

STEGANOGRAFI DENGAN DERET UNTUK MENGACAK POLA PENEMPATAN PADA RGB

Renddy, Teady Matius Surya Mulyana
Renddy.wr@gmail.com, tmulyana@bundamulia.ac.id
Teknik Informatika Universitas Bunda Mulia

Abstrak

Perkembangan teknologi diseluruh dunia mengakibatkan tidak terjaminnya keamanan, sehingga harus ada sebuah sistem yang dibuat untuk meminimalisir ketidakamanan sebuah data melalui media internet. Maka aplikasi steganografi membantu untuk menyamarkan sebuah data dalam sebuah gambar.

Steganografi merupakan metode untuk menyembunyikan pesan didalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada suatu pesan didalam media tersebut.

Untuk meningkatkan kerahasiaan data dalam steganografi, ditambahkan modus yang didapat dari selisih nilai kunci dan jumlah bit karakter sehingga didapat permutasi dari nilai RGB yang bervariasi.

Penggunaan kunci dapat meningkatkan penyembunyian data, karena semakin tinggi nilai maka variasi modus yang didapat semakin acak atau rumit.

Kata kunci: Steganografi, RGB, kunci, bit

PENDAHULUAN

Perkembangan jaman ini telah mempengaruhi seluruh belahan dunia yang mempermudah masing-masing pekerjaan dari setiap individu, sehingga tidak perlu membuang banyak waktu dan dana untuk melakukan komunikasi, mendapatkan informasi serta bertukar data satu sama lain melalui media internet. Akan tetapi, dengan kemajuan teknologi pun ada sisi ketidakamanan, seperti terjadinya penipuan, pembobolan ATM, pengambilan data tanpa diketahui pemiliknya, dll.

Sehingga perlu diciptakan sebuah sistem dimana data yang akan ditransfer dari satu orang kepada yang lain harus disamarkan dalam sebuah media. Media yang digunakan untuk menyamarkan data tersebut adalah sebuah objek gambar. Dengan gambar tersebut data akan disamarkan sehingga tidak mengundang kecurigaan dari *hacker* yang berusaha untuk mencuri atau memanipulasi data penting.

Selain itu, dari penelitian ini memberikan manfaat untuk memberikan wacana bagi steganografi bahwa suatu penyamaran data pada steganografi dapat dilakukan dengan metode deret pada *channel-channel* RGB.

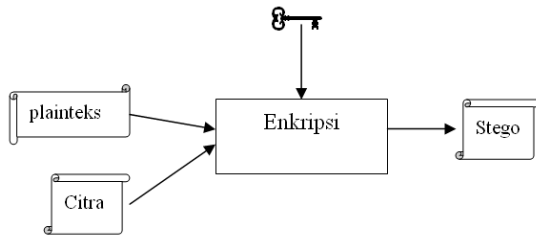
LANDASAN TEORI

Sutoyo (Sutoyo, 2009)[4] menjelaskan, steganografi merupakan metode untuk menyembunyikan pesan didalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada suatu pesan didalam media tersebut. Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos* yang artinya “tersembunyi/terselubung” dan *graphein* “menulis” sehingga kurang lebih artinya “menulis (tulisan) terselubung”.

Steganografi sebagaimana yang dijelaskan oleh Ariyus (Ariyus, 2006)[1] seperti yang dikutip Mulyana (Mulyana, 2013)[2] adalah cabang ilmu yang mempelajari tentang bagaimana menyembunyikan informasi didalam informasi lainnya. Lebih khusus, Sutoyo (Sutoyo, 2009)[4] menjelaskan bahwa *steganography* dalam pengolahan citra adalah sebuah teknik penyembunyian pesan pada sebuah media berupa citra.

Mulyana (Mulyana, 2013)[2] mengilustrasikan proses enkripsi yang diperagakan pada gambar 1. Pada teknik steganografi dilakukan dengan cara

menguraikan plainteks karakter per karakter. Kemudian setiap karakter akan diuraikan bit per bit. Bit-bit yang diuraikan dari plainteks akan disisipkan pada salah satu atau semua channel RGB pada sel tertentu yang sudah ditentukan sesuai dengan kunci yang dipergunakan.

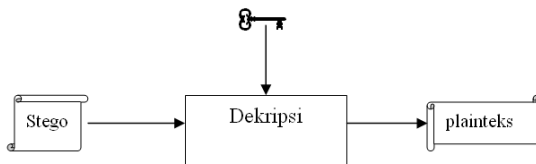


Gambar 1. Proses Enkripsi

Proses penyisipan bit pada nilai piksel dilakukan dengan cara menyamakan nilai bit terakhir dari channel yang akan disisipi pada piksel tersebut dengan nilai bit dari plainteks yang akan disisipkan.

Kunci pada Steganografi dapat berupa suatu bilangan yang menentukan posisi piksel-piksel yang akan disisipi oleh bit-bit dari plainteks. Channel-channel RGB dapat pula dianggap sebagai posisi yang berdiri pada masing-masing channel RGB atau dapat juga dianggap sebagai satu kesatuan posisi penyisipan bit plainteks.

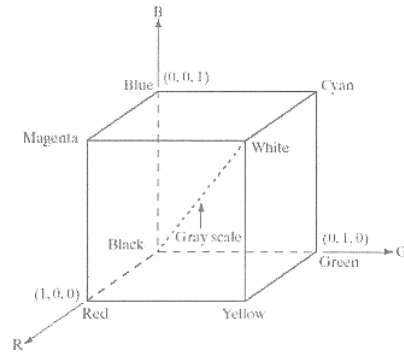
Gambar 2 mengilustrasikan proses dekripsi. Proses dekripsi dilakukan dengan cara mengambil nilai dari masing-masing posisi piksel sesuai dengan ketentuan kunci. Untuk setiap nilai yang diambil dari masing-masing piksel tersebut, diambil bit terakhir dan digabungkan sampai terkumpul 8 bit. Setelah terkumpul 8 bit maka akan didapatkan sebuah karakter.



Gambar 2. Proses Dekripsi

Sutoyo (Sutoyo, 2009)[4] menjelaskan, model warna RGB berorientasi *hardware*, terutama untuk warna monitor dan warna pada kamera video. Dalam model ini

tiap warna ditunjukkan dengan kombinasi tiga warna primer. Ketiga warna primer tersebut membentuk sistem koordinat cartesian tiga dimensi. Lihat gambar 3. Subruang pada diagram tersebut menunjukkan posisi tiap warna. Nilai RGB terletak pada satu sudut dan nilai *cyan*, *magenta*, dan *yellow* berada di sudut lainnya. Warna hitam berada pada titik asal, sedangkan warna putih terletak pada titik terjauh dari titik asal. *Grayscale* membentuk garis lurus dan terletak di antara dua titik tersebut.



Gambar 3. Skema Warna Kubik RGB

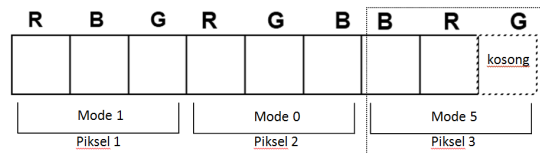
ANALISIS DAN PERANCANGAN

Renddy (Renddy, 2014)[3] menerapkan suatu metode pada algoritma pada pemrograman. Pada kenyataannya orientasi apapun baik itu prosedural dan terstruktur, pemrograman berorientasi objek maupun pemrograman visual.

Pada mode variasi RGB telah ditentukan indeks pola yang terjadi dengan pola permutasi berikut :

- > RGB merupakan indeks ke 0
- > RBG merupakan indeks ke 1
- > GBR merupakan indeks ke 2
- > GRB merupakan indeks ke 3
- > BGR merupakan indeks ke 4
- > BRG merupakan indeks ke 5

Contoh penempatan karakter pada masing-masing pixel pada citra 10 x 10 sebagai berikut :



Gambar 4. Penempatan Karakter R Pada Piksel

Untuk menentukan sebuah rumusan agar mendapatkan beberapa variasi mode nilai RGB dengan enam kemungkinan yang akan terbentuk dari sebuah rumus.

Rumus ini didapat dari beberapa kali percobaan yang dilakukan menggunakan tabel pengujian. Dengan beberapa ketentuan yang ada sebagai berikut :

1. Modus ditentukan oleh kunci dan jumlah bit karakter
2. Dalam satu karakter disimpan dalam tiga piksel
3. Menggunakan mod enam bukan menggunakan yang lain dikarenakan enam menunjukkan jumlah pola yang mungkin terjadi dari nilai R, G dan B.
4. Mod menentukan jumlah pola yang akan dibentuk

Dari ketentuan yang ada didapat sebuah rumusan yang berfungsi untuk menentukan variasi mode. Ada enam kemungkinan yang terjadi yang akan digunakan sebagai mode untuk mengacak letak deret RGB tersebut. Persamaannya dapat dilihat pada rumus (1)

$$\text{modus} = (C - i) \bmod 6 \dots\dots\dots (1)$$

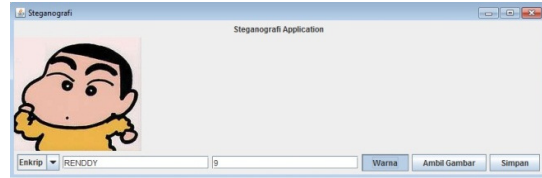
Notasi yang digunakan pada rumus (1) adalah :

1. i merupakan jumlah bit karakter
2. C merupakan sebuah variabel input untuk menentukan kunci yang akan digunakan untuk enkripsi

Dengan rumusan tersebut deret dari nilai RGB dapat diacak sesuai dengan mode yang ada mulai dari indeks nol sampai dengan indeks kelima. Dengan tujuan agar data yang telah disisipkan pada masing-masing piksel tidak mudah diambil atau ditebak. Karena setiap karakter akan disisipkan dengan masing-masing nilai RGB yang berbeda mode serta dibagi kedalam tiga piksel.

PEMBAHASAN

Setelah tipe pemrosesan telah dipilih kemudian menginput nilai kata dan nilai C sebagai kunci enkripsinya. Apabila nilai kata dan nilai C telah diisi, klik tombol warna untuk memprosesnya seperti gambar 5.

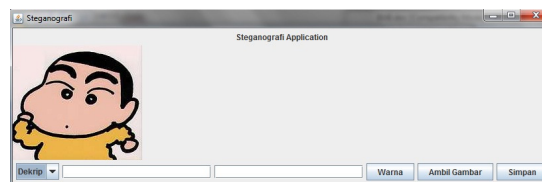


Gambar 5. Input Nilai Enkripsi

Selanjutnya, gambar yang diproses dalam penyisipan kata-kata kedalam gambar akan terlihat sama tanpa adanya perubahan bentuk maupun warna. Gambar asli dan gambar hasil proses terlihat sama saja yang dapat dilihat pada gambar 6.

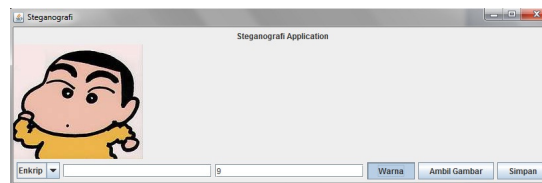


Gambar 6. Hasil Proses Enkripsi



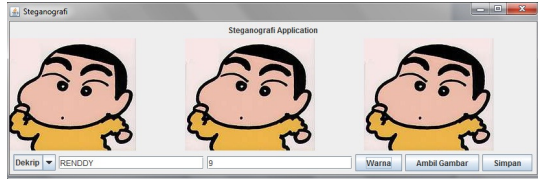
Gambar 7. Pemilihan Tipe Pemrosesan Dekripsi

Setelah pemilihan proses selesai, maka selanjutnya input nilai C dengan nilai yang diisi sewaktu enkripsi seperti pada gambar 5. Nilai diisi sama dikarenakan nilai C sebagai kunci enkripsi. Diilustrasikan seperti gambar 8.



Gambar 8. Input Nilai Dekripsi

Apabila nilai C telah diisi, selanjutnya klik button warna untuk melakukan pemrosesan gambar yang akan didekripsi. Maka nilai kata yang sebelumnya telah dienkripsi akan muncul seperti gambar 9.



Gambar 9. Hasil Proses Dekripsi

Dengan demikian setiap kata yang telah disisipkan pada gambar dengan nilai C sebagai kunci akan ditampilkan kembali pada textfield kata. Sehingga perlu diingat nilai C tersebut saat melakukan enkripsi data.

Tabel 1. Tabel Uji Steganografi

Nama Citra	Enkripsi Gambar Berubah	Stego	Data Dapat di Baca
Sinchan.jpg	TIDAK	Sinchan.png	YA
Flower.jpg	TIDAK	Flower.png	YA
Penguin.jpg	TIDAK	Penguin.png	YA
Krisan.jpg	TIDAK	Krisan.png	YA
Desert.jpg	TIDAK	Desert.png	YA
-	-	-	-
-	-	-	-
Hydrangeas.jpg	TIDAK	Hydrangeas.png	YA
Koala.jpg	TIDAK	Koala.png	YA
Lighthouse.jpg	TIDAK	Lighthouse.png	YA
Tulips.jpg	TIDAK	Tulips.png	YA
Jellyfish.jpg	TIDAK	Jellyfish.png	YA

Hasil pengujian steganografi dapat dilihat pada tabel 1. Berdasarkan uji coba yang telah dilakukan dari 100 gambar, hasil yang didapat saat enkripsi gambar tidak ada yang berubah. Disamping itu hasil stego dalam ekstensi .png agar . Dari setiap data yang telah dienkripsi dapat dibaca kembali ketika melakukan dekripsi. Hasil dari pengujian ini 100% berhasil.

KESIMPULAN

- Aplikasi yang dibuat mampu menyamarkan sebuah data
- Penggunaan nilai C sebagai kunci dapat meningkatkan penyembunyian data, karena semakin tinggi nilai maka variasi modulus yang didapat semakin acak atau rumit

SARAN

- Dengan fitur dan aplikasi yang sama, lakukan penelitian untuk metode steganografi dengan enkripsi dan dekripsi gambar menggunakan kunci huruf. Memanfaatkan huruf sebagai input nilai C sebagai kunci yang akan melalui tahap konversi nilai ke biner membuat enkripsi data semakin rumit dilacak

DAFTAR PUSTAKA

- [1] Ariyus. Donny, *Kriptografi*, Graha Ilmu, Yogyakarta, 2006
- [2] Mulyana. Teady M.S., *Kajian Penerapan Operasi Bitwise pada Steganografi*, *Jurnal Teknologi Informasi*, vol 9, pp 18-23., 2013
- [3] Renddy, *Steganografi Dengan Deret Untuk Mengacak Pola Penempatan Pada RGB*, Skripsi S1, Universitas Bunda Mulia, Jakarta., 2014
- [4] Sutoyo, T., mulyanto, E., Suhatono V., Nurhayanti OD., Wijanarto., *Teori Pengolahan Digital*, Andi Offset, Semarang, 2009.