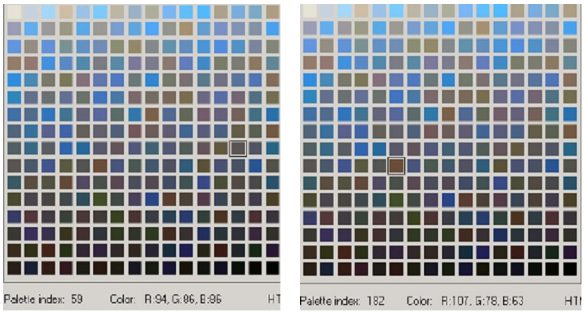
5.2 Analisis Hasil Citra Steganografi dengan mode Berwarna

Pada mode berwarna ini, digunakan berkas yang sama, serta citra yang sama dengan uji yang telah pertama kali dilakukan. Pesan yang akan disisipkan masih menggunakan ukuran yang mendekati ukuran daya tampung maksimal dari citra yang digunakan, dan hasil yang didapat

Bisa dilihat pada gambar berikut

Gambar 8 *Citra Awal dan Steganogram*

Didapatkan citra awal dan steganogram memiliki karakteristik yang hampir sama persis. Apabila digunakan teknik Ekstraksi Gradasi Warna, maka didapatkan ekstraksi gradasi warna seperti berikut ini:



Gambar 9 *Pallete* Hasil Ekstraksi

Pada citra berwarna, didapatkan hasil bahwa setelah dilakukan penurutan warna berdasarkan gradasi, terlihat adanya perubahan variasi warna, yang diakibatkan perubahan LSB pada setiap pixel warna yang telah disisipi pesan.

Pada analisis lebih mendalam, tampak pada gradasi warna biru urutan R,G,B berikut ini :

192, 220, 206 192, 220, 201
192, 220, 203 192, 220, 199
192, 220, 202 192, 220, 198

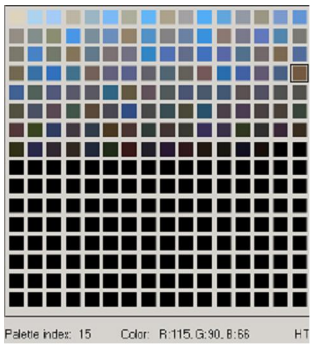
192, 220, 196
192, 220, 194
192, 220, 192

Pada urutan tersebut, tampak pada LSB, terjadi perubahan nilai *Blue* yang tidak merata, dan menimbulkan gradasi warna baru yang sebelumnya tidak ada.

Perubahan gradasi warna menjadi lebih halus dibandingkan dengan citra awal pada mode berwarna ini dapat menjadi sebuah indikasi bahwa telah terjadi sebuah penyisipan pesan pada citra.

5.2.1 Penambahan Jumlah Pesan Mendekati Daya Tampung Maksimal Citra

Pada sub uji coba kedua, dipergunakan skenario yang sama, yaitu pesan yang disisipkan ditambah sehingga mendekati daya tampung maksimal citra. Setelah dilakukan ekstraksi *pallete* warna, maka didapatkan *pallete* sebagai berikut:



Gambar 10 *Pallete* hasil eksktraksi dengan berkas pesan mendekati daya tampung maksimal citra

Sedangkan dalam penggunaan STEGO 2 BIT, semakin didapat jumlah gradasi warna yang semakin besar, begitu pula dengan STEGO 3 BIT. Hal ini disebabkan semakin banyak pesan yang harus ditampung pada sebuah pixel, sehingga menjadikan perubahan warna menjadi lebih banyak.

Steganografi dengan menggunakan mode berwarna memberikan sebuah keuntungan tersendiri. Hal ini dikarenakan pada mode berwarna, nilai R,G,dan B dapat bervariasi, sehingga menyulitkan steganalis untuk dapat mengetahui adanya indikasi pesan yang disisipkan pada sebuah citra.

Hal yang bertolak belakang didapatkan ketika citra yang digunakan adalah citra *grey scale*. Warna abu-abu selalu diindikasikan dengan komposisi warna R, G, dan B yang selalu sama.

Namun pada steganografi, dikarenakan adanya penyisipan pesan yang dapat mengubah salah satu komposisi warna, maka hal ini menyebabkan adanya perubahan LSB, yang

mengakibatkan komposisi warna menjadi tidak seimbang lagi, walaupun secara inspeksi visual biasa, hal tersebut akan sangat sulit diidentifikasi oleh seseorang.

Contoh pada uji kasus pertama, nilai R, G dan B untuk sebuah warna pada indeks ke-25 adalah 87,87, 86. Perubahan sebesar 1 bit pada LSB ini akan tampak pada metode pengurutan gradasi warna, dan dapat menjadi sebuah indikasi bahwa terdapat citra tersebut telah disisipi pesan rahasia.

6. Kesimpulan

Perubahan gradasi warna pada inspeksi visual pada area tertentu dari citra awal dan steganogram pada umumnya tidak dapat dibedakan. Namun apabila citra awal dan steganogram diletakkan bersebelahan dan dilakukan inspeksi secara seksama, maka ada sedikit perbedaan yang dapat diketahui, Terutama apabila semakin banyak bit yang digunakan dalam sebuah pixel untuk menyimpan pesan, semakin mudah diketahui pula ada pesan yang tersembunyi dalam citra tersebut

Berikut beberapa metode STEGO N BIT dan beberapa karakteristik yang menjadi ciri masing-masing dari sisi pengurutan gradasi *pallete* warna.

		Stego 1 Bit	Stego 2 Bit	Stego 3 Bit
Analisis Pola Gradasi *Pallete*	Tidak dapat dipecahkan			
	Sulit dipecahkan			
	Mudah dipecahkan	x	x	x
Inspeksi Visual	Tidak dapat dipecahkan			
	Sulit Dipecahkan	x	x	
	Mudah dipecahkan			x

Daftar Pusaka

[1] Curran, Kevin. (2003). An Evaluation of Image Based Steganography Methods.University of Ulster, Ireland.

[2] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[3] Peter, Wayner. (2002). Disappearing Cryptography, Information Hiding: Steganography and Watermarking, 2nd Edition, Morgan Kaufmann.