# Tanda Tangan Digital Untuk Gambar Menggunakan Kriptografi Visual dan Steganografi

Shirley - 13508094
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
[1]*if18094@students.if.itb.ac.id*

***Abstract*—Berkembangnya teknologi dengan pesat menimbulkan pergeseran peradaban manusia, dari peradaban manual menjadi peradaban digital. Tentu saja hal tersebut juga memicu banyaknya data-data digital yang tercipta yang bisa kita *share* dengan mudah dan cepat melalui jaringan internet. Namun, hal tersebut menyebabkan sulitnya melakukan autentikasi data yang tersebar melalui internet, khususnya untuk gambar-gambar digital. Makalah ini ingin mencoba memperkenalkan cara baru untuk autentikasi gambar digital menggunakan kriptografi visual dan steganografi. Kriptografi visual adalah suatu cara penyandian sedemikian sehingga dekripsi pesan bisa dilakukan hanya dengan indera penglihatan manusia, tidak perlu menggunakan komputer. Sementara Steganografi adalah penyampaian pesan rahasia sedemikian sehingga orang tidak akan mencurigai adanya pesan rahasia yang terkandung dalam suatu data. Pembubuhan tanda tangan digital ini dilakukan dengan cara pembagian gambar yang menjadi tanda tangan ke dalam beberapa bagian menggunakan visual kriptografi dan menyisipkan satu bagian gambar tersebut ke dalam gambar yang dibubuhi tanda tangan dengan menggunakan steganografi.**

***Index Terms*—Tanda tangan digital, kriptografi visual, steganografi, gambar digital.**

## I. PENDAHULUAN

Pada era teknologi seperti saat ini, hampir semua bentuk fisik mulai muncul dalam bentuk digital. Buku, dokumen, dan surat yang awalnya beralaskan kertas sekarang muncul sebagai data digital. Seperti halnya yang terjadi dengan dokumen, gambar pun mulai muncul dalam bentuk gambar digital.

Gambar digital sudah menjadi hal yang umum saat ini. Ada banyak gambar digital yang di-share di internet, dengan berbagai macam ukuran dan bentuk. Dengan fenomena seperti itu, distribusi gambar menjadi lebih mudah dan cepat. Misalnya saja, kita bisa mempublikasikan gambar hasil buatan kita kepada banyak orang dalam jangka waktu yang relatif cepat dengan cara mendistribusikannya lewat internet, tidak perlu membuat pameran atau semacamnya.

Walaupun demikian, populernya gambar digital ini, selain membawa dampak positif, hal tersebut juga membawa dampak negatif. Salah satu dampak negatifnya adalah autentikasi kepemilikan suatu gambar digital. Dalam banyak kasus, suatu gambar sudah tidak bisa lagi dikenali siapa pemilik sebenarnya yang mengunggah gambar tersebut ke internet sehingga sulit untuk mengklaim gambar tersebut.

Tentu saja sudah ada beberapa cara yang biasanya dipakai untuk autentikasi kepemilikan dari suatu gambar digital, salah satunya adalah mendigitalisasi tanda tangannya. Beberapa orang mencoba membubuhkan tanda tangan atau tanda khusus pada gambarnya. Biasanya tanda tangan di-scan, kemudian ditambahkan ke gambarnya, seperti tanda tangan pelukis pada lukisan. Akan tetapi, cara seperti ini kuran efektif karena tanda tangan yang dibubuhkan langsung seperti itu sangat mudah untuk dihapus menggunakan teknologi yang ada sekarang.

Beberapa mencoba membubuhkan tanda tangannya menggunakan watermarking, akan tetapi, dengan kecanggihan teknologi sekarang, gambar-gambar watermarking itu masih bisa dengan mudah dihapus, misalnya menggunakan Photoshop.

Oleh sebab itu, kita perlu memikirkan cara baru yang lebih efektif untuk membubuhkan "tanda tangan" kita ke gambar-gambar digital sehingga autentikasi gambar digital bisa dengan mudah dilakukan dan aman dari plagiarisme.

## II. KRIPTOGRAFI VISUAL

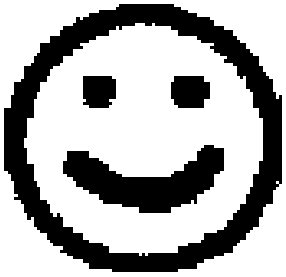
### *A. Definisi Kriptografi Visual*

Kriptografi Visual adalah teknik kriptografi yang memungkinkan dienkripsinya informasi visual (seperti gambar, teks, dan semacamnya) dengan yang unik. Keunikan dari cara tersebut adalah bahwa dekripsinya dapat dilakukan dengan menggunakan sistem visual manusia, tanpa bantuan komputer.

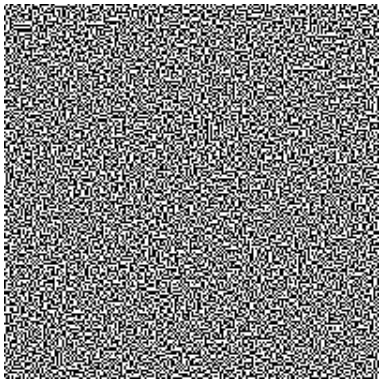
Kriptografi visual ini dikembangkan pertama kali oleh Moni Naor dan Adi Shamir pada tahun 1994. Mereka mendemonstrasikan sebuah skema sharing visual rahasia yang gambarnya dipecah menjadi n bagian sehingga hanya seseorang yang memiliki n bagian tersebut yang

bisa mendeskripsi gambar. Jika kurang 1 gambar saja, maka gambar tidak akan bisa didekripsi.

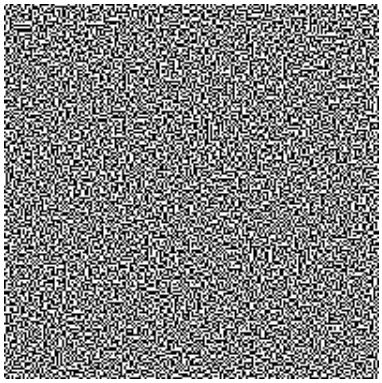
Seperti yang telah disebutkan, cara dekripsi dari kriptografi visual ini sangat unik karena dapat dilakukan hanya dengan mengandalkan indera penglihatan manusia saja. Cara enkripsinya adalah setiap bagian dimasukkan ke transparansi yang berbeda dan dekripsi dilakukan dengan menumpuk setiap bagian gambar tersebut. Untuk mendekripsinya, kita hanya perlu menumpuk semua bagian gambarnya saja. Ketika semua gambarnya ditumpuk, maka gambar aslinya akan terlihat.



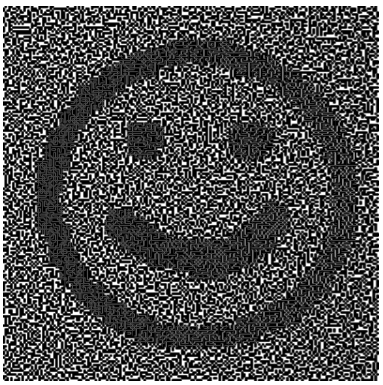
Gambar 1 – Gambar Asli



Gambar 2 – Share 1



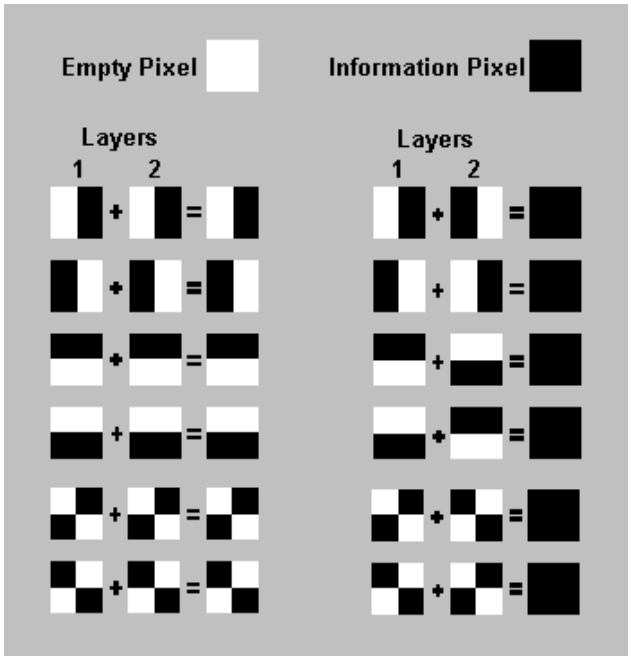
Gambar 3 – Share 2



Gambar 4 – Hasil Dekripsi

### *B. Skema Dasar Visual Kriptografi*

Seperti yang terlihat pada gambar di atas, untuk melakukan enkripsi pada kriptografi visual, setiap pixel pada gambar akan dibagi ke dalam blok-blok kecil. Biasanya jumlah blok putih dan jumlah blok hitam selalu sama. Jika sebuah pixel dibagi menjadi dua bagian, maka akan ada sebuah blok putih dan sebuah blok hitam. Jika pixel dibagi menjadi empat bagian, maka akan ada dua blok putih dan dua blok hitam. Demikian seterusnya. Untuk lebih jelasnya, perhatikan gambar di bawah ini.




Gambar 5 – Skema Kriptografi Visual

Pada gambar di atas, kita bisa melihat bahwa jika sebuah pixel dibagi menadi empat bagian, maka kita akan mendapatkan enam *state* yang berbeda. Jika sebuah pixel di layer 1 menggunakan salah satu state, maka pixel di layer 2 memiliki dua kemungkinan pilihan state : sama dengan layer 1 atau merupakan kebalikan dari layer 1. Jika pixel pada layer 2 sama dengan layer 1, maka pixel hasil penumpukkan akan menjadi setengah hitam dan setengah putih. Hasil pixel penumpukkan seperti itu

dinamakan abu-abu atau kosong. Jika pixel pada layer 1 dan 2 berkebalikkan, maka hasil penumpukkannya akan hitam semua. Hasil penumpukkan ini dinamakan pixel informasi. Pixel yang bisa dijadikan kriptografi visual tentu saja adalah pixel informasi.

Untuk membagi pixel tersebut, ada berbagai macam cara, misalnya membagi dua kiri dan kanan, atau atas dan bawah. Kita juta bisa membaginya menjadi 4 bagian dengan putih dan hitam terletak diagonal. Untuk meningkatkan keamanan, sebaiknya pembangkitan tata letak dilakukan secara acak. Selain itu, penggunaan 4 bagian lebih aman dibandingkan hanya 2 bagian.

## III. STEGANOGRAFI

### *A. Definisi Steganografi*

Steganografi merupakan gabungan antara seni dan sains dalam membuat pesan tersembunyi dengan cara sehingga tidak ada orang, baik pengirim maupun penerima, mencurigai adanya pesan yang disembunyikan. Kata steganografi berasal dari bahasa Yunani *steganos* yang berarti "disembunyikan" dan *graphei* yang berarti "tulisan".

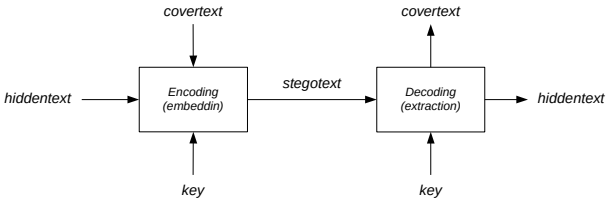
Keuntungan dari steganografi, dibandingkan dengan kriptografi, adalah bahwa pesan tersembunyi tersebut tidak akan menimbulkan kecurigaan. Teks yang dienkripsi menggunakan kriptografi, tidak peduli betapa kuatnya algoritma yang digunakan, akan muncul sebagai deretan sandi yang menimbulkan kecurigaan. Maka dari itu, biasanya kita menggunakan kriptografi untuk menjaga isi dari pesan tersebut, dan steganografi untuk menjaga pengiriman secara tersembunyi antara pengirim dan penerima.

Sejak pertama kali digunakan, sudah berkembang berbagai macam cara steganografi, salah satunya adalah steganografi digital yang menggunakan data digital dan enkripsi dilakukan menggunakan komputer. Steganografi digital bisa digunakan untuk berbagai macam data digital, misalnya teks, audio, gambar, maupun video.

### *B. Skema Dasar Steganografi*

Dalam steganografi sendiri, terdapat beberapa properti yang diperlukan, yaitu :

- *Embedded message (hiddentext)* : merupakan pesan yang akan disembunyikan. Pesan tersembunyi ini bisa berbentuk teks, gambar, audio, video, dan lain-lain. Dalam kasus kali ini, yang akan kita gunakan lebih kepada gambar.
- *Cover-object (covertext)* : merupakan pesan yang digunakan untuk menyembunyikan embedded message. Pesan ini bisa berupa teks, gambar, audio, video, dan lain-lain walaupun dalam makalah kali ini kita akan lebih membahas yang gambar.
- *Stego-object (stegotext)* : merupakan pesan yang sudah berisi pesan tersembunyi (*embedded message*).
- *Stego-key* : merupakan kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari stegotext.



Gambar 6 – Skema Umum Steganografi

Cara yang digunakan untuk bisa menyisipkan gambar ke dalam gambar dalam steganogrfi ada bermacam-macam, salah satunya adalah dengan memanfaatkan *Least Significant Bit* (LSB).

Jika menggunakan LSB, tentu saja kita perlu mengubah gambar, baik gambar yang akan disembunyikan maupun gambar yang menjadi *cover* ke dalam bentuk bit. Kemudian, untuk setiap byte pada gambar cover, untuk LSBnya akan diganti menggunakan bit dari gambar yang akan disembunyikan.

Contohnya jika kita ingin menyisipkan pada citra 24-bit. Setiap pixel panjangnya 24 bit, yaitu 3x3 byte, masing-masing komponen warna meran (R) 1 byte, hijau (G) 1 byte, dan biru (B) 1 byte.

00110011 10100010 11100010
(misal *pixel* berwarna merah)

Kemudian kita ingin memasukkan *embedded message* 010, maka hasilnya akan menjadi :

00110010 10100011 11100010

Walaupun diganti, karena yang diganti merupakan LSB, jika hanya menggunakan indera penglihatan manusia maka tidak akan terlihat adanya perbedaan.

Untuk memperkuat steganografinya, kita bisa menggunakan pembangkit bilangan acak untuk mengacak susunan bit yang kita sisipkan sehingga lebih sulit untuk dilacak.

Gambar 7 – Contoh Cover Image

Gambar 8 – Contoh Embedded Image

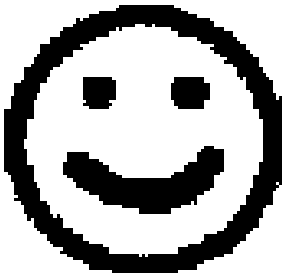
Gambar 9 – Contoh Hasil Steganografi

## IV. IMPLEMENTASI

Seperti yang telah dijelaskan di atas, pembuatan tanda tangan digital menggunakan cara yang biasa terlalu rentan. Tanda tangan hanya berupa sederetan kode yang bisa diubah atau dihapus dengan mudah. Tanda tangan digital yang biasa memang lebih cocok untuk pemeriksaan apakah data sudah diubah oleh orang lain atau belum, tetapi tidak bisa digunakan secara efektif sebagai autentikasi dari sebuah data karena tanda tangan digital seperti itu mudah diubah atau dihilangkan. Pada akhirnya, dalam kasus pada makalah ini, jika menggunakan tanda tangan digital yang biasa untuk autentikasi sebuah gambar, tanda tangan tersebut dapat dengan mudah diganti dengan tanda tangan digital milik orang lain sehingga kita tidak bisa lagi mengklaim gambar tersebut adalah milik kita.

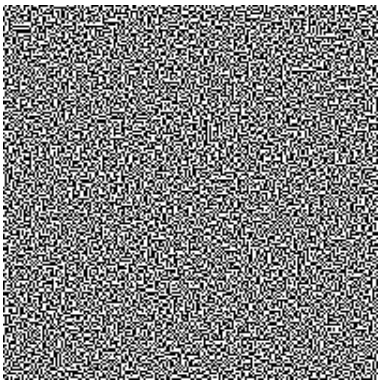
Untuk kasus seperti ini, penulis ingin mengusulkan cara baru untuk membuat tanda tangan digital untuk gambar, yaitu menggunakan cara kriptografi visual dan steganografi.

Pada mulanya, siapkan tanda tangan berupa gambar yang menunjukkan tanda tangan atau ciri khas yang ingin kita sisipkan ke dalam gambar yang kita miliki. Contohnya :

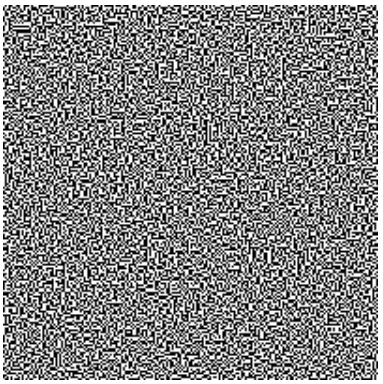


Gambar 10 – Gambar yang akan disisipkan

Kemudian, enkripsi gambar tersebut menggunakan kriptografi visual menjadi dua bagian gambar.



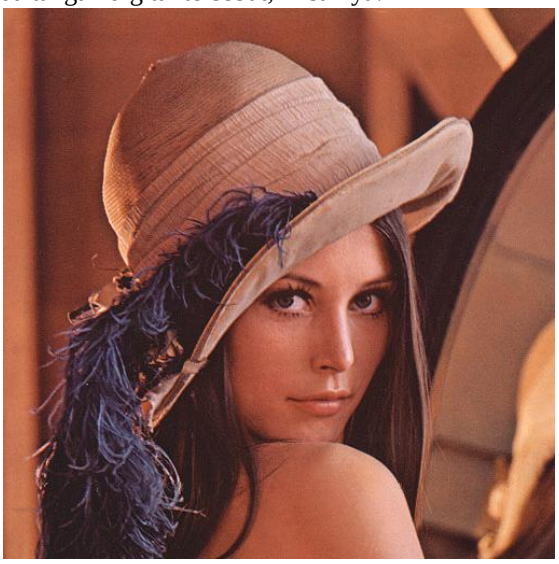
Gambar 11 – Share 1



Gambar 12 – Share 2

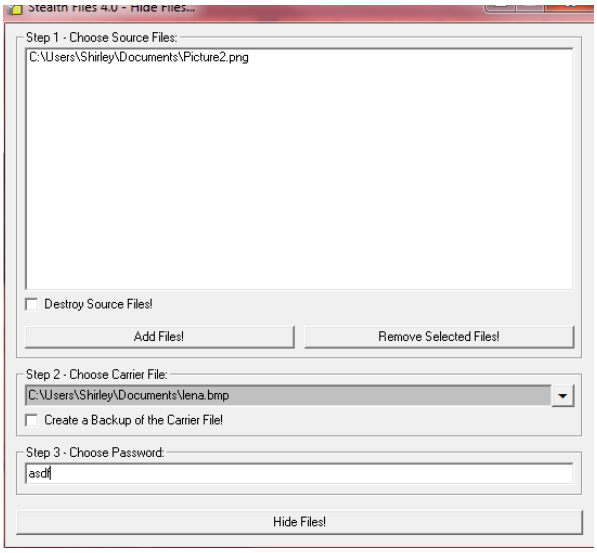
Gambar Share 1 adalah gambar yang akan kita sisipkan

sebagai tanda tangan digital pada gambar tersebut. Sedangkan Share 2 adalah gambar yang akan kita simpan sebagai alat untuk autentikasi gambar tersebut. Setelah kita mendapatkan kunci dan tanda tangan digitalnya, maka kita perlu menetapkan gambar yang ingin kita sisipkan tanda tangan digital tersebut, misalnya:



Gambar 13 – Gambar yang akan dibubuhi

Kemudian gambar Share 1 pun disisipkan ke dalam gambar cover menggunakan steganografi LSB 1 bit dengan menggunakan kunci asdf.




Gambar 14 – Screenshot Program

Gambar 15 – Gambar Hasil Pembubuhan Tanda Tangan Digital

## V. ANALISIS

### *A. Hasil*

Jika hasilnya dilihat secara sekilas menggunakan indera penglihatan manusia saja, tidak akan terlihat perbedaan yang dihasilkan dengan pembubuhan tanda tangan tersebut. Akan tetapi, jika gambar tersebut diekstrak, maka akan terlihat adanya gambar bagian share kriptografi visual dari gambar yang kita jadikan tanda tangan atau ciri khas kita.

Walaupun memang *noise* yang terjadi relatif sedikit sehingga sulit terdeteksi, cara ini memiliki beberapa kelemahan, antara lain besarnya gambar yang menjadi tanda tangan digital kita tidak boleh terlalu besar. Cara ini menggunakan steganografi dengan memanfaatkan LSB, sehingga gambar yang akan disisipkan harus memiliki ukuran jauh lebih kecil daripada gambar yang disisipi. Jika gambar yang disisipkan (dalam kasus ini adalah gambar yang menjadi tanda tangan kita) lebih besar daripada gambar yang dibubuhi tanda tangan, maka *noise* yang terjadi akan besar dan akhirnya dapat dideteksi oleh mata manusia.

### *B. Perbandingan dengan Tanda Tangan Digital Menggunakan Kode*

Jika kita membandingkan cara ini dengan tanda tangan digital pada umumnya, kita bisa mendapatkan beberapa keuntungan.

Keuntungan pertama dari cara ini adalah cara ini lebih sulit untuk dideteksi dan dihapus. Jika menggunakan cara tanda tanda tangan digital yang biasa, kita cukup mencari tag tanda tangan digitalnya dalam data gambar tersebut, kemudian menghapusnya atau menggantinya dengan tanda tangan yang lain. Jika menggunakan cara ini, akan lebih sulit untuk melacak adanya tanda tangan digital, karena tanda tangan tersebut disisipi didalam bit-bit gambar

tersebut. Selain itu, kalaupun dapat dideteksi adanya tanda tangan tersebut, akan sulit untuk menghapusnya karena letak bit yang disisipkan tersebar dengan urutan yang tidak diketahui oleh penyerang.

Keuntungan yang kedua adalah walaupun mungkin penyerang berhasil merubah sedikit bagian dari tanda tangan digital kita, karena tanda tangan digital tersebut merupakan gambar yang dienkripsi menggunakan kriptografi visual, maka walaupun sudah berubah sedikit, tetapi ketika dicocokkan dengan kunci yang kita pegang, gambar tanda tangan kita akan tetap terlihat. Dengan demikian, kepemilikan gambar tetap bisa dipertahankan.

Walaupun cara ini memiliki keuntungan dibandingkan dengan cara biasa, tetapi cara ini juga memiliki kelemahan, yaitu lebih sulit digunakan jika untuk verifikasi data. Cara ini lebih tepat digunakan untuk autentikasi data, bukan untuk verifikasi karena dengan penggunaan kriptografi visual, maka jika terjadi perubahan, jika perubahan tersebut hanya sedikit, maka perubahan tersebut tidak akan terlihat. Dengan demikian, cara ini tidak cocok untuk digunakan sebagai verifikasi.

## VI. KESIMPULAN

Kesimpulan yang dapat diambil dari penggunaan Kriptografi Visual dan Steganografi untuk tanda tangan digital ini adalah :

- Tanda tangan yang dibubuhkan hanya bisa berupa gambar karena untuk enkripsi tanda tangannya menggunakan kriptografi visual.
- Pembubuhan tanda tangan dengan cara ini hanya cocok digunakan sebagai alat untuk autentikasi data, bukan untuk verifikasi data.
- Pembubuhan tanda tangan dengan cara ini hampir tidak terdeteksi dengan indera penglihatan manusia biasa.
- Gambar yang digunakan sebagai tanda tangan harus berukuran jauh lebih kecil daripada gambar yang dibubuhi tanda tangan untuk menghindari terjadinya *noise* yang terlalu besar.
- Pembubuhan tanda tangan menggunakan cara ini lebih sulit untuk diserang dibandingkan dengan cara tanda tangan digital biasa.

## REFERENCES


[1] Munir, Rinaldi, (2011), Bahan Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika, Institut Teknologi Bandung.

[2] Naor, Moni, Shamir, Adi, Visual Cryptography Visual Cryptography, 1998.

[3] http://homes.esat.kuleuven.be/~fvercaut/talks/visual.pdf

[4] http://www.strangehorizons.com/2001/20011008/steganography.shtml

[5] http://www.fileguru.com/apps/visual_cryptographic_steganography_in_images


## 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, 9 Mei 2011

Shirley - 13508094