Kriptografi Visual tanpa Ekspansi Piksel dengan Pembangkitan Warna dan Kamuflase Share

Georgius Rinaldo Winata / 13509030
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
Georgius.rinaldo@students.itb.ac.id

***Abstrak*—Kriptografi visual adalah salah satu cara penyembunyian makna dalam bentuk citra. Kriptografi yang berhubugan dengan citra sehingga bisa berupa penyisipan (steganografi) atau pengaburan makna dari citra itu sendiri. Pada makalah ini, topik yang akan dibawa adalah pengaburan makna citra atau kriptografi visual. Dalam Kriptografi visual terdiri dari beberapa share yang dibentuk dari aslinya. Teknik ini dibuat dengan ekspansi piksel sehingga menghasilkan noise dan memperbesar ukuran citra. Selain itu karena adanya noise dari pembangkitan share, hasil dekripsi dari citra tidaklah sepenuhnya seperti semula. Oleh karena itu, pada makalah ini akan dibahas mengenai kriptografi visual tanpa ekspansi piksel dengan tujuan menghilangkan noise yang ada pada share. Teknik ini dengan menggunakan pemecahan warna-warna yang ada pada file yang akan dibangkitkan sebagai share dalam hasil enkripsi.**

***Index Terms*—Kriptografi Visual, Steganografi, Share, Enkripsi, Dekripsi**

I. PENDAHULUAN

Kriptografi visual adalah salah satu teknik kriptografi yang berhubungan dengan pemanfaatan citra (*image*) sebagai medianya. Dalam teknik kriptografi ini peran citra dapat sebagai apapun baik plainteks ataupun kunci dengan hasil enkripsi berupa citra juga. Teknik kriptografi ini bisa dikatakan cukup aman karena dalam citra berhubungan dengan kemampuan indra manusia untuk mencernanya apakah citra ini adalah sebuah pesan rahasia atau bukan. Selain itu perubahan yang kurang berarti seperti pesan singkat yang disisipkan dalam citra tidak akan membawa perubahan yang signifikan pada citra. Selain itu memang dalam dunia pencitraan atau fotografi untuk *noise* adalah hal yang biasa terutama pada citra yang gelap. Oleh karena itu teknik ini bisa dikatakan cukup aman.

Dalam makalah ini, teknik yang akan dibahas bukanlah steganografi, tetapi pembangkitan share dari citra yang ada yang berlaku sebagai plainteks. Pada teknik pembangkitan share ini pada umumnya menghasilkan noise-noise yang merusak citra aslinya. Hal ini terjadi karena teknik yang digunakan untuk pembangkitannya menggunakan ekspansi piksel. Oleh karena itu, pada makalah ini akan dibahas mengenai pembuatan share dengan pembangkitan warna seperti yang dilakukan seniman, misalnya warna hijau yang dibentuk dari biru dan kuning. Dengan begitu share-share yang dihasilkan tidak perlu diekspansi pikselnya. Pembangkitan warna untuk share dengan cara yang lain juga bisa dilakukan pada teknik ini tergantung dari format berkas yang akan dibuat sharenya. Dalam makalah ini, akan dibatasi penggunaan format citra bitmap 24 bit untuk pembangkitan share dengan teknik yang dimodifikasi.

II. TEORI DASAR

A. Kriptografi Visual

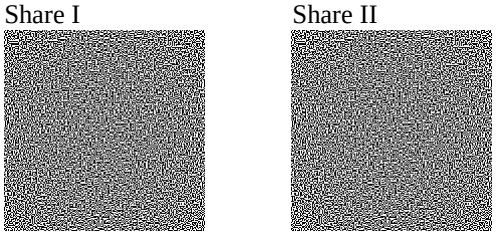
Kriptografi visual adalah sebuah teknik kriptografi yang memungkinkan penyembunyian informasi visual atau citra (enkripsi) sehingga tidak bermakna. Dengan teknik ini, proses dekripsi tidak perlu dilakukan dengan media komputer atau cukup dilakukan dengan menggabungkan dengan biasa (mekanikal). Teknik ini diperkenalkan pertama kali oleh Moni Naor dan Adi Shamir dalam jurnal *Eurocrypt'94*. Teknik ini terbatas hanya pada citra atau citra saja. Teknik ini dilakukan dengan membagi citra plainteks menjadi beberapa sejumlah share yang merupakan hasil enkripsinya. Dari beberapa hasil enkripsi tadi, proses dekripsi dilakukan dengan menumpuk share yang ada dengan benar sehingga terlihat makna dari citra tersebut.

Contoh:

Gambar 1. Plainteks

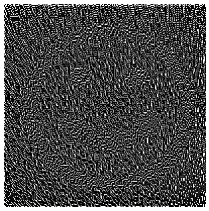
Enkripsi dengan dua buah share:

Share I Share II



Gambar 2. Share

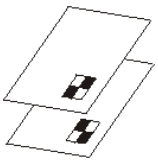
Dekripsi dengan menumpuk share



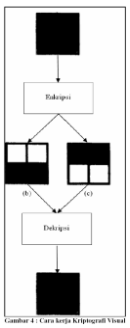
Gambar 3. Hasil dekripsi

Ada beberapa model teknik kriptografi visual yang diperkenalkan. Cara-cara yang pertama adalah model sederhana. Metode ini menggunakan citra biner hitam putih. Pembangkitan share dilakukan dengan bantuan representasi citra ke matriks secara acak. Representasi hitam dengan menggunakan angka 1 dan putih dengan menggunakan angka 0. Model ini sangat sederhana sehingga tidak aman. Oleh karena itu diciptakan lagi teknik yang baru oleh Shamir dan Noor .Cara yang kedua yang merupakan perbaikannya adalah teknik kriptografi visual dengan menggunakan metode ekspansi piksel. Pada metode yang digunakan ini akan dihasilkan *noise* yang membuat hasil dekripsi citra tidak sama persis dengan plainteksnya karena adanya piksel tambahan hasil enkripsi. Pada metode ini satu piksel dibagi menjadi beberapa sub piksel tergantung banyak sharenya sebagai pengganti matriks yang sebelumnya diajukan.

Gambar 8 : Pembentukan subpixel dengan m = 4



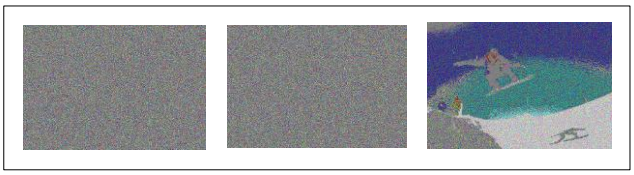
Citra 4. Satu piksel menjadi 4 subpiksel yang memecah warna hitam menjadi beberapa bagian



Gambar 5. Dekripsi piksel

Teknik kriptografi ini memiliki beberapa kelemahan. Salah satunya adalah *noise*. Seperti yang telah disebutkan sebelumnya, *noise* ini mengakibatkan hasil dekripsi citra tidak sesuai dengan plainteks yang dienkripsi. Hal ini terjadi pada metode ekspansi.

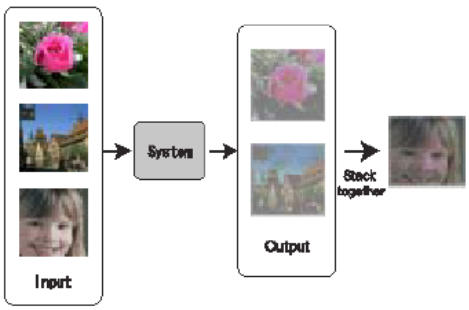
Citra asli



Share 1 **Share** **Hasil dekripsi**

Gambar 5. Kriptografi visual berwarna dengan noise

Kelemahan kedua yang ada dalam kriptografi visual ini adalah bahwa share yang dihasilkan tidak memiliki makna. Dengan begitu, tentu akan menimbulkan kecurigaan bagi orang lain yang mendapatkan share ini dan berasumsi terdapat pesan rahasia dalam share yang Ia dapat. Hal ini bisa digabungkan dengan steganografi. Dengan menyisipkan share pada citra lain dapat membantu mengurangi atau bahkan menghilangkan kecurigaan dari pihak lain yang mendapat share.



Gambar 6. Kamuflase kriptografi visual denga steganografi

Akan tetapi, hal ini menghilangkan elemen kriptografi visual yang menyatakan bahwa "proses dekripsi dilakukan secara mekanik atau tanpa komputer dengan cara ditumpuk". Dengan steganografi ini, tentu akan digunakan bantuan komputer tentunya seiring dengan berkembanya teknologi hal ini tidaklah menjadi masalah.

B. Struktur Berkas Bitmap (BMP)

Bitmap adalah suatu bentuk ekstensi berkas dari sebuah citra. Berkas dengan tipe ini digunakan di banyak tempat dan sudah kmpatibel. Tipe bitmap ini mempunyai resolusi yang cukup baik. Berikut adalah spesifikasi dari format bitmap.

Type	Bitmap
Colors	1-, 4-, 8-, 16-, 24-, and 32-bits
Compression	RLE, uncompressed
Maximum Image Size	32Kx32K and 2Gx2G pixels

Multiple Images Per File	No
Numerical Format	Little-endian
Originator	Microsoft Corporation

Format bitmap ini sendiri terdiri dari berbagai versi sehingga organisasi file dari tiap versi berbeda-beda. Tiap versi ini dikembangkan berdasarkan kebutuhan sistem operasi. Walau begitu format bitmap umumnya mempunyai struktur yang sama sebagai berikut.

Penjelasan singkat dari sturkuturnya adalah sebagai berikut. Pada header terdiri dari tipe, ukuran, reserved 1 dan 2, dan offset. Adapun fungsi header adalah untuk memeriksa apakah berkas yang dibuka adalah berkas dengan tipe bitmap yang sah atau tidak. Kemudian diikuti dengan tipe infoheader yang terdiri dari ukuran header (dalam byte), panjang citra, lebar citra, jumla *color planes*, bits tiap piksel, tipe kompresi, ukuran citra (dalam byte), xresolution, yresolution, jumlah warna, dan warna penting. Format info header ini memiliki panjang sebanyak 40 byte dengan fungsi sebeagai member tahu informasi dari citra bitmap yang dibuka.

Berikut adalah struktur dari file 32-bit bitmap yang akan dipakai dalam makalah ini.

a. BMP Header
   1. BM, *"magic number"* unsigned int 66 77, besar: 2 byte
   2. Besar bitmap, besar: 4 byte
   3. *Unused application specific*, besar: 4 byte
   4. Offset dimana pixel array bisa ditemukan, besar: 4 byte

b. DIB Header
   1. Besar byte DIB header, besar: 4 byte
   2. Width, besar: 2 byte
   3. Height, besar: 2 byte
   4. Banyak color plane, besar: 2 byte
   5. BI_Bitfield, besar: 4 byte
   6. Besar raw data dalam array piksel, besar: 4 byte
   7. Resolusi horizontal citra, besar: 4 byte
   8. Resolusi vertikal citra, besar: 4 byte
   9. Banyak warna dalam palette, besar: 4 byte
   10. Warna penting, besar: 4 byte
       ➔ Jika 0 artinya semua warna penting
   11. Red channel bitmask, besar: 4 byte
   12. Green channel bitmask, besar: 4 byte
   13. Blue channel bitmask ,besar: 4 byte
   14. Alpha channel bitmask, besar: 4 byte
   15. Tipe color space, besar: 4 byte
   16. Deifinisi LCS_windows_color_space, besar: (24h) + (4+4+4 byte)

c. Pixel Array
   Bentuk Array (3 byte)
   A B C D → warna alpha pixel pixel
   Contoh: 255 0 0 127

III. Aplikasi Modifikasi Pembangkitan Share

Pada makalah ini, akan dibahas mengenai metode pembangkitan share tanpa ekspansi piksel dengan tujuan mengurangi noise. Adapun cara yang diajukan ada dua yaitu dengan menggunakan teknik warna dasar seperti seni yaitu pembangkitan warna dari primer, sekunder, dan tersier, dan menggunakan pemecahan warna dari file format citra yang ada yaitu merah, hijau, dan biru (RGB). Pada modifikasi ini diharapkan tetap menjaga keamanan dari share dan tidak memperbesar citra. Dari hasil modifikasi ini akan dianalisis dan dicari kelemahannya.

Tolak ukur yang digunakan untuk penilaian terhadap pembangkitan share ini adalah sebagai berikut:

1. Apakah share yang dihasilkan masih bermakna
2. Apakah share yang dihasilkan dapat dikamuflase dengan baik pada citra lain
3. Apakah share dapat didekripsi secara mekanik sesuai kaidah kriptografi visual
4. Apakah hasil kamuflase dengan steganografinya cukup baik

A. Teknik Pembangkitan Share dengan Pencampuran Warna

Pada teknik ini, proses enkripsi dilakukan selayaknya seorang seniman. Teknik yang diajukan ini akan memisahkan warna-warna dari citra yang akan dienkripsi (plainteks) oleh seseorang menjadi warna-warna pembentuknya. Sama seperti teknik pencampuran warna pada seni yaitu warna sekunder dibentuk dari warna primer dan warna tersier dibentuk dari warna sekunder. Hal inilah yang akan diterapkan pada pembangkitan share dari plainteks dan akan dilakukan per pikselnya tanpa perlu membagi piksel-piksel itu menjadi sub piksel. Warna yang ada dalam piksel itu akan dipecah menjadi pembentuknya misalnya warna hijau akan dipecah menjadi biru dan kuning, dan sebagainya. Share bisa dibagi menjadi beberapa bagian berdasarkan ketentuan berikut:

1. Piksel pada share akan dipecah berdasarkan warna

pembentuknya

2. Jika jumlah share lebih dari dua dan warna pembentuknya hanyalah dua atau bahkan satu (warna primer), maka transparansi (alpha) dari warna pada piksel yang akan diubah
   Contoh pemecahan:

   Warna dalam 1 piksel adalah merah

Dua Share		
Share	**Warna**	**Alpha**
1	Merah	50%
2	Merah	50%

   Warna dalam 1 piksel adalah hijau

Empat Share		
Share	**Warna**	**Alpha**
1	Biru	25%
2	Biru	25%
3	Kuning	25%
4	Kuning	25%

3. Jika warna pembentuknya lebih dari dua, maka share akan dipecah secara biasa dan digunakan perhitungan transparansi (alpha) untuk memenuhi syarat jumlah share

B. Teknik Pembangkitan Share berdasarkan Format Warna Berkas Citra (RGB)

Pada teknik yang kedua ini, akan dibahas pembangkitan warna berdasarkan warna pada berkas citra yang menjadi plainteks. Metode ini dengan memanfaatkan pemecahan bitfield dari berkas yang merepresentasikan warna dari tiap piksel. Dalam format berkas bitmap terdapat bitfield yang merepresentasikan warna merah, biru, hijau, dan transparansi (alpha). Representasi ini akan dipecah-pecah untuk pembangkitan warna share dengan menyesuaikan dengan jumlah share yang ada.

Pada bagian ini dapat dibagi menjadi dua cara, yaitu:

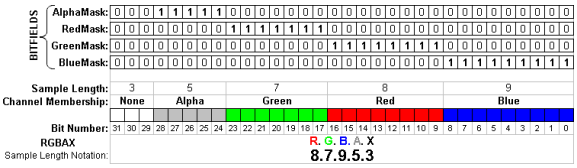
1. Pemisahan berdasarkan warna pembentuk dasar (merah, hijau, biru)
2. Pemisahan berdasarkan pemecahan bit komponen warna dasar berdasarkan beberapa share

Cara yang pertama adalah memecah suatu plainteks citra menjadi warna dasar penyusunnya. Proses ini menyebabkan share yang terbentuk adalah tiga buah saja karena hanya terdiri dari warna merah, hijau, dan biru. Share-share ini dibentuk dengan cara mengambil masing-masing komponen warna dasar pembentuk plainteks yang ada. Setelah diambil, warna dasar ini akan dipisah menjadi tiga buah share dan disimpan sebagai berkas bitra yang baru.

Cara yang kedua adalah berdasarkan pemecahan bit komponen warna penyusun plainteks. Metode ini mempunyai maksimal 8 share karena satu buah warna memiliki nilai 1 byte (8bit). Dari 1 byte itu akan diambil beberapa bagian bit sebagai share yang nantinya dari pengambilan bit-bit tersebut akan dikumpulkan dan dijadikan sebuah share.

Contoh:

Di bawah ini adalah komponen bit penyusun sebuah warna.



Share yang ingin dibentuk: 4

Diambil masing-masing dari RGBAX (merah hijau biru alfa) 2 bit dari tiap-tiap bytenya.

Contoh:

Pengambilan warna primitif merah

1	1	1	0	0	0	1	1

Diambil 2 bit pertama untuk share pertama, 2 bit kedua untuk share kedua, dan seterusnya, sehingga sharenya adalah:

- Share 1

1	1	0	0	0	0	0	0

- Share 2

0	0	1	0	0	0	0	0

- Share 3

0	0	0	0	0	0	0	0

- Share 4

0	0	0	0	0	0	1	1

Dan diteruskan pada byte berikutnya untuk green, alpha, dan blue.

Kedua teknik ini tentu akan menghasilkan share yang berbeda. Pada teknik yang pertama akan dihasilkan suatu share dengan warna yang seragam sedangkan pada share yang kedua akan dihasilkan warna yang teracak karena pemecahan bit. Walaupun menghasilkan warna yang berbeda, teknik kedua ini mempunyai cara dekripsi yang sederhana dengan komputer, yaitu dengan menggunakan operasi OR sehingga dari share-share yang ada dapat dikembalikan plainteksnya dan tentunya tanpa ada noise yang dihasilkan sedangkan cara yang pertama cukup dengan ditumpuk baik secara mekanik atau digital.

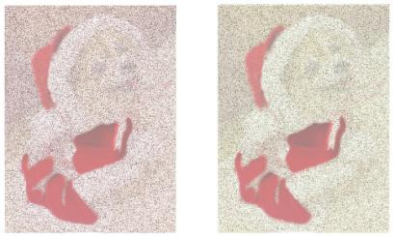
IV. Perbandingan dan Analisis Modifikasi Teknik Kriptografi Visual

A. Teknik Pembangkitan Share dengan Pencampuran Warna

Pada teknik ini akan dicoba membuat share dari plainteks citra sebagai berikut.

Gambar 7. Citra yang akan dieknripsi

Citra ini akan dibentuk share-sharenya dengan memecahnya menjadi warna dasar pembentuknya dengan dua buah share. Hasil dari pemecahannya adalah sebagai berikut



Gambar 8. Share 1 dan Share 2 yang dihasilkan

Dari kedua share yang dihasilkan terdapat masalah terbentuk. Masalah pertama adalah, bahwa share masih dapat diterawang jika dibagi menjadi dalam jumlah yang kecil karena tidak menggunakan ekspansi piksel yang dapat mengaburkan makna. Masalah yang terjadi adalah jika warna terlalu kontras dan mendominasi. Bisa dilihat pada citra share yang telah diperlihatkan. Terdapat warna merah yang juga merupakan warna primer yang tidak bisa dipecah lagi (masalah yang lebih buruk atau worst case). Warna ini tidak bisa dipecah lagi sehingga hanya perlu dikurangi transparansinya (alpha) sehingga pada share yang sedikit dapat terlihat jelas dan diterawang. Diikuti dengan warna ini mendominasi sebagian besar citra sehingga share masih terlihat bermakna. Hal ini dapat bermasalah juga misalnya pada citra landscape atau pemandangan yang mempunyai warna yang mendominasi seperti langit, perairan, dll.

Untuk share-share tersebut juga belum maksimal ketika dikamuflasekan. Ketika dikamuflasekan ke citra yang lain

B. Teknik Pembangkitan Share berdasarkan Format Warna Berkas Citra (RGB)

Pada teknik kedua ini ada dua model teknik yang diajukan. Pada subbab ini akan dibahas terlebih dahulu model yang pertama

I. Pemisahan berdasarkan warna pembentuk dasar (merah, hijau, biru)

Teknik ini dilakukan dengan pemecahan citra menjadi share yang merupakan warna penyusunnya. Dalam kasus ini warna penyusunnya terdiri dari merah, hijau, dan biru (RGB). Teknik ini sudah pernah dilakukan sebelumnya seperti yang dikutip dari makalah Sozan Abdulla, hanya saja dalam makalahnya Ia menggunakan warna dasar cyan, magenta, dan yellow (CMY). Dalam makalah ini akan dicoba juga dengan citra yang serupa pada makalah referensi Sozan Abdulla

Gambar 9. Citra yang akan dienkripsi

.

Gambar 10. Citra yang telah dipisah (RGB)

Share yang dihasilkan merupakan permisahan dari warna pembentuk plainteks. Masing-masing share merupakan perwakilan warna yang terbentuk dari hasil pemisahan komponen RGB dari plainteks. Share ini masih sangat lemah karena masih memiliki makna walaupun warnanya telah berbeda dari aslinya.

Untuk pengujian lebih lanjut, ketiga share ini akan dimasukkan ke gambar lain sebagai kamuflase.

Gambar 11. Contoh share yang telah dikamuflasekan

Pemilihan citra penutup (cover image) yang tepat menentukan hasil dari steganografi yang baik. Hal ini bisa dilihat pada contoh citra pada gambar 11. Pada citra yang pertama (kiri) dapat dilihat masih membekas warna biru pada penyisipan share sedangkan pada citra kedua (kanan) share telah terkamuflase dengan baik. Oleh karena itu, pemilihan citra untuk cover juga perlu dipertimbangkan dengan baik supaya hasil steganografi dapat maksimal.

II. Pemisahan berdasarkan pemecahan bit komponen warna dasar berdasarkan beberapa share

Teknik ini dilakukan dengan pemecahan bit citra untuk pembentukan sharenya. Tiap bit pada citra plainteks akan diambil sejumlah sharenya dengan share terbanyak sejumlah 8 buah share karena disesuakan dengan ukuran satu byte yang bisa dipecah menjadi 8 bit.

Contoh uji citra plainteks masih menggunakan gambar 7 dengan hasil share sebagai berikut.

Gambar 12. Share yang dihasilkan dengan pemecahan bit penyusun warna

Pada share yang dihasilkan dapat dilihat bahwa masih terlihat citra aslinya. Citra share yang dihasilkan terlihat samar-samar dengan noise berwarna putih. Hal ini dikarenakan dari algoritma pemecahan bit, warna-warna yang tadinya ada digantikan dengan warna putih pada sharenya sehingga pada kasus ini tiap share saling mengisi kekosongan pada share lain.

Pengujian lebih lanjut adalah dengan menyisipkan share ke citra lain sebagai kamuflase. Pada contoh dicobakan penyisipan pada gambar yang cukup kontras sebagai kasus terburuk. Ternyata menghasilkan sedikit noise pada bagian bagian tertentu. Bisa dilihat pada bagian tengah garis horizon terdapat noise-noise yang merupakan komponen dari share yang ada.

Gambar 12. Salah satu share yang telah disisipkan

V. KESIMPULAN

Berdasarkan dari pengujian yang ada, dapat dilihat bahaw kombinasi teknik yang kedua dengan pemisahan bit adalah teknik yang terbaik. Hal ini bisa dilihat dengan banyaknya noise ketika digabung dengan gambar yang sangat kontras dan kamuflase yang cukup baik. Jika dibandingkan dengan share teknik pertama dan teknik kedua yang menggunakan pemisahan warna dasar, ketika share digabungkan dengan gambar yang tidak kontras ternyata menghasilkan kamuflase yang kurang baik yang memperlihatkan citra yang ingin disembunyikan.

Jika dilihat dari share yang dihasilkan, share dengan teknik kedua lebih bagus karena cukup samar. Share yang dihasilkan semakin baik jika jumlah sharenya semakin banyak. Hal ini dapat dilihat pada teknik pertama maupun teknik kedua model kedua.

Selain itu, pemilihan citra penutup (cover image) untuk kamuflase dari share sangatlah penting. Hal ini dikarenakan warna yang kontras dan dominan dapat menimbulkan perbedaan pada citra hasil kamuflase. Dengan kamuflase yang buruk tentu akan menimbulkan kecurigaan pada citra tersebut.

REFERENCES

[1] Munir, Rinaldi, Ir.,M.T. 2005. Diktat Kuliah IF-5054 Kriptografi. Bandung : Informatika ITB

[2] arxiv.org/pdf/1004.4445

[3] http://www.fileformat.info/format/bmp/egff.htm

[4] http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah1-2006.htm

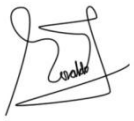
[5] http://msdn.microsoft.com/en-us/library/dd183377(v=vs.85)

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, 13 Mei 2012

ttd



Georgius Rinaldo Winata / 13509030