Pemanfaatan *Second Least Significant Bit* dan Kunci Dua Kata Untuk Mencegah Serangan *Enhanced LSB* Pada Citra Digital

Achmad Dimas Noorcahyo - 13508076
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18076@students.if.itb.ac.id

***Abstract*—Dalam steganografi ranah spasial, metode *Least Significant Bit* (LSB) adalah metode yang umum digunakan. Karena tekniknya yang sederhana, metode LSB memiliki kekuatan yang rendah. Metode steganalisis yang sering digunakan untuk menemukan pesan tersembunyi dalam gambar menggunakan LSB adalah Metode *Enhanced LSB*. Teknik serangannya adalah dengan mengganti semua bit dari komponen warna citra megikuti nilai bit paling kanan citra tersebut. Pada makalah ini, penulis akan memodifikasi metode steganografi LSB berdasarkan ide bahwa penyisipan bit pesan tidak selalu mengubah LSB. Jika bit pesan bernilai sama dengan nilai LSB saat ini, maka tidak terjadi perubahan LSB. Perbedaan baru terjadi apabila nilai LSB saat ini dan bit pesan yang akan disisipkan berbeda. Teknik yang digunakan pada makalah ini adalah menempatkan bit pesan pada *Second Least Significant Bit* yaitu bit kedua paling kanan saat bit pesan berbeda dengan bit terakhir LSB . Jika nilai LSB dan bit pesan bernilai sama tidak dilakukan aksi apapun. Untuk mengingat pada langkah berapa bit pesan ditulis pada *Second Least Significant Bit* maka dilakukan pencatatan semua nomor langkah saat penyisipan *Second* LSB dilakukan. Setelah pesan disisipkan, nomor-nomor ini juga disisipkan ke dalam gambar. Kunci *seed* untuk menyimpan nomor penyisipan *Second* LSB dibuat berbeda dengan kunci untuk menyimpan pesan sehingga jumlah kata untuk kunci harus berjumlah dua buah. Pada makalah ini juga akan dicantumkan hasil-hasil pengujian steganalisis *Enhanced* LSB terhadap citra hasil metode LSB biasa dan juga terhadap citra hasil metode LSB modifikasi. Hasil keduanya akan dibandingkan untuk menguji performansi dari metode LSB dengan memanfaatkan *Second* LSB ini. Hasil eksperimen menunjukkan bahwa penyisipan citra dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata terbukti tak terpengaruh terhadap serangan *Enhanced* LSB.**

***Index Terms*—Metode LSB, Serangan *Enhanced* LSB, Modifikasi Metode LSB, *Second Least Significant Bit*.**

I. PENDAHULUAN

Steganografi merupakan teknik dan suatu seni penyembunyian pesan di dalam pesan lainnya [4]. Pada umumnya tujuan steganografi adalah memastikan tidak ada kecurigaan dalam penyampaian pesan [1]. Pada steganografi, pesan dapat disembunyikan dalam berbagai bentuk. Namun, di dalam era digital saat ini, steganografi dilakukan menggunakan komputer digital dan pesan serta media penyimpanan steganografi yang dgunakan berupa file-file digital seperti gambar digital, dokumen, file audio, bahkan file video.

Bentuk steganografi yang banyak digunakan adalah steganografi dalam citra digital. Penyisipan dilakukan dengan memanfaatkan bit gambar atau frekuensi gambar [1]. Teknik pemanfaatan bit gambar yang sederhana adalah Metode *Least Significant Bit* yaitu metode penyisipan pesan di dalam bit terakhir gambar. Namun, pemakaian metode steganografi dalam citra perlu dipertimbangkan dengan baik. Pasalnya seiring dengan berkembangnya steganografi, teknik-teknik steganalisis untuk mendeteksi adanya pesan dalam gambar juga berkembang tak kalah pesat.

Metode LSB merupakan metode steganografi yang termudah. Meskipun begitu, metode LSB dikenal sebagai metode yang tidak memiliki kekuatan tinggi [4]. Pendeteksian pesan dalam gambar dapat dideteksi dengan menggunakan serangan-serangan steganalisis visual [4]. Salah satu serangan terkenal yang dapat mengungkap pesan penyisipan dengan LSB adalah serangan *Enhanced* LSB. *Enhanced* LSB bekerja dengan mengubah bit- bit warna mengikuti bit terakhir yang kemungkinan sudah disisipi bit pesan. Jika terdapat pesan maka dapat terlihat dengan jelas kerusakan pada gambar [2].

Karena mudah terkena serangan *Enhanced* LSB, metode LSB rawan digunakan untuk menyisipkan pesan-pesan yang penting. Hal ini sangat disayangkan mengingat kemudahan yang dipunyai oleh metode LSB. Dalam makalah ini, penulis akan memodifikasi metode LSB sehingga tidak terpengaruh terhadap serangan *Enhanced* LSB. Dengan prinsip-prinsip penyisipan bit yang sama namun sedikit penanganan khusus dan penambahan data, maka teknik yang ditawarkan ini akan membuat gambar yang disisipi pesan menggunakan LSB menjadi kuat namun tetap mempertahankan ciri kemudahannya.

II. METODE *LEAST SIGNIFICANT BIT*

Metode *Least Significant Bit* merupakan metode

steganografi dalam ranah spasial yang paling mudah [4]. Metode LSB memanfaatkan keterbatasan visual pada indera mata manusia yang kurang peka terhadap sedikit perubahan warna [1].

Cara yang digunakan adalah menggantikan bit paling tidak signifikan (*Least Significant Bit*) dari gambar dengan bit pesan. Bit yang paling tidak signifikan dari gambar adalah bit warna yang terletak di paling kanan. Jika bit warna paling kanan diubah, maka perbedaan nilai byte dari warna tersebut hanya berkurang atau bertambah satu. Perubahan ini tidak mampu dideteksi dengan indera penglihatan manusia [1].

Teknik penggantian bit pada metode LSB seperti berikut :

Misalkan byte-byte warna pada gambar

10111010 11101011 11011011 10101010

dan bit pesan yang akan disisipkan 1011

Maka, hasil penyisipan pada bit *LSB* gambar tersebut menghasilkan bit-bit gambar baru :

10111011 11101010 11011011 10101011

Biasanya penyisipan bit-bit data dilakukan pada urutan byte gambar yang acak. Bilangan urutan dibangkitkan secara acak menggunakan pembangkit bilangan acak-semu (*PRNG*: *pseudo-random number generator*). Pada pembangkit bilangan ini diperlukan nilai awal sebagai umpan (*seed*) agar penerima dapat membangkitkan kembali deretan bilangan acak yang sama menggunakan umpan tersebut. Nilai umpan berasal dari kunci yang berupa kata. Dari kata tersebut dibuat suatu bilangan bulat dengan cara yang diinginkan. Cara yang mudah yaitu dengan menghitung penjumlahan nilai integer dari semua huruf yang ada [1].

III. Serangan *Enhanced* LSB

Metode LSB merupakan metode steganografi yang lemah dan mudah dikenakan teknik-teknik steganalisis tertentu [4]. Karena teknik LSB menggunakan prinsip pengubahan bit sederhana, maka serangan steganalisis secara visual dapat langsung mendeteksi kebaradaan pesan dalam gambar. Serangan steganalisis visual sendiri adalah metode subjektif melibatkan indera penglihatan manusia untuk mengamati bagian gambar yang dicurigai [3]. Salah satu serangan visual yang terkenal dapat mendeteksi pesan yang disembunyikan dengan metode LSB dengan baik adalah serangan *Enhanced* LSB [2].

Serangan *Enhanced* LSB adalah sebuah algoritma pengecekan keberadaan pesan di dalam gambar dengan cara mengubah semua bit dalam satu kompunen warna menjadi nilai yang sama 1 atau 0 mengikuti nilai bit paling kanan (*Least Significant Bit*) dari komponen warna tersebut [2].

Enhanced LSB dilakukan pada tiga komponen warna RGB yaitu *Red*, *Green*, dan *Blue*. Setiap komponen warna direpresentasikan oleh satu byte. Setiap byte komponen warna ini memiliki masing-masing satu buah bit *LSB*.

Apabila bit *LSB* pada komponen warna tersebut adalah 1, maka semua bit pada byte tersebut diganti dengan bit 1 sehingga nilai byte tersebut adalah 11111111 atau 255 dalam desimal. Sedangkan, apabila bit *LSB* tersebut adalah 0, maka semua bit pada byte tersebut diganti dengan bit 0 sehingga nilai byte tersebut adalah 00000000 atau 0 dalam desimal.

Misalnya terdapat sebuah *pixel* dengan komposisi byte sebagai berikut :

Red 11001011
Green 10110110
Blue 11101001

Maka setelah mengalami *Enhanced LSB* byte-byte diatas akan menjadi :

Red **11111111**
Green **00000000**
Blue **11111111**

Setelah melalui proses ini, maka dapat terlihat pada citra hasil bahwa bagian gambar yang tidak disisipi pesan akan mendekati bagian gambar semula. Sedangkan bagian gambar yang mengandung pesan rahasia akan menjadi rusak setelah disaring. Kerusakan ini dapat dideteksi secara visual dengan menggunakan indera penglihatan manusia [2].

Dengan teknik serangan *Enhanced* LSB, metode steganografi dengan pemanfaatan *Least Significant Bit* dapat dengan mudah dianalisis keberadaan pesannya. Maka, dibutuhkan suatu metode lain atau modifikasi untuk menghilangkan pengaruh *Enhanced* LSB pada citra stego.

IV. Teknik Yang Diusulkan : Pemanfaatan *Second* LSB dan Kunci Dua Kata

Untuk melindungi gambar berpesan dari serangan *Enhanced* LSB, pada makalah ini diusulkan teknik baru dengan prinsip penyisipan bit seperti metode LSB biasa namun dengan pengembangan teknik tertentu.

Serangan *Enhanced* LSB pada prinsipnya melakukan pendeteksian pada bit paling kanan dari setiap byte komponen warna pada gambar. Kemudian bit-bit lainnya dimanipulasi mengikuti nilai dari bit paling kanan tersebut. Jika bit paling kanan sudah disisipi pesan sehingga berubah, maka pada hasil citra *Enhanced* LSB terdapat kerusakan pada pixel-pixel yang terubah..

Karena serangan *Enhanced* LSB hanya menyerang bit pertama, maka ide yang muncul untuk menghindari serangan ini adalah memanfaatkan bit-bit lain selain bit LSB untuk menyisipkan pesan. Bit yang paling baik untuk disisipi pesan selain bit *Least Significant Bit* adalah bit *Second Least Significant Bit*. Bit ini adalah bit yang terletak dua dari kanan. Jika bit ini diubah maka nilai warna keseluruhan hanya akan bertambah atau berkurang

sebanyak 3 nilai. Berdasarkan eksperimen penulis, perubahan sebanyak ini juga tidak dapat dideteksi oleh indera penglihatan manusia.

Namun, jika memperhatikan teknik penyisipan pada metode LSB, terdapat peluang untuk membuat cara ini lebih efisien. Pada teknik LSB, penyisipan bit pesan tidak selalu mengubah nilai *Least Significant Bit*.

Jika bit pesan bernilai satu dan nilai LSB saat ini juga satu, maka tidak akan terjadi perubahan LSB. Begitu juga apabila nilai pesan bernilai nol dan nilai LSB saat ini juga nol. Dalam kasus ini, jika nilai pixel dikenakan metode *Enhanced* LSB, maka tidak terjadi kerusakan apapun. Kerusakan baru terjadi apabila terjadi perubahan LSB dari nol ke satu ataupun dari satu ke nol. Yaitu jika nilai LSB saat ini dan bit pesan yang akan disisipkan berbeda.

Dapat disimpulkan dari kedua kasus tersebut bahwa pada metode LSB, perubahan bit dalam suatu pixel baru akan terjadi jika bit LSB dan bit pesan memiliki nilai yang berbeda.

Berdasarkan perilaku tersebut, maka dalam konteks pemanfaatan *Second Least Significant Bit*, jika bit pesan yang akan disisipkan ternyata bernilai sama dengan nilai LSB, bit pesan tersebut tidak perlu diletakkan pada *Second Least Significant Bit*. Pada kasus seperti ini tetap digunakan *Least Significant Bit* untuk penyisipan pesan. Lagipula nilai dari LSB tidak akan berubah jika nilainya sama dengan bit pesan yang disisipkan. Jika bit LSB tidak berubah berarti serangan *Enhanced* LSB tidak akan menghasilkan kerusakan.

Dengan kombinasi penempatan pesan pada LSB dan *Second* LSB berdasarkan kasus kesamaan nilai bit pesan dengan bit LSB, maka tidak akan ada bit yang berubah pada posisi paling kanan sehingga citra tidak mempan terhadap serangan *Enhanced* LSB. Selain itu karena tidak semua nilai *Second* LSB perlu diubah, maka akan diperoleh efisiensi yang cukup baik dan perubahan warna pada gambar dapat diminimalisasi.

Masalah yang harus diperhatikan saat menggunakan teknik modifikasi ini adalah kita harus mengingat pada langkah berapa bit pesan ditulis pada *Second Least Significant Bit* dan pada langkah berapa bit pesan tetap dituliskan pada *Least Significant Bit*. Hal ini penting agar nantinya pesan dapat diekstraksi kembali oleh penerima.

Cara untuk mengingatnya adalah dengan melakukan pemantauan nomor random yang dihasilkan. Jika bit LSB dan bit pesan berbeda (berarti bit pesan harus diletakkan di *Second* LSB), nomor random pada langkah tesebut disimpan dalam suatu tabel. Setelah semua pesan disisipkan, nomor-nomor dalam tabel juga disisipkan ke dalam gambar supaya penerima dapat mengetahui pada nomor random keberapa harus mengambil bit dari LSB dan pada nomor random keberapa harus mengambil bit dari *Second* LSB. Nomor-nomor ini semuanya disisipkan pada *Second Least Significant Bit* dari gambar.

Proses penyisipan nomor random juga memerlukan *seed* untuk membangkitkan nomor peletakan bit. *Seed* ini berasal dari kunci berupa kata. Karena dibutuhkan dua kunci pada teknik ini, satu untuk penyisipan pesan dan satu untuk penyisipan nomor random lokasi diubahnya *Second* LSB, maka kunci keseluruhan berupa dua buah kata. Kata yang pertama untuk pembangkitan nomor untuk menyisipkan pesan dan kata yang kedua untuk pembangkitan nomor untuk menyisipkan nomor dalam tabel.

Langkah-langkah modifikasi metode LSB dengan pemanfaatan *Second Least Significant Bit* :

```
{Data yang dibutuhkan
 gambar : data gambar
 pesan  : data pesan dalam bentuk array bit
 KunciKata1 : kata pertama
 KunciKata2 : kata kedua
}


{Penyisipan pesan pada gambar menggunakan kata
kunci pertama}

seed := toangka(KunciKata1)
random  := buatrandom(seed)

panjangpesan := getpanjang(pesan)

for  i:=1 to (panjangpesan)

nrandom := bilanganrandomselanjutnya(random)
arraybitwarna := getnomorwarna(gambar) di
posisi pixel nrandom

if  not (arraybitwarna[32] = pesan[i]) then
     arraybitwarna[31] := pesan[i]
     tambah nrandom pada arraynomorint
end if

{Jika arraybitwarna[32] = pesan[i] tak perlu
dilakukan apapun}

gambar := setnomorwarna(arraybitwarna) di
posisi pixel nrandom

end for


{Penyisipan nomor random saat Second LSB
dimodifikasi pada gambar menggunakan kata
kunci kedua}

seed := toangka(KunciKata2)
random  := buatrandom(seed)
arraynomorbit := kebentukbit(arraynomorint)

panjangarrnomor := getpanjang(arraynomorbit)

for  i:=1 to (panjangarrnomor)

nrandom := bilanganrandomselanjutnya(random)
arraybitwarna := getnomorwarna(gambar) di
posisi pixel nrandom

arraybitwarna[31] := arraynomorbit[i]

gambar := setnomorwarna(arraybitwarna) di
posisi pixel nrandom

end for
```

Dengan menggunakan kunci dua kata yang sama, pesan dapat diekstraksi kembali. Penerima akan menggunakan Kata kunci yang kedua terlebih dahulu untuk mendapatkan daftar nomor random tempat *Second Least Significant Bit* diubah. Kemudian baru menggunakan kata

kunci yang pertama untuk mengambil bit-bit pesan dalam gambar. Selama pengambilan bit pesan dilakukan pengecekan apakah nomor random saat ini terdapat dalam daftar. Jika nomor random ada dalam daftar, bit yang diambil adalah *Second Least Significant Bit*, sedangkan jika nomor random tidak ada dalam daftar, bit yang diambil adalah *Least Significant Bit*.
Langkah-langkah ekstraksi pesan dituliskan sebagai *pseudocode* berikut :

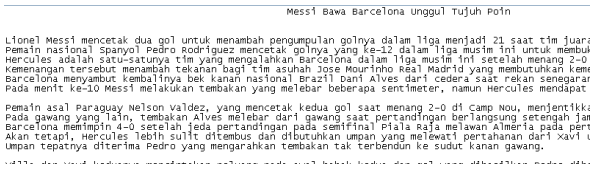
```
{Data yang dibutuhkan
 gambar : data gambar
 KunciKata1 : kata pertama
 KunciKata2 : kata kedua
}


{mengambil daftar nomor random menggunakan
kata kunci kedua}

seed := toangka(KunciKata2)
random  := buatrandom(seed)

repeat

nrandom := bilanganrandomselanjutnya(random)
arraybitwarna := getnomorwarna(gambar) di
posisi pixel nrandom

tambah arraynomorbit dengan arraybitwarna[31]

until (ditemukan bit penanda berhenti)


{mengambil pesan pada gambar menggunakan kata
kunci pertama}

seed := toangka(KunciKata1)
random  := buatrandom(seed)

arraynomorint = tointeger(arraynomorbit)

repeat

nrandom := bilanganrandomselanjutnya(random)
arraybitwarna := getnomorwarna(gambar) di
posisi pixel nrandom

if  (nrandom terdapat pada arraynomorint) then
     tambah hasil dengan arraybitwarna[31]
else
     tambah hasil dengan arraybitwarna[32]
end if

until (ditemukan penenda berhenti)


stringhasil := tostring(hasil)


output(stringhasil)
```

V. EKSPERIMEN DAN HASIL

Pengujian dilakukan menggunakan kakas Visual C# .NET dengan memodifikasi program steganografi metode *Least Significant Bit* biasa yang sudah dibuat sebelumnya oleh penulis. Citra yang digunakan untuk bahan uji adalah citra'bee-2.bmp' yang berukuran 300 x 300 pixel. Citra memiliki kontras yang tinggi antara gambar dengan latar belakangnya yang berwarna putih. Berikut adalah tampilan citra asli yang belum disisipi ataupun dikenakan metode apapun.

Gambar 1. Citra uji asli.

Pesan yang digunakan selama pengujian berupa pesan teks dengan ukuran sedang. Berikut adalah potongan teks yang digunakan :



Messi Bawa Barcelona Unggul Tujuh Poin

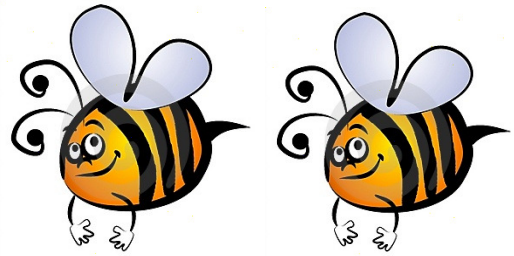
Lionel Messi mencetak dua gol untuk menambah pengumpulan golnya dalam liga menjadi 21 saat tim juara
Pemain nasional Spanyol Pedro Rodriguez mencetak golnya yang ke-12 dalam liga musim ini untuk membuk
Hercules adalah satu-satunya tim yang mengalahkan Barcelona dalam liga musim ini setelah menang 2-0
Kemenangan tersebut menambah tekanan bagi tim asuhan Jose Mourinho Real Madrid yang membutuhkan kem
Barcelona menyambut kembalinya bek kanan nasional Brazil Dani Alves dari cedera saat rekan senegara
Pada menit ke-10 Messi melakukan tembakan yang melebar beberapa sentimeter, namun Hercules mendapat

Pemain asal Paraguay Nelson Valdez, yang mencetak kedua gol saat menang 2-0 di Camp Nou, menjentikk
Pada gawang yang lain, tembakan Alves melebar dari gawang saat pertandingan berlangsung setengah ja
Barcelona memimpin 4-0 setelah jeda pertandingan pada semifinal Piala Raja melawan Almeria pada pert
Akan tetapi, Hercules lebih sulit ditembus dan dibutuhkan umpan yang melewati pertahanan dari Xavi
Umpan tepatnya diterima Pedro yang mengarahkan tembakan tak terbendung ke sudut kanan gawang.

Eksperimen 1 : Uji Imperceptibility

Eksperimen pertama dilakukan untuk melihat *Imperceptibility* yakni mutu gambar setelah disisipi pesan baik untuk metode LSB biasa maupun metode LSB yang dimodifikasi. Tujuannya untuk memastikan modifikasi tetap menghasilkan gambar yang tidak dapat dipersepsi perubahannya oleh mata manusia.

Gambar 2a merupakan gambar 'bee' yang sudah disisipi pesan menggunakan metode LSB biasa, sedangkan gambar 2b adalah gambar 'bee' yang disisipi pesan menggunakan metode LSB dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata.



(a) (b)

Gambar 2. (a) Citra uji yang disispi pesan dengan metode LSB biasa. (b) Citra uji yang disisipi pesan dengan metode LSB dengan pemanfaatan *Second* LSB dan kunci dua kata.

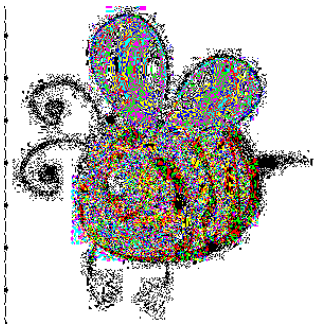
Perbedaan gambar antara gambar stego hasil dari penyisipan pesan menggunakan dua metode tersebut tidak dapat terlihat secara visual. Kedua gambar tersebut sama-sama berhasil menyembunyikan pesan tanpa terdeteksi indera penglihatan manusia.

Eksperimen 2 : Uji Serangan *Enhanced* LSB

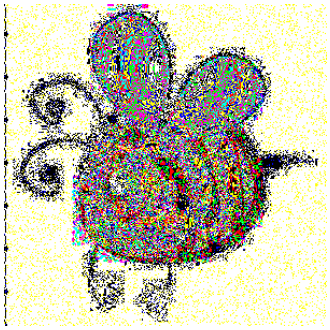
Eksperimen kedua merupakan eksperimen utama untuk mengecek keberhasilan tujuan dari modifikasi metode yang dilakukan. Eksperimen ini dilakukan untuk melihat efek serangan *Enhanced* LSB terhadap citra yang disisipi pesan menggunakan metode LSB termodifikasi. Citra hasil penyisipan menggunakan metode LSB biasa juga akan diuji dengan serangan *Enhanced* LSB. Hasilnya akan dibandingkan dengan citra hasil serangan *Enhanced* LSB pada citra hasil penyisipan metode LSB termodifikasi..

Program *Enhanced* LSB dibuat oleh penulis menggunakan kakas yang sama dengan program penyisipan pesan yaitu Visual C# .NET.

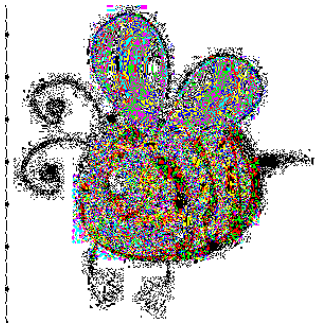
Gambar 3 adalah hasil serangan *Enhanced* LSB terhadap citra awal yang tidak berpesan. Gambar 4 adalah hasil serangan *Enhanced* LSB terhadap citra yang sudah disisipi pesan menggtunakan metode LSB biasa. Sedangkan, gambar 5 adalah hasil serangan *Enhanced* LSB terhadap citra yang sudah disisipi pesan menggunakan metode LSB dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata.



Gambar 3. Hasil serangan *Enhanced* LSB terhadap citra tak berpesan.



Gambar 4. Hasil serangan *Enhanced* LSB terhadap citra yang sudah disisipi pesan dengan metode LSB biasa.



Gambar 5. Hasil serangan *Enhanced* LSB terhadap citra yang sudah disisipi pesan dengan metode LSB dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata.

Gambar 3 merupakan gambar yang tidak disisipi pesan apabila dikenakan serangan *Enhanced* LSB. Meskipun citra hasil berupa bintik-bintik warna dasar seperti hitam, putih, kuning, dan merah namun bentuk citra tetap konsisten dengan citra asli. Latar belakang gambar juga tetap mempertahankan warna putih seperti halnya gambar asli tanpa ada kerusakan. Hal ini menunjukkan bahwa tidak ada pesan tersembunyi di dalam citra.

Gambar 4 memperlihatkan serangan *Enhanced* LSB terhadap citra yang sudah disisipi pesan menggunakan metode *Least Significant Bit*. Pada citra hasil serangan terdapat kerusakan yang tersebar pada seluruh area gambar berupa bintik-bintik berwarna kuning. Hal ini megungkap fakta bahwa terdapat pesan tersembunyi di dalam gambar tersebut.

Gambar 5 memperlihatkan bahwa serangan LSB tidak menyebabkan kerusakan pada citra hasil penyisipan metode LSB dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata. Citra hasil terlihat konsisten dengan citra asli. Citra ini sama persis dengan citra hasil serangan *Enhanced* LSB terhadap citra tak berpesan yang ada di gambar 3. Hal ini dapat mengelabui steganalis yang mengasumsikan bahwa tidak terdapat pesan tersembunyi di dalam citra tersebut.

Hasil eksperimen ini membuktikan bahwa metode LSB yang dimodifikasi bersifat aman terhadap serangan *Enhanced* LSB. Hal ini karena meskipun terdapat pesan yang disisipkan, namun tidak ada satupun LSB yang berubah dengan adanya teknik modifikasi ini.

VI. ANALISIS DAN EVALUASI

Hasil eksperimen menunjukkan bagaimana performansi dari citra yang disisipi pesan menggunakan metode LSB dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata. Gambar 5 menunjukkan bahwa metode ini tidak terpengaruh terhadap serangan *Enhanced* LSB. Keamanan dapat dicapai karena adanya modifikasi pada algoritma yang mencegah nilai bit LSB berubah.

Namun, metode modifikasi *Least Significant Bit* ini menyebabkan peningkatan kompleksitas pemrograman Selain itu struktur data yang digunakan sebagai fasilitator algoritma juga bertambah. Pada metode LSB yang

dimodifikasi, dibutuhkan suatu struktur array untuk menyimpan nomor random saat *Second Least Significant Bit* mengalami perubahan. Penambahan proses berupa penyisipan nomor-nomor random pada gambar pada umumnya akan membuat jumlah komputasi semakin banyak. Secara umum, dapat dikatakan bahwa apabila diinginkan metode steganografi citra yang lebih sederhana dan tidak butuh keamanan tinggi, cukup digunakan metode LSB biasa. Jika dibutuhkan metode steganografi citra yang menuntut keamanan, maka metode modifikasi LSB yang diusulkan pada makalah ini dapat berguna.

Dari segi *imperceptibilitiy* , hasil eksperimen pada gambar 2 menunjukkan bahwa meskipun banyak bit *Second Least Significant Bit* yang diubah, citra yang disisipi pesan menggunakan metode modifikasi LSB tetap tidak bisa dideteksi perubahannya. Jika dibandingkan dengan gambar asli maka tidak dapat terlihat adanya perbedaan oleh indera penglihatan manusia. Hal ini membuktikan bahwa perubahan nilai warna sebesar 3 (jika *Second* LSB berubah) juga masih tidak dapat terdeteksi oleh mata manusia. Algoritma implementasi dari metode modifikasi LSB sebenarnya sudah berusaha meminimalisasi perubahan *Second Least Significant Bit* dengan cara membandingkan nilai bit LSB dan nilai bit pesan yang akan disisip. Apabila nilainya sama, maka pesan tidak disisip pada *Second* LSB melainkan tetap di LSB. Dengan menghitung probabilitas, cara ini seharusnya mampu meminimalisasi perubahan *Second Least Significant Bit* sebesar 50 %.

Meskipun sudah dilakukan minimalisasi dan juga sudah dibuktikan melelui eksperimen untuk memastikan citra tetap *imperceptible* , namun hal yang pasti adalah jumlah perubahan nilai warna pada citra hasil metode LSB yang dimodifikasi pasti lebih besar jika dibandingkan dengan metode LSB biasa. Untuk contoh gambar yang digunakan dalam eksperimen, memang perubahan warna masih tidak dapat dideteksi. Namun, penulis tidak dapat memastikan bahwa untuk semua citra, metode ini tetap mempertahankan sifat *imperceptible* yang dimilikinya.

Berikut ini adalah tabel perbandingan Metode LSB biasa dengan metode LSB menggunakan *Second Least Significant Bit* dan kunci dua kata.

Metode LSB
- Rawan terhadap serangan *Enhanced* LSB - Sederhana dan Mudah - Perubahan nilai warna lebih sedikit
Metode LSB dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata
- Aman terhadap serangan *Enhanced* LSB - Tingkat kesulitan pemrograman lebih tinggi dan membutuhkan tambahan struktur data - Perubahan nilai warna lebih banyak namun tetap *imperceptible*

VII. KESIMPULAN

Di dalam makalah ini telah dipresentasikan teknik pemanfaatan *Second Least Significant Bit* dan kunci dua kata sebagai modifikasi dari metode steganografi *Least Significant Bit*. Teknik yang dilakukan adalah dengan menempatkan bit pesan pada *Second Least Significant Bit* apabila nilainya berbeda dengan nilai bit LSB. Apabila bit pesan dan LSB bernilai sama, bit pesan tetap disisipkan di *Least Significant Bit*. Untuk mengingat posisi tempat *Second* LSB diubah, digunakan kata kunci kedua untuk menyimpan nomor random di dalam gambar. Hasil eksperimen menunjukkan bahwa metode modifikasi dengan pemanfaatan *Second Least Significant Bit* dan kunci dua kata terbukti aman dari serangan *Enhanced* LSB untuk citra uji citra berkontras tinggi. *Enhanced* LSB pada citra hasil menunjukkan konsistensi yang baik dibandingkan dengan gambar asli dan tidak mengalami kerusakan.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Kriptografi*. Penerbit Informatika, 2007.

[2] Anneria Sinaga, Yulie, "Program Steganalisis Metode *LSB* pada Citra dengan *Enhanced LSB,* Uji *Chi-Square,* dan *RS-Analysis*," *Makalah Tugas Akhir Teknik Informatika ITB.*

[3] http://deepaksharma.net/.../**Qualitative**%20**Approaches**%20to%20**Steganalysis**.doc/
Tanggal Akses : 1 Maret 2011, 17. 34 WIB

[4] http://kleiman**math**.awardspace.com/lectures/StegoTalk%20112707.ppt/
Tanggal Akses : 1 Maret 2011, 18. 11 WIB

[5] http://www1.chapman.edu/~nabav100/.../**ImageSteganography**.pdf/
Tanggal Akses : 1 Maret 2011, 19. 32 WIB

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23Maret 2011

ttd

Achmad Dimas Noorcahyo
NIM : 13508076