STEGANOGRAFI GANDA
DENGAN MANIPULASI GAMBAR

Garibaldy W Mukti – NIM : 13506004

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : subghost1802000@yahoo.com

Abstrak

Makalah ini membahas tentang penerapan steganografi pada gambar inversi, yaitu penyisipan suatu data rahasia dalam sebuah gambar yang hanya bisa di ekstraksi melalui inversi gambar tersebut. Steganografi ini secara umum merupakan suatu ilmu penyembunyian informasi dengan cara menyisipkan informasi tersebut dalam sebuah media lain, contohnya gambar.

Media gambar ini dapat dimanipulasi dengan berbagai macam cara, misalnya diinversi, yaitu mengganti bit-bit warna tiap pixelnya dengan kebalikan dari warna yang aslinya. Misalnya yang awalnya hitam diubah menjadi warna putih. Selain itu bisa juga gambar tersebut ditransposisi pixel-pixelnya. Manupulasi seperti ini dilakukan untuk menyiapkan media penyimpanan data. Hal ini ditujukan agar penyisipan data tersebut bisa lebih aman.

Dalam makalah ini juga akan dibahas mengenai bagaimana proses penyisipan data tersebut secara mendetail, mulai dari penyiapan gambar normal hingga data tersebut tersisipkan dan proses pengekstraksian data itu sendiri berdasarkan kunci yang diberikan.

***Kata kunci**: steganography, inversion image, extract hidden data*

1. Pendahuluan

Sekarang ini banyak terjadi pencurian data digital dalam proses pengiriman data. Sebagai contohnya bila ada orang yang ingin membeli barang secara online via web, otomatis ia harus mengirimkan data kartu kreditnya melalui web tersebut. Namun bagaimana cara ia memastikan bahwa web tersebut aman? Apakah web tersebut tidak di-*hack* oleh pihak-pihak tertentu yang ingin mencuri data-data pribadi seseorang?

Untuk mencegah terjadinya hal-hal tersebut diperlukan sebuah cara yang menjanjikan keamanan dan keabsahan dari data yang dikirim. Selain dari penyajian saluran yang aman untuk proses pengiriman data, diperlukan juga media yang aman untuk data itu sendiri, agar ketika ada penyusup dalam jaringan tersebut yang ingin merusak ataupun mencuri data, ia tidak dapat mengakses data terebut karena data tersebut telah terkunci.

Salah satu cara untuk menjaga keamanan tersebut adalah dengan menyisipkan data-data rahasia tersebut ke dalam suatu media yang dapat disebarkan secara publik sedemikian rupa hingga data yang disispkan tersebut tidak dapat dilihat secara langsung. Apabila data tersebut ingin diekstrak, maka harus ada sebuah program yang bisa mengekstraksinya dengan kunci tertentu. Apabila kunci yang dimasukkan tersebut salah, maka data yang akan diperolehnyapun tidak akan valid.

Mengenai medianya, kita dapat menyimpannya dalam sebuah gambar. Gambar tersebut dapat dimanipulasi terlebih dahulu sebelum dan sesudah penyisipan data itu dilakukan untuk menambah kualitas keamanan penyimpanan data tersebut.

2. Gambar dan Manipulasinya

Gambar yang dijadikan media penyimpanan data rahasia bisa dimanipulasi terlebih dahulu. Manipulasi ini ditujukan untuk meningkatkan kualitas keamanan media penyimpanan data rahasia tersebut. Manipulasi tersebut ada berbagai macam, misalnya inversi, transposisi, grayscale, dan color conversion.

Setiap metode manipulasi gambar ini merupakan perubahan warna-warna pixel dengan suatu

aturan atau cara tertentu sehingga gambar hasil manipulasi tersebut berbeda dengan gambar aslinya.

Gambar 1 Sample Gambar Normal

Data gambar yang disimpan ini berbentuk hexadesimal, yaitu 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 yang dilambangkan dengan 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Sedangkan formatnya itu sendiri adalah dengan ARGB, yaitu 32-bit blok pixel.

ARGB ini melambangkan 4 kumpulan 8-bit blok data. 8-bit blok yang pertama merupakan data transparansi pixel, 8-bit yang kedua merupakan tingkat warna merah, 8-bit yang ketiga merupakan tingkat warna hijau, dan 8-bit yang ketiga merupakan tingkat warna biru. Setiap 8-bit blok data tersebut menggunakan 2 digit hexadesimal untuk mengetahui tingkatan warnanya.

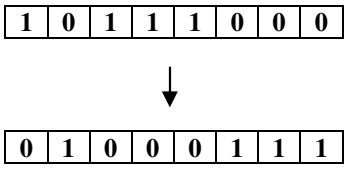
2.1. Gambar Inversi

Gambar inversi, seperti yang telah dijelaskan dalam abstrak makalah ini, merupakan gambar yang sama seperti gambar normal, namun setiap pixel warnanya merupakan inversi dari warna pixel gambar aslinya. Sebagai contoh warna hitam menjadi putih. Inversi warna ini bukanlah seperti inversi warna dalam dunia nyata melainkan inversi warna secara digital.

Gambar 2 Hasil Inversi dari Gambar 1

Dalam gambar inversi, bentuk asli gambar masih jelas terlihat. Hal ini dikarenakan manipulasi gambar hanya sebatas perubahan warna setiap pixelnya, yaitu warna inversinya.

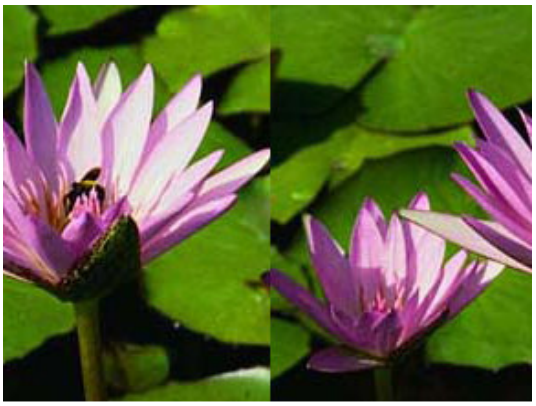
Dari segi data binernya, setiap pixel dari gambar ini sudah berbeda jauh. Bit yang awalnya bernilai 1 dijadikan 0, begitu pula kebalikannya, bit yang awalnya bernilai 0 dijadikan 1. Hal ini dilakukan untuk setiap bit yang terkandung di dalam gambar, kecuali bagian *header* dan *footer*-nya, karena *header* tersebut hanya mengandung data tipe file gambar dan informasi mengenai gambar tersebut, seperti dimensi gambar ataupun tipe gambar (.jpg, .bmp, dll), sedangkan *footer* hanya mengandung meta data gambar dalam bentuk xml



Gambar 3 Sample Inversi Bit Pixel pada Gambar

2.2. Gambar Tranposisi

Gambar transposisi merupakan gambar normal yang posisi pixel-pixelnya ditukar satu sama lain. Hal ini mengakibatkan bentuk gambar bisa berubah sangat banyak.



Gambar 4 Hasil Transposisi Pixel dari Gambar 1

Dalam contoh **Gambar 4**, terlihat gambar tidak terlalu berubah dari gambar aslinya. Hal ini dikarenakan transposisi pixel secara semi global, yaitu pixel-pixel yang ada di sebelah kiri ditukar dengan pixel-pixel yang ada di sebelah kanan.

Namun untuk transposisi yang lebih rumit, misalnya transposisi acak bisa jadi bentuk asli gambar sudah tidak bisa diketahui lagi.

2.3. Gambar Grayscale

Seperti layaknya gambar inversi, pada gambar grayscale bentuk asli gambar masih terlihat, namun informasi warnanya telah dibuang, yag tersisa hanyalah informasi cahaya pada tiap pixelnya.

Informasi cahaya tersebut bisa dikalkulasi dari campuran warna-warna pixel aslinya, sehingga pada saat proses perubahan gambar dari gambar normal ke gambar inversi sebelumnya dilakukan kalkulasi cahaya pada tiap pixel tersebut.

Gambar 5 Hasil Grayscale dari Gambar 1

Seperti yang terlihat pada gambar 5, semakin tinggi hasil kalkulasi cahaya pada warna pixel aslinya, maka semakin putih warna pixel pada gambar grayscalenya. Begitu pula kebalikannya, semakin rendah hasil kalkulasi cahaya pada warna pixel aslinya, maka semakin hitam warna pixel pada gambar grayscalenya.

Namun proses grayscale tidak seperti proses inversi. Proses ini merupakan proses yang *irreversible*, yaitu tidak dapat dikembalikan seperti semula. Hal ini dikarenakan hasil kalkulasi cahaya tersebut merupakan hasil kombinasi kalkulasi warna merah, hijau, dan biru yang terkandung dalam setiap pixelnya. Dan dari nilai kombinasi tersebut kita tidak bisa menentukan nilai masing-masing warna merah, hijau, dan biru dari gambar aslinya.

2.4. Gambar Color Conversion

Dalam gambar color conversion ini, suatu jenis warna diubah nilainya dan diterapkan pada setiap pixel yang ada dalam gambar asli sehingga gambar tersebut berubah. Nilai dari gambar asli tersebut dijadikan suatu variabel yang akan ditambahkan pada nilai warna yang berkorespondensi dengan nilai warna pada gambar calon hasil color conversion.

Gambar 6 Hasil Color Conversion (Merah) dari Gambar 1

Dalam contoh gambar diatas, sebuah warna yaitu merah ditentukan sebagai variabel peubah dari **Gambar 1**. Lalu warna tersebut dikalkulasi dengan tiap pixel dari gambar calon hasil konversi, sehingga terciptalah **Gambar 6**.

3. Steganografi

Steganografi ini merupakan penyisipan data dalam sebuah media digital lain. Salah satu medianya adalah gambar. Gambar tersebut

seakan menjadi data itu sendiri, karena apabila gambarnya rusak, maka datanya tidak akan bisa diambil kembali.

Proses penyimpanannya sendiri adalah setiap blok data disisipkan dalam data pixel gambar. Karena perubahan data pixel sedikit, maka perbedaan gambar tidak akan terlihat secara langsung oleh mata.

Steganografi juga merupakan salah satu teknik kriptografi kunci simetris dimana kunci untuk mengekripsi sama dengan kunci untuk mendekripsi.

4. Steganografi Ganda

Steganografi ganda merupakan 2 tingkat steganografi dimana media gambar itu sendiri harus dimanipulasi terlebih dahulu sebelum proses penyisipan datanya dilakukan. Seperti yang telah dijelaskan sebelumnya, hal ini dilakukan untuk mendapatkan media yang tingkat keamanannya lebih tinggi dari media steganografi biasa. Proses manipulasi tersebut bisa bermacam-macam, yaitu dengan inversi, *color conversion*, transposisi pixel, dan grayscale.

Steganografi ganda ini secara tidak langsung memerlukan 2 buah kunci dalam proses kerjanya. Kunci yang pertama digunakan untuk mengetahui bagaimana pixel harus di proses, dan kunci yang kedua adalah bagaimana data yang disimpan dalam pixel-pixel tersebut diambil. Namun dalam prakteknya kedua kunci tersebut bisa dijadikan satu untuk mempermudah pengaksesan oleh user, kemudian dipecah kembali menjadi 2 oleh programnya.

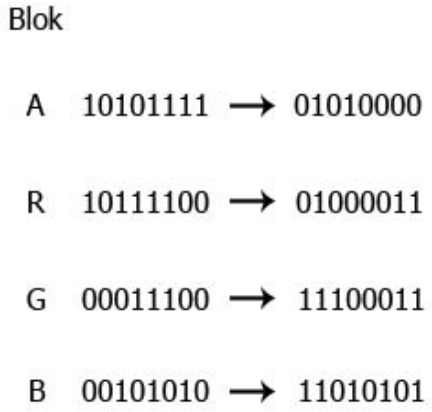
Proses pixel itu sendiri bisa dikategorikan dalam 4 metode secara umum, yaitu gambar inversi, color conversion, transposisi, dan grayscale. Dalam kriptografi blok cipher, 4 bagian proses pixel ini seperti layaknya ECB, CFB, CBC, dll, yaitu metode enkripsi blok, namun dalam hal ini keempat metode tersebut adalah cara utama proses pixel.

4.1 Kunci 1 – Proses Pixel

Kunci pertama ini merupakan kunci yang penting dalam steganografi ganda. Hal ini dikarenakan apabila kunci yang pertama salah, walaupun kunci yang kedua benar, data yang diambil tidak akan valid. Gambar yang dihasilkan oleh kunci yang kedua ini juga bukan merupakan gambar yang seharusnya.

4.1.1 Gambar Inversi

Dalam gambar inversi, setiap bit dalam blok ARGB ditukar antara bit yang 0 menjadi bit 1, sedangkan bit 1 menjadi bit 0.



Gambar 7 Sample Blok Gambar Inversi

Dalam contoh gambar diatas, setiap bit blok pixel diinversikan nilainya. Setelah didapat kumpulan blok pixel hasil inversi, barulah kunci kedua akan diterapkan.

Namun penggunaan kunci pertama tidak sesederhana ini. Kita bisa menambah tingkat kerumitannya dengan mencegah perubahan salah satu blok antara ARGB ataupun salah satu bit dalam kumpulan 8-bit blok data masing-masing ARGB tersebut. Hal ini mungkin mengakibatkan perubahan dalam gambar yang akan terlihat namun perubahan tersebut tidak akan signifikan.

4.1.2 Gambar Grayscale

Dalam gambar grayscale, prosesnya berbeda dengan gambar inversi. Tiap bit blok pixelnya tidak sekedar diinversikan saja melainkan harus ada perhitungan kombinasi tiap blok ARGB.

Tiap blok ARGB tersebut harus dijadikan bentuk desimal terlebih dahulu, kemudian dikalkulasi dalam suatu rumusan tertentu hingga didapat nilai grayscalenya. Nilai grayscale tersebut kemudian disimpan kembali dalam bentuk hexadesimal yang kemudian dijadikan nilai untuk blok R, G, dan B (ketiga blok ini harus memiliki nilai yang sama agar hasil gambar adalah gambar grayscale).

Penggunaan kunci pertama dalam gambar grayscale adalah saat proses kalkulasi warna grayscalenya, dimana dimasukkan suatu nilai yang bisa di-*generate* melalui kunci yang diberikan user yang kemudian dijadikan variabel peubah yang ditambahkan dalam nilai grayscalenya. Hal ini tidak akan mengubah bentuk gambar melainkan hanya akan mengubah tingkat brightness (intensitas cahaya) pada gambar hasil grayscale bila dibandingkan perubahan grayscale secara biasa. Namun hal itu bukan perngaruh besar karena perubahan intensitas caya itu sendir tidak akan terlalu besar.

4.1.3 Gambar Transposisi

Gambar transposisi ini merupakan pertukaran pixel-pixel secara massal karena semua pixel yang ada dalam gambar akan diproses, sedangkan pixel mana saja yang akan bertukar posisinya dan target pixel pertukarannya ditentukan oleh kunci yang diberikan user.

Transposisi tersebut bisa berupa transposisi sederhana seperti **Gambar 4** ataupun transposisi denga menggunakan substitusi pixel-per-pixel. Substitusi pixel-per-pixel ini merupakan pertukaran pixel dimana posisi pixel yang berdekatan tidak akan berdekatan pada hasil pertukaran pixelnya. Hal ini mengakibatkan gambar hasil transposisi pixel akan berbeda jauh dengan gambar aslinya.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

7	2	14	10
12	13	4	5
8	16	1	9
11	3	15	6

Gambar 8 Sample Blok Gambar Transposisi 4x4 Pixel

Seperti yang terlihat pada **Gambar 8**, koordinat pixel yang berubah sangat berbeda dengan koordinat awal, sehingga gambar hasil transposisi akan jauh berbeda dengan gambar aslinya.

4.1.4 Gambar *Color Conversion*

Gambar hasil color conversion ini memiliki salah satu intensitas RGB yang meningkat dan / atau menurun. Perubahan intensitas blok yang dipilih (R, G, atau B) dan peningkatannya didapat dari kunci yang diberikan oleh user. Peningkatan tersebut tidak mengubah bentuk gambar, melainkan mengubah salah satu intensitas warna dalam tiap pixelnya saja (karena setiap pixel mengandung semua blok ARGB, hanya nilainya saja yang berbeda-beda)

4.2 Kunci 2 – Proses Penyisipan Data

Kunci kedua digunakan pada saat penyisipan data ke dalam gambar yang telah sebelumnya di proses oleh kunci pertama.

Kunci yang diberikan oleh user akan digunakan untuk menentukan dalam blok mana (ARGB) potongan-potongan blok data rahasia akan disisipkan dan selang antar pixel yang digunakan. Oleh karena itu ada syarat yang harus dipenuhi oleh media penyimpanan gambarnya,, yaitu :

$$M \geq (d * r) * 2$$

M = jumlah pixel media penyimpanan
d = ukuran data
r = selang penyimpanan
2 = nilai penyimpanan blok data, 4 karena ada 4 blok, yaitu ARGB, dan masing-masing blok berjumlah 8 bit

Langkah-langkah penyimpanan data berlangsung sebagai berikut :

1. Kalkulasi panjang data
2. Bagi data berdasarkan jumlah pixel yang ada
3. Masukkan kunci pertama untuk pemrosesan gambar
4. Proses gambar
5. Masukkan kunci kedua
6. Kalkulasi kunci kedua untuk menentukan selang dan posisi penyisipan data
7. Masukkan setiap 4 bit data ke dalam 1 blok pixel ARGB dengan selang tertentu (dari kunci kedua)
8. Lakukan proses pembalikkan gambar sesuai dengan kunci pertama

Setelah keseluruhan proses dilalui, gambar akan kembali menjadi seperti semula, namun dengan sedikit perubahan dari segi visual (mungkin juga tidak terlihat apabila menggunakan metode inversi atau color conversion) dan mengandung sisipan data rahasia dalam setiap pixelnya.

Namun dalam metode inversi, color conversion, dan transposisi, metode penyimpanan dan pengekstraksian data berbeda dengan metode grayscale, karena dalam grayscale proses manipulasi gambarnya irreversible.

Dalam metode grayscale, kita bukan menyisipkan data setelah gambar dibuat menjadi grayscale, melainkan pada saat awal, tanpa harus dijadikan grayscale terlebih dahulu. Selain itu pada saat proses penyisipan gambar selesai, gambar tidak perlu dimanipulasi balik untuk proses ekstraksi datanya.

Langkah-langkah penyimpanan data dalam metode grayscale adalah sebagai berikut :

1. Kalkulasi panjang data
2. Bagi data berdasarkan jumlah pixel yang ada
3. Masukkan kunci pertama untuk pemrosesan gambar
4. Kalkulasi rumus grayscale dengan kunci pertama
5. Masukkan kunci kedua
6. Kalkulasi setiap 4 bit data dengan hasil dari langkah no 4
7. Masukkan setiap hasil langkah no 6 ke dalam 1 blok pixel ARGB dengan selang tertentu (dari kunci kedua)

5. Kesimpulan

Steganografi merupakan salah satu metode kriptografi yang membutuhkan media penyimpanan data yang rahasia. Dalam steganografi itu sendiri ada beberapa jenis, slaha satunya dalah dengan menggunakan gambar sebagai media penyimpanannya.

Steganografi Ganda merupakan pengembangan metode steganografi yang bertujuan untuk meningkatkan tingkat keamanan dari steganografi biasa, yaitu dimana gambar yang dijadikan media harus dimaipulasi terlebih dahulu.

Dari keempat metode steganografi ganda pada gambar, metode grayscale merupakan metode yang paling aman. Hal ini dikarenakan proses manipulasi gambar yang irreversible, sehingga proses penyimpan data harus dikalkulasi sejak awal dan tanpa harus memanipulasi gambar secara langsung.

DAFTAR PUSTAKA

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

[2] Hearn, Donald (2004). Graphics Principles and Practice In C. Prentice Hall.