Kriptografi Visual dengan Memanfaatkan Algoritma ElGamal untuk Citra Berwarna

Ahmad Fauzan - 13510004
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510004@std.stei.itb.ac.id

***Abstract*—Berbagi citra manjadi kebiasan semua orang dewasa ini. Namun bagaimana jika berbagi citra yang hanya boleh diketahui oleh penerima dan pengirim. Berbagi citra melalui internet secara aman menjadi salah satu permasalahan yang dihadapi. Kriptografi Visual adalah salah satu solusinya.**

Berbeda dengan kriptografi visual yang ada. Kriptografi visual yang akan digunakan hanya dapat dipakai untuk citra digital. Kriptografi ini digunakan untuk berbagi citra digital.

Makalah ini akan membahas tentang kriptografi visual denga algoritma kunci publik yang ada. Algoritma kunci publik yang akan digunakan adalah algoritma ElGamal.

***Index Terms*—Kriptografi visual, ElGamal, Citra.**

I. PENDAHULUAN

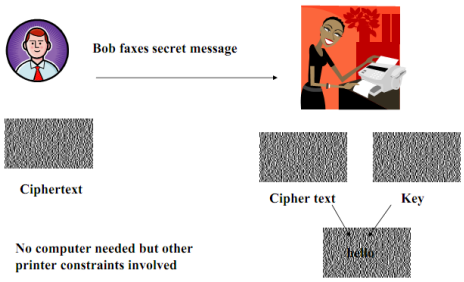
Pesan sekarang ini belum tentu adalah sebuah teks. Pesan dapat berupa sebuah gambar atau foto. Gambar keindahan alam bisa mewakili pesan untuk menjaga kelestarian alam. Foto seseorang dapat berupa pesan untuk menunjukkan diri. "Visual/Gambar/Foto bisa mewakili beribu kata". Begitulah kata pepatah. Sekarang ini, pesan teks sangat terkesan kuno dan kurang menjelaskan maksud. Kebutuhan orang untuk berbagi pandangan itu juga penting. Salah satu alat yang cukup ampuh dalam berbagi pandangan adalah dengan memvisualisasikan pandangan tersebut (gambar, foto atau video).

Pada zaman modern ini, banyak cara seseorang berbagi citra dengan orang lain, baik secara private ataupun public. Secara publik, orang dapat berbagi citra melalui media social, blog atau website. Secara private seseorang dapat berbagi citra, melalui chat, media social, email ataupun fax. Gambar dapat menjelaskan tentang hal besar yang sangat rahasia.

Dunia sekarang ini semakin global bahkan yang privasi dapat menjadi publik. Berbagi citra ke dua orang pun terkadang tidak aman. Kriptografi merupakan salah satu solusi untuk berbagi pesan rahasia. Namun bagaimana dengan citra ? Apa yang dapat dilakukan kriptografi untuk merahasiakan gambar tersebut ? Jawabannya adalah kriptografi Visual. Namun, adakah cara agar kriptografi visual ini efektif dan pesan tidak dapat dibaca oleh penyadap ?

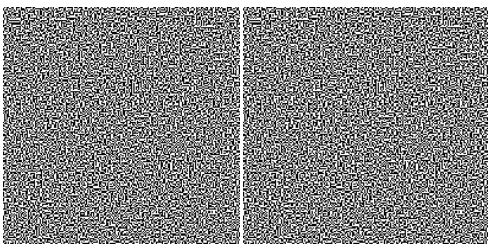
II. KRIPTOGRAFI VISUAL

Kriptografi visual ada teknik merahasiakan pesan yang dikhususkan untuk gambar/citra. Pertama kali dikenalkan oleh Moni Naor dan Adi Shamir tahun 1994. Metode pertama kali yang digunakan adalah dengan membagi citra menjadi beberapa bagian (share). Share ini jika digabung akan menjadi sebuah gambar yang berarti.



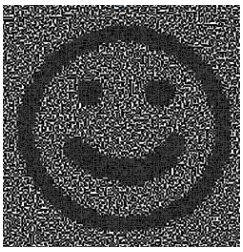
Gambar 1.Kriptografi visual

Misal sebuah gambar di enkripsi menjadi dua buah share.



Gambar 2. Kriptografi visual : Enkripsi

Jika kedua share itu ditumpuk maka akan menghasilkan sebuah gambar berarti.

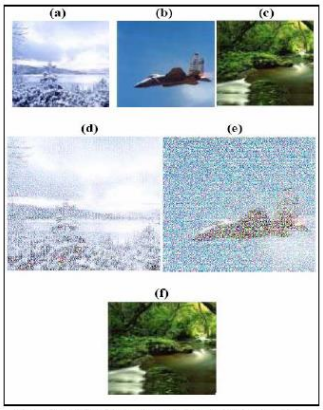


Gambar 3. Kriptografi visual : Dekripsi

Namun, methoda yang disarankan oleh Moni Naor dan Adam shamir ini terbatas hanya untuk citra tak berwarna

dan tidak cukup digunakan untuk gambar yang memiliki detil yang tinggi karena memiliki Noise dari hasil enkripsinya.

Dalam pengembangannya, bermunculan teknik-teknik yang lain. Dari Yu Chang tahun 2000 dengan kamuflase.



Gambar 13 : Kriptografi Visual Chang dkk.

Gambar 4. Kriptografi Visual Yo Chang tahun 2000

(a) dan (b) Gambar untuk klamufase sedang (c) adalah plainteks. (d) dan (e) adalah hasil enkripsi. (f) adalah hasil dekripsi.

III. ALGORITMA ELGAMAL

Algoritma ElGamal adalah sebuah algoritma untuk kriptografi kunci public. Algoritma ini dibuat oleh Taher ElGamal pada tahun 1985. Algoritma ini memiliki keamanan yang terletak pada kesulitan dalam menghitung logaritma diskrit.

Properti bilangan ElGamal.

1. Bilangan prima, p
2. Bilangan acak, g (g < p)
3. Bilangan acak, x (x < p); rahasia
4. $Y = g^x \bmod p$
5. m = plainteks
6. a dan b (chiperteks)

Dalam melakukan aksinya ElGamal memiliki 3 tahapan antara lain.

1. Pembangkitan Kunci
   Algoritma ElGamal merupakan algoritma kunci public. Dalam pembuatan kunci, ada beberapa langkah yang harus dilakukan.
   a. Pilih sembarang bilangan prima p
   b. Pilih 2 bilangan acak, g dan x; g < p & 1 <=x<=(p-2)
   c. Hitung $y = g^x \bmod p$

   Setelah itu, maka akan terbentuk dua buah kunci, yaitu kunci public (berisi y,g,p) dan kunci private (x,p).

2. Proses Enkripsi
   Dalam algoritma enkripsi, kunci yang digunakan adalah kunci public (y,g,p). Tahapan-tahapan proses enkripsi.
   a. Potong pesan menjadi blok-blok. (m1,m2….)
   b. Pilih bilangan acak k (1<=k<=(p-2))
   c. Setiap blok lakukan enkripsi

   $$a = g^k \bmod p$$
   $$b = y^k m \bmod p$$

   Pasangan a dan b merupakan pasangan chiperteks. Hasil enkripsi 2 kali lipat besar dari pesan.

3. Proses Dekripsi
   Kunci untuk proses dekripsi adalah kunci privat(x,p). Tahapan-tahapan dalam proses dekripsi :
   a. Gunakan x untuk menghitung

   $$(a^x)^{-1} = a^{p-1-x} \bmod p$$

   b. Hitung plainteks m dengan

   $$m = \frac{b}{a^x} \bmod p = b(a^x)^{-1} \bmod p$$

   Susun kembali blok-blok hasil dekripsi.

Pada dasarnya Algortima ini digunakan untuk berbagai macam kebutuhan, enkripsi data sangat bisa diandalkan dengan algoritma ini dan untuk kebutuhan signature. Dalam makalah ini, akan dijelaskan juga penggunaanya dalam kriptografi visual.

IV. CITRA

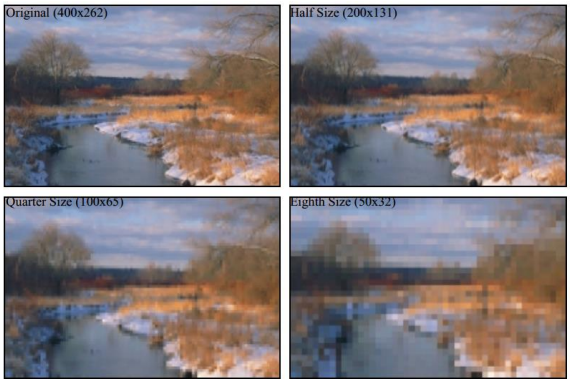
Citra/gambar adalah sebuah artifak yang menggambarkan atau merekan visualisasi dari suatu persepsi. Citra digital adalah representasi dari sebuah citra yang dijadikan sebuah array 2 dimensi agar dapat dibaca oleh computer. Citra digital disusun oleh beberapa pixel. Setiap pixel merepresentasikan sebuah warna pada satu poin pada citra, jadi pixel seperti titik kecil untuk sebuah warna.

Ada beberapa tipe citra digital.

1. Citra hitam dan putih
2. Citra berwarna
3. Citra binary
4. Citra warna berindeks

Ada beberapa property yang dimiliki oleh citra digital.

1. Resolusi
   Resolusi merupakan ukuran gambar dalam satuan pixel. Seperti yang dijelaskan sebelumnya pixel merupakan titik-titik warna pada gambar. Resolusi menentukan jumlah pixel dalam citra. Semakin besar resolusi, maka semakin besar dan detil dari kualitas citra tersebut.

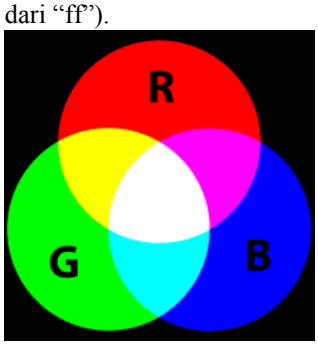


Gambar 5. Resolusi Citra

2. Kumpulan Pixel/Warna
   Bagian terkecil dari citra digital adalah pixel. Pixel mewakili warna pada gambar. Warna dalam pixel dapat direpresentasikan dengan 2 tipe, yaitu RGB dan CYK.

Warna pada pixel citra digital dapat direpresentasika menjadi 2 tipe.

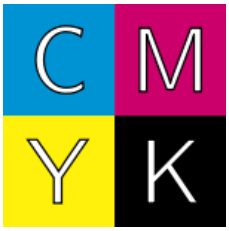
1. RGB (Red, Green, Blue).
   Kebanyakan computer sekarang ini menggunakan representasi ini untuk mengedit atau melihat sebuah citra digital. Pembentukan warna berdasarkan 3 warna dasar, yaitu merah, hijau, dan biru.
   Di dalam computer, biasanya warna RGB direpresentasika dengan nilai hexa decimal 0xffffff. Dua digit pertama mewakili warna merah, dua berikutnya warna hijau dan dua paling kanan mewakili warna biru (0xRRGGBB). Nilai setiap warna mewakili keikutsertaan warna tersebut. Nilai maksimal dari keterangan warna adalah 255 (nilai hexa dari "ff").



Gambar 6. Visualisasi RGB

   Contoh : Warna biru diwakili oleh 0x0000ff, warna putih diwakili oleh 0xffffff dan warna hitam oleh 0x000000.

2. CMYK (Cyan, Magenta, Yellow, Key/Black)
   Berbeda dengan RGB, warna hitam pada RGB adalah ketidakikutsertaan warna tersebut pada suatu warna. Sedang , CMYK memisahkan warna hitam dalam pembentukan warna. Warna putih adalah dimana ketika keempat warna CMYK bernilai 0.



Gambar 7. CMYK

   CMYK sangat jarang digunakan untuk mengatur warna sebuah pixel dalam citra digital. Pengaturan ini biasanya digunakan untuk percetakan.

V. KRIPTOGRAFI VISUAL DENGAN ELGAMAL

Setelah mengetahui seluk-beluk citra, kriptografi visual dan Algoritma ElGamal. Seperti sebelumnya dijelaskan, Algoritma ElGamal menghasilkan dua buah nilai chiperteks yaitu a dan b. Salah satu dari kedua nilai tersebut akan dijadikan chiperteks dan yang lain akan digunakan sebagai kunci. Nilai a sebagai nilai kunci dan nilai b sebagai chiperteks.

Pada kriptografi visual dengan ElGamal ini akan digunakan 3 buah kunci. Kunci pertama adalah kunci public. Kunci public akan digunakan untuk meng-enkripsi sebuah citra menjadi dua buah share. Share a dan share b.

Kunci kedua adalah kunci share. Kunci share merupakan kunci hasil dari enkripsi gambar. Kunci ini berukuran sama seperti citra. Kunci ini berupa sebuah gambar yang tidak berarti apa-apa. Kunci share ini sebenarnya adalah share a hasil enkripsi.

Kunci Ketiga adalah kunci private. Kunci private dan kunci share digunakan untuk proses dekripsi dari cchiper-citra yang telah dihasilkan oleh proses enkripsi.

Ada 3 proses utama dalam pengimplementasian kriptografi visual dengan ElGamal ini.

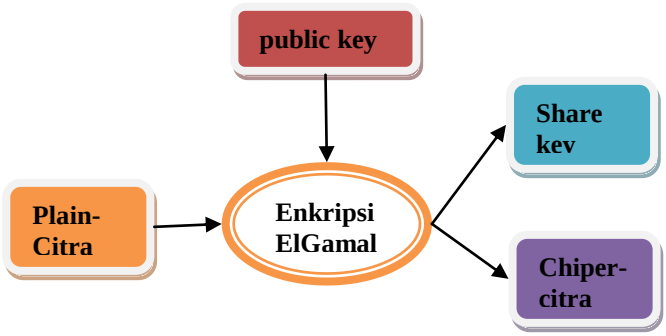
1. Pembangkitan kunci (kunci public dan private).
   Pembangkitan kunci sama seperti pembangkitan kunci pada ElGamal biasa.
   Hasil keluaran proses ini adalah kunci publik (y,g,p) dan kunci private (x,p).

2. Enkripsi dan pembangkitan kunci share
   Pada enkripsi kriptografi visual, tahapan-tahapan yang dilakukan adalah :
   a. Gunakan kunci publik untuk nilai-nilai pada proses ini. (Kunci publik diambil dari proses pembangkitan kunci).
   b. Buat dua buah buffer citra. Buffer (1) untuk menampung kunci share dan buffer (2) untuk menampung chiper-citra.
   c. Tunjuk satu atau beberapa buah pixel.
   d. Masukkan pixel tersebut kedalam pesan yang akan diproses (m).
   e. Pilih bilangan acak k (1<=k<=(p-2))
   f. Pada m, lakukan enkripsi

$$a = g^k \bmod p$$
$$b = y^k m \bmod p$$

g. Masukkan nilai a pada buffer (1) dan b ke buffer (2) dengan posisi sama seperti plain-citra. Ulangi lagi dari langkah (b) sampai semua pixel dalam citra telah diproses.

Hasil dari proses ini adalah sebuah chiper-citra dan sebuah kunci share.



Gambar 8. Skema Enkripsi Kriptografi visual dengan ElGamal

3. Dekripsi

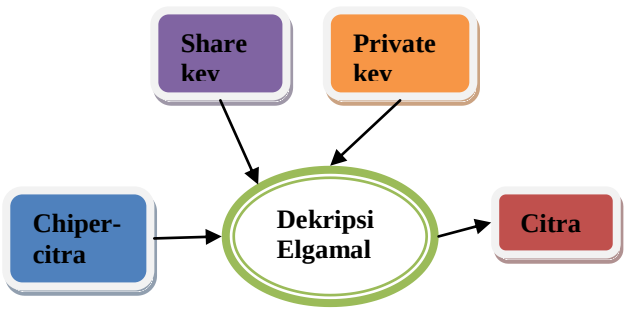
Pada dekripsi kriptografi visual dengan ElGamal, ada beberapa tahapan.

a. Buat sebuah buffer citra untuk menerima plain-citra.
b. Gunakan kunci private dan kunci share.
c. Pilih satu atau beberapa pixel pada posisi yang sama di kunci share dan chiper-citra.
d. Hitung m dengan

$$m = \frac{b}{a^x} mod\ p = b(a^x)^{-1} \bmod p$$

a merupakan nilai dari pixel yang ditunjuk pada kunci share sedang b adalah nilai pixel yang ditunjuk pada chiper-citra.

e. Masukkan m ke buffer pada posisi yang sama yang ditunjuk ke chiper-citra. Ulangi dari proses b hingga semua pixel dalam chiper-citra telah diproses.



Gambar 9. Skema Dekripsi Kriptografi visual dengan ElGamal

Untuk pemilihan pixel dalam proses Dekripsi dan Enkripsi ada beberapa metode yang dapat dilakukan.

1. One-pixel RGB
   Pada metode ini, pemilihan dilakukan dengan memilih satu buah pixel. Metode pemilihan ini sebaiknya diambil jika nilai p > 16777215. Jadi setiap proses melibatkan hanya satu pixel RGB.

2. One-segment RGB
   Pada metode ini, pemilihan dilakukan hanya pada satu segment warna, misal merah. Metode pemilihan ini sebaiknya diambil jika nilai p > 255. Proses enkripsi dan dekripsi dilakukan persegment pixel (satu pixel 3 kali proses untuk menciptakan pixel chiper-citra).

3. One-pixel CMYK
   Sama seperti metode one-pixel RGB, perbedaannya hanya pada representasi warna.

4. One-segment CMYK
   Sama seperti metode one-segment RGB, perbedaanya hanya pada representasi warna.

5. N-pixel RGB
   Pada metode ini, pemilihan dilakukan ke beberapa pixel sekaligus. Jelas, untuk proses ini membutuhkan nilai p dua kali lipat dari nilai p pada one-pixel RGB. Nilai p > 0xffffffffffff (Terlalu besar untuk diproses).

6. N-segment RGB
   Pemilihan dilakukan pada beberapa pixel sekaligus. Namun , pemroosesan dilakukan persegmen dari pixel-pixel tersebut. Jadi sederatan pixel tersebut diproses 3 kali sesuai dengan segmen pada RGB.
   Contoh : dipilih 2 pixel dengan nilai 0xffab12 dan 0xab13de. Maka pemrosesan 3 kali dengan nilai masing-masing ffab untuk nilai merah, ab13 hijau dan 12de untuk biru.

7. N-pixel CMYK
   Sama seperti many-pixel RGB, perbedaannya hanya direpresentasi warna.

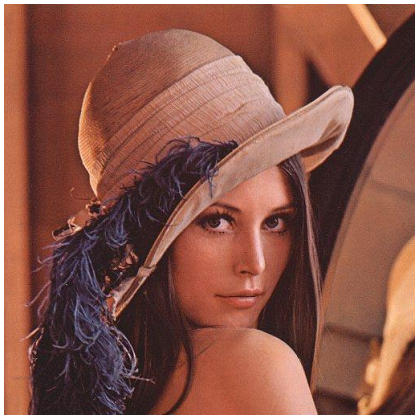
8. N-segment CMYK
   Sama halnya seperti many-segment RGB, pixel dengan CMYK akan diproses sebanyak 4 kali sesuai dengan segmennya.
   Misal : 0xffddea12 dan 0xab13cadd. Maka pemrosesan dilakukan dengan nilai-nilai ffab untuk Cyan, dd13 untuk Magenta, eaca untuk Yellow dan 12dd untuk Key(black).

VI. ANALISIS

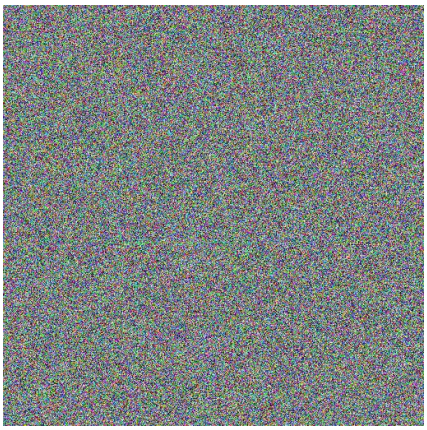
Berikut hasil penggunaan Kriptogafi visual dengan ElGamal dengan metode pemilihan One-pixel RGB.

Kunci :

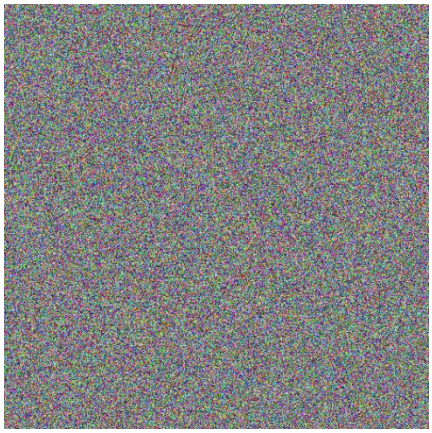
1. Kunci public : y = 5240469, g = 5522109, p = 16777259
2. Kunci private : x = 15960294, p = 16777259



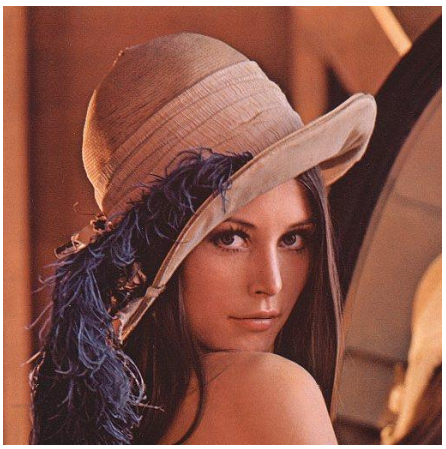
Gambar 10. Plain-image (Sebelum enkripsi)



Gambar 11. Share a (kunci share)



Gambar 12. Share b (chiper)



Gambar 13. Plain-image setelah dekripsi

Dengan metode ElGamal ini, dirasa dapat membantu pengiriman citra digital dengan aman. Namun, penulis mengetahui beberapa kekurangan dari metode yang ditawarkan ini :

1. Pemrosesan cenderung sulit.
2. Sulit untuk menyepakati metode pemilihan pixel yang digunakan.
3. Kurang cocok untuk chiper-citra yang bertujuan untuk dikirim dengan media cetak.
4. Mudah diketahui kalau citra tersebut merupakan chiper. Harus menggunakan kamuflase.

Kelebihan dari Metode ini :

1. Sangat aman karena cipher sulit untuk dipecahkan karena memiliki dua buah kunci untuk dekripsi (kunci private dan kunci share).
2. Hasil dekripsi memiliki kualitas yang sama dengan plain-citra yang digunakan enkripsi.
3. Tidak ada noise, karena pemrosesan dilakukan perpixel.

VII. MANFAAT DARI METODE INI

Manfaat dari metode ini adalah :

1. Memberikan metode yang lebih aman dan ampuh dalam bertukar/berkirim citra digital.
2. Metode ini menyediakan enkripsi dan dekripsi yang tidak mengurangi kualitas citra.
3. Metode ini menyediakan metode penyampaian citra secara lebih aman jika digabung dengan teknik kamuflase (seperti metode yang ditawarkan You Chang).

VIII. KESIMPULAN

Pemanfaatan algoritma ElGamal dalam kriptografi visual sangat baik. Penggunaannya menyebabkan tingkat keamanan naik dibanding dengan algoritma sebelumnya. Metode ini juga tidak mengurangi kualitas gambar hasil dekripsi dan tidak ada noise.

Namun, waktu pemrosesannya masih dirasa lama. Dalam pemilihan pixel yang diproses pengirim dan penerima harus menyepakati metodenya. Perlunya metoda kamuflase untuk menyembunyikan chiper-citra karena mudah diketahui kalau itu adalah chiper.

ElGamal sejauh ini sulit dipecahkan, maka bisa dikatakan Metode kriptografi visual ini sangat sulit untuk dipecahkan oleh penyadap. Sayangnya, metode ini tidak cocok untuk pengirima citra yang dicetak seperti fax.

DAFTAR PUSTAKA

[1] Slide kuliah Rinaldi Munir IF3058 Kriptografi

[2] Sachs, Jonathan. Digital Image Basics. Digital Light & Color. 1996-1999.

[3] Moni Naor, Adi Shamir. "Visual Cryptography". Department of Aplied Math adn Computer Sience, Weizmann Institute, Israel.

[4] You-Chang Hou. "Visual Cryptography for Color Images". *The Journal of the Pattern Recognition Society*. Department of Information Management, National Central University. 2002.

[5] Taher ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Information Theory*., published on Jul 1985.

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, 19 Mei 2013

Ahmad Fauzan
13510004