# APLIKASI VIDEO STEGANOGRAPHY DENGAN METODE *LEAST SIGNIFICANT BIT* (LSB)

Dian Dwi Hapsari, Lintang Yuniar Banowosari
*Universitas Gunadarma*
dhe.dee29@yahoo.com, lintang@staff.gunadarma.ac.id

**ABSTRACT**

*Message sent by someone is expected to not to be read by other unrelated people. The content can include secret and privacy materials. For that reason, the sender often sends the message in a hidden way. To solve such problem, a video steganography, which can ensure the security of the message sent, is developed by incorporating a message within a video file. This application is developed based on the LSB method by modifying LSB bits in each byte in the file. The steps of the development process include application design, application implementation, application testing, and application analysis. Tools used in the development include Java System Development Kit (J2SDK) programming version 1.4.2_03 and Edit Plus software for coding purpose. The testing process is conducted for the embedding and retrieving processes. The steganography application can read video files with types of 3gp, avi, flv, and mpeg and hide message in the form of images, texts, videos, and documents. There are a number of rooms for improvement, since some facilities have not been developed.*

***Keywords:*** *Steganography, Least Significant Bit (LSB), Embedding, Retrieving.*

## 1. Pendahuluan

### 1.1 Latar Belakang Masalah

Seringkali seseorang yang hendak mengirim pesan kepada orang lain, tidak ingin isi pesan tersebut diketahui oleh orang lain. Biasanya isi pesan tersebut bersifat sangat rahasia atau pribadi, yang hanya boleh diketahui antara pihak pengirim dan pihak penerima pesan, atau kalangan terbatas saja. Oleh karena itu, biasanya pengirim tersebut mengirim pesan secara sembunyi-sembunyi agar tidak ada pihak lain yang mengetahui.

Walaupun seringkali dilakukan dengan sembunyi-sembunyi tetapi tetap saja pesan tersebut dapat diketahui oleh orang lain ataupun karena mungkin adanya suatu hambatan atau masalah seperti misalnya media pesannya berupa kertas dan kertas tersebut jatuh di jalan atau rusak terkena air. Hal-hal seperti itu membuat orang yang mengirim pesan rahasia tersebut semakin lama semakin malas atau lelah untuk melakukannya dan menginginkan sesuatu yang lebih aman dan mudah untuk mengirim pesan tersebut.

Salah satu hal yang dapat dilakukan untuk mengatasi situasi di atas adalah mengembangkan suatu aplikasi yang mampu menyamarkan pesan tersebut pada suatu media yang dapat diakses oleh setiap orang. Teknik ini disebut steganografi, setiap orang bisa menampilkan atau membuka media tersebut, namun tidak menyadari bahwa media tersebut telah dibubuhkan pesan rahasia oleh pengirim.

Sudah banyak penulisan ataupun artikel yang membahas steganografi, tetapi kebanyakan membahas steganografi pada citra dan audio. Sudah banyak metode yang dilakukan untuk steganografi pada citra dan audio ini dan sudah banyak pula metode steganografi yang digunakan untuk mendeteksinya, sedangkan yang membahas steganografi pada video sangat jarang karena menggabungkan steganografi pada citra dan audio, pada dasarnya video merupakan gabungan citra yang "bergerak" dan audio, yang lebih sulit dideteksi.

Dalam penulisan ini, penulis akan mengembangkan program steganografi yang mampu menyembunyikan informasi rahasia di dalam media video. Media video yang digunakan berformat avi, 3gp, flv, dan mpeg.

Tujuan penelitian ini adalah untuk mengembangkan aplikasi video steganografi yang dapat memberikan keamanan pada suatu informasi rahasia dengan menyembunyikannya dalam file video menggunakan bahasa pemrograman Java.

## 2. Landasan Teori

### 2.1 Steganografi

Kata steganografi berasal dari bahasa Yunani yaitu steganos yang berarti penyamaran atau penyembunyian dan graphein atau graptos yang berarti tulisan sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia (informasi) tertulis ke dalam pesan lain dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut.

Meskipun memiliki tujuan yang sama dengan kriptografi, keduanya merupakan hal berbeda. Pada kriptografi informasi diamankan sedemikian rupa sehingga orang lain tidak mengenali informasi tersebut, sedangkan steganografi menyembunyikan informasi sedemikian rupa sehingga tidak disadari keberadaannya oleh orang lain. Satu hal yang

menjadi kelebihan dari steganografi adalah kemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi di dalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya.

### 2.2 Least-Significant Bit Modification

Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan *Least Significant Bit* (LSB). Walaupun banyak kekurangan pada metode ini, tetapi kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang. Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada stego, harus digunakan format lossy compression, karena metode ini menggunakan bit-bit pada setiap piksel pada citra. Jika digunakan format *lossy compression,* pesan rahasia yang disembunyikan dapat hilang.

## 3. Metode Penelitian

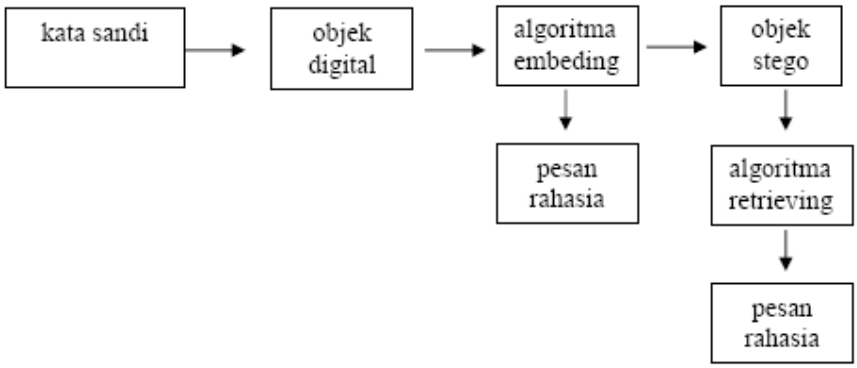
Pendekatan yang digunakan untuk melakukan penyembunyian informasi adalah pendekatan *Least Significant Bit* (LSB). Adapun untuk membuat aplikasi ini, diperlukan tahapan-tahapan agar dapat mencapai tujuan penelitian. Tahapan pembuatan aplikasi yang dilakukan adalah perancangan aplikasi, pemrograman dengan bahasa pemrograman Java, uji coba program, dan analisis hasil.

Aplikasi steganografi ini menggunakan bahasa pemrograman Java. Dalam menuliskan program Java dibutuhkan *tools* agar program Java dapat dibuat, diuji, dijalankan, dan didokumentasikan. Untuk itu penulis menggunakan Java 2 System Development Kit (J2SDK) versi 1.4.2_03 dan perangkat lunak Edit Plus untuk mengimplementasikan koding program.

## 4. Steganografi dengan LSB

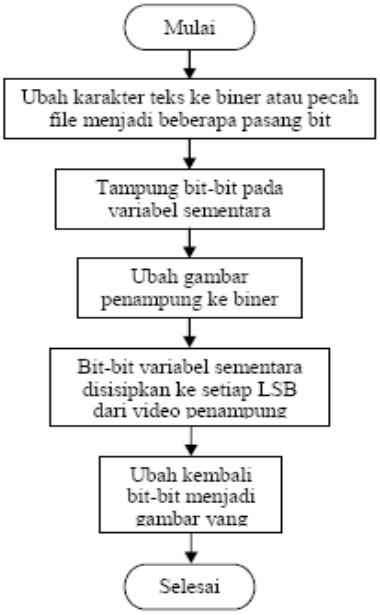
### 4.1 Gambaran Umum Program

Secara umum program steganografi ini digunakan untuk menyembunyikan suatu data atau informasi ke dalam sebuah media sehingga sulit dideteksi keberadaan data atau informasi tersebut karena hasil dari penyembunyian tersebut tidak berbeda dengan sumbernya. Media yang digunakan dalam penulisan ini adalah objek digital berupa file video. Setelah media tersebut ditentukan, data atau informasi tersebut baru dapat disisipkan atau disembunyikan ke dalam media tersebut. Gambar 1 dapat memperlihatkan gambaran umum proses steganografi.



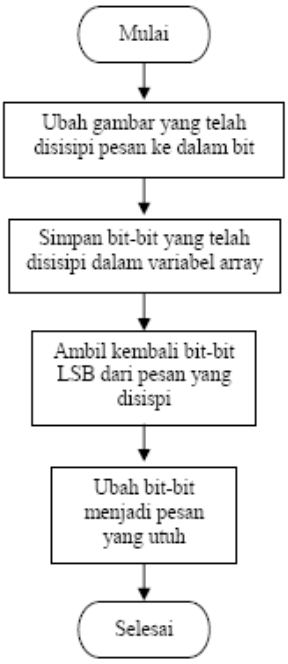

Gambar 1. Struktur Sistem Steganografi

Untuk menyisipkan informasi atau data rahasia ke dalam objek digital diperlukan suatu algoritma yang disebut dengan algoritma *embedding*. Gambar 2 memperlihatkan proses dari algoritma embedding. Algoritma tersebut dapat memodifikasi objek digital sehingga menghasilkan objek digital baru yang berisi informasi tersembunyi. Dalam proses modifikasi, perubahan yang terjadi antara objek digital (media asli) dengan objek digital baru hasil modifikasi media tidak boleh terlalu terlihat perbedaannya.




Gambar 2. Diagram Alur Proses pada Algoritma *Embedding*

Kemudian untuk mengambil data rahasia yang telah disisipkan di dalam objek stego, dibutuhkan suatu algoritma yang disebut dengan algoritma_retrieving. Proses pada algoritma retrieving dapat dilihat pada Gambar 3. Algoritma retrieving ini adalah kebalikan dari algoritma embedding. Algoritma retrieving digunakan untuk mengambil atau mengembalikan data atau informasi dari file video tersebut. Algoritma steganografi ini memodifikasi beberapa pixel yang terdapat di dalam file video untuk dimasukkan informasi baru kedalamnya.

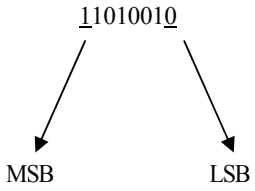



Gambar 3. Diagram Alur Proses pada Algoritma Retrieving

**4.2. Teknik Steganografi dengan LSB**

Teknik Steganografi Modifikasi LSB dilakukan dengan memodifikasi bit-bit yang termasuk bit LSB pada setiap byte warna pada sebuah pixel. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit-bit informasi lain yang ingin disembunyikan. Setelah semua bit informasi lain menggantikan bit LSB di dalam file tersebut, maka informasi telah berhasil disembunyikan. Ketika informasi rahasia tersebut ingin kembali dibuka, maka

bit-bit LSB yang sekarang ada, diambil satu per satu kemudian disatukan kembali menjadi sebuah informasi yang utuh seperti semula. Penentuan bit-bit LSB dilakukan secara berurutan, mulai dari byte awal sampai byte terakhir sesuai panjang dari data rahasia yang akan disembunyikan.




Gambar 4. MSB dan LSB

Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya tidak berpengaruh terhadap persepsi visual/auditori. Contoh Penggunaan Metode LSB pada tahap *encode*:

1. Misalkan penyisipan pada citra 24-bit. Setiap pixel panjangnya 24 bit (3 x 3 byte, masing-masing komponen R (1 byte), G (1 byte), dan B (1 byte)).
   00110011 10100010 11100010 (misal pixel berwarna merah)

   Misalkan *embedded message*: 010
   Encoding: 00110010 10100011 11100010
   (pixel berwarna "merah berubah sedikit", tidak dapat dibedakan secara visual dengan citra aslinya).

2. Jika pesan = 10 bit, maka jumlah byte yang digunakan = 10 byte
   00110011 10100010 11100010 10101011 00100110
   10010110 11001001 11111001 10001000 10100011

   Pesan: 1110010111
   Hasil penyisipan pada bit LSB:
   00110011 10100011 11100011 10101010 00100110
   10010111 11001000 11111001 10001001 10100011

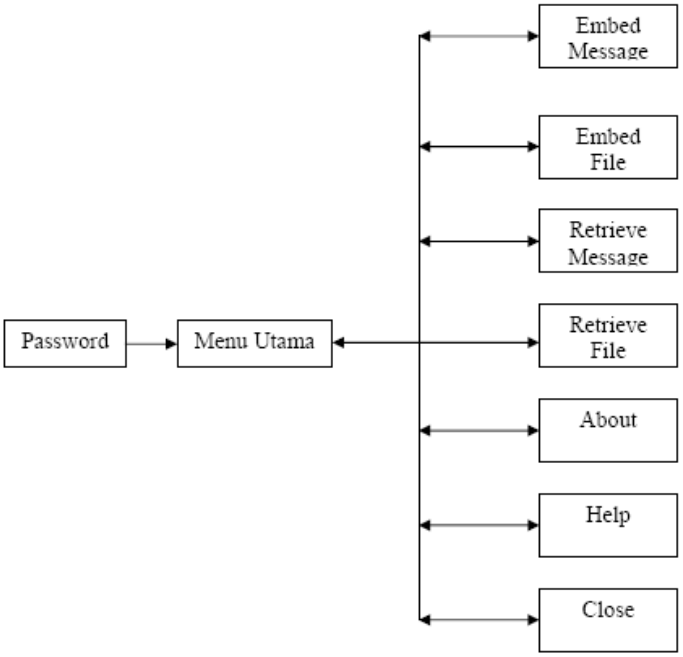
**4.3 Perancangan Program**

**4.3.1 Struktur Navigasi**

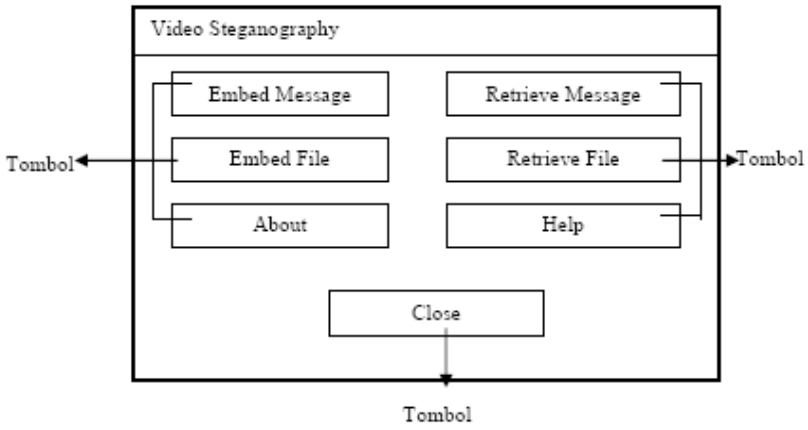
Struktur navigasi aplikasi ini mempunyai 9 halaman. Halaman Password merupakan tampilan awal dalam program ini seperti pada gambar 6. Jika password yang diinput sesuai dengan password dalam program ini maka pemakai dapat masuk ke halaman Menu Utama. Selanjutnya di dalam halaman Menu Utama terdapat tombol-tombol yaitu Embed_Message yang digunakan untuk menyembunyikan pesan berupa teks dan akan menuju ke halaman Embed_ Message, Embed_ File digunakan untuk menyembunyikan pesan berupa file dan akan menuju ke halaman Embed_File. Retrieve_Message digunakan untuk menampilkan informasi atau pesan rahasia berupa teks dan akan menuju ke halaman Retrieve_Message. Retrieve_File digunakan untuk menampilkan informasi atau pesan rahasia berupa file dan akan menuju ke halaman Retrieve File, About yang akan menuju ke halaman About, Help yang menuju ke halaman Help dan Close yang digunakan untuk keluar dari aplikasi ini. Hal tersebut dapat dilihat pada Gambar 5.

**4.3.2 Perancangan Tampilan Program**

Pada halaman menu utama terdapat 7 tombol seperti yang terlihat pada Gambar 5 dan 6 yaitu tombol_Embed_Message yang digunakan untuk menampilkan halaman Embed_Message, tombol_ Embed_File_ yang digunakan untuk menampilkan halaman tombol_ Embed_File, tombol Retrieve_Message digunakan untuk menampilkan halaman Retrieve_Message, tombol Retrieve_File digunakan untuk menampilkan halaman Retrieve_Message, tombol About digunakan untuk menampilkan halaman About, tombol Help digunakan untuk menampilkan halaman Help yang berisi informasi tentang cara penggunaan aplikasi dan tombol Close yang digunakan untuk menutup dan mengakhiri dari aplikasi.




Gambar 5. Struktur Navigasi Program




Gambar 6. Menu Utama Program

**4.4 Uji Coba Program**

Untuk mengetahui sejauh mana keberhasilan program dalam memodifikasi video sebagai media penampung, maka dilakukan uji coba program supaya pada saat menyembunyikan dan mengembalikan pesan rahasia program dapat berjalan dengan efektif.

Dalam program ini, dilakukan uji coba berbagai format video. Format video yang digunakan dalam uji coba adalah avi, 3gp, flv, dan mpeg. Ternyata semua format video tetap tersimpan dalam format yang sama dan hasil dari embedding dan retrieving tidak merusak video. Secara garis besar pelaksanaan uji coba dibedakan dalam dua tahap yaitu tahap embedding dan tahap retrieving.

**4.4.1 Pengujian Tahap Embedding**

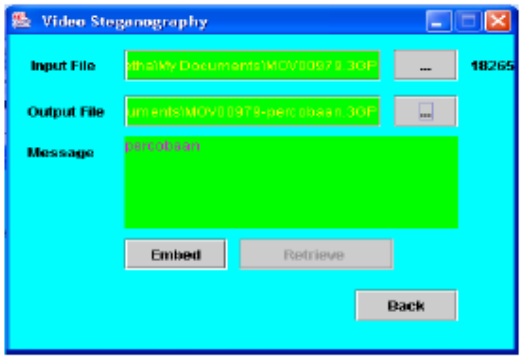
Dalam tahap ini, pengujian hanya dilakukan dalam lingkup proses penyisipan data. Beberapa masukan diperlukan untuk memulai proses penyisipan data, contoh tampilan program pada tahap ini dapat dilihat pada Gambar 6. Masukan yang diperlukan di antaranya adalah sebagai berikut:

1. Pengambilan Data Carier

Pengambilan data video yang akan berfungsi sebagai pembawa pesan rahasia dapat dilakukan dengan menggunakan tombol untuk mencari dalam bagian Input file.

2. Pengambilan Data Pesan Rahasia
Pengambilan data pesan rahasia sama halnya dengan pengambilan data pembawa, yaitu dengan menekan tombol untuk mencari pada bagian data file.

3. Hasil Keluaran Tahap Embedding
Untuk mendapatkan hasil keluaran tahap embedding, dilakukan dengan menentukan lokasi atau direktori dan nama file yang akan digunakan sebagai file keluaran tersebut dengan menekan tombol untuk mencari pada output file.




Gambar 7. Contoh Tampilan pada Proses Embedding

### 4.4.2 Pengujian Tahap Retrieving

Dalam tahap ini, pengujian hanya dilakukan dalam lingkup proses pengembalian data, contoh tampilan proses pada tahap ini dapat dilihat pada Gambar 7. Beberapa masukan diperlukan untuk memulai proses pengambilan data. Masukan yang diperlukan diantaranya adalah sebagai berikut:

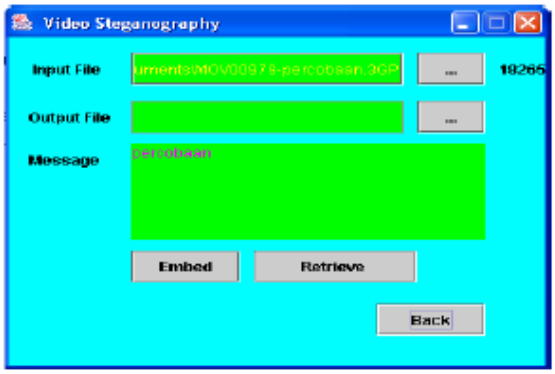
1. Pengambilan Data Carier
Pengambilan data pembawa pesan rahasia dapat dilakukan dengan menggunakan tombol untuk mencari dalam bagian Input File.

2. Hasil Keluaran Tahap Retrieving
Untuk mendapatkan hasil keluaran tahap retrieving, ialah dengan memilih tombol Retrieve.

## 5. Hasil

Dari hasil uji coba sebelumnya dengan format video avi, 3gp, flv, dan mpeg, didapatkan bahwa hasil yang didapat sesuai dengan apa yang diharapkan, yaitu program Steganografi ini dapat memenuhi tujuan, yaitu dapat memodifikasi media video yang di dalamnya terdapat pesan rahasia tanpa diketahui keberadaan pesan rahasia tersebut.

Walau terkadang terjadi hal yang tidak diinginkan, yaitu waktu yang dibutuhkan untuk melakukan proses terkadang lama, terlebih untuk memproses pesan rahasia yang besarnya hampir mendekati batas maksimum ukuran pesan rahasia yang dapat ditampung dan ukuran media penampung yang digunakan kurang dari 1000 MB.




Gambar 8. Contoh Tampilan pada Proses Retrieving

## 6. Penutup

Program aplikasi steganografi berjalan dengan baik dan berhasil menyisipkan data atau informasi rahasia ke dalam media penampung berupa video tanpa seseorang menyadari keberadaan data atau informasi di dalam video tersebut.

Data atau informasi yang telah disisipkan sebelumnya dapat diekstrak kembali, di mana proses penyisipan dan ekstraksi data membutuhkan waktu yang lebih lama apabila ukuran media penampung dan data atau informasi yang disisipkan dan diekstraksi besar.

Program aplikasi steganografi ini mampu membaca file video dengan tipe format 3gp, avi, flv, dan mpeg, serta dapat menyembunyikan pesan rahasia ke dalam media video dengan berupa gambar, teks, video, dokumen. Aplikasi ini dibuat agar dapat dikembangkan lagi. Dikarenakan aplikasi ini masih belum sempurna dan masih terdapat kekurangan-kekurangan yaitu salah satunya adalah informasi yang disimpan belum dapat lebih besar memorinya dari objek video itu sendiri.

Untuk pengembangan lebih lanjut dapat menggunakan metode lain yang lebih efisien dalam pemrosesannya sehingga proses steganografi yang dilakukan bisa lebih cepat dan dapat menampung banyak data atau informasi. Dari segi tampilan juga dapat dikembangkan menjadi lebih menarik dan untuk lebih mempersulit orang yang tidak dikehendaki dalam mendapatkan data atau informasi, alangkah baiknya sebelum dilakukan proses penyisipan, terlebih dahulu dilakukan proses enkripsi terhadap data atau informasi.

## Daftar Pustaka

[1] Kadir, A. (2004). *Dasar Pemrograman Java 2*. Yogyakarta: Andi Yogyakarta.
[2] Hermawan, B. (2004). *Menguasai Java 2 & Object Oriented Programming*. Jakarta.
[3] Sukmawan, B. (2008). *Steganografi*, http://students.ukdw.ac.id/~22033120/steganografi.html, diakses terakhir tanggal 02 Juni 2009
[4] Putut W, D. (2008). *Audio Steganografi*, http://images.doank29.multiply.com/attachment/0/Rkb9qgoKCp4AAEwAjaU1/Steganografi.doc?nmid=42039797, diakses terakhir tanggal 03 Juni 2009
[5] Henry. (2008). *Video Steganography*, http://budi.insan.co.id/courses/security/2006/henry_report.pdf, diakses terakhir tanggal 04 Juni 2009
[6] Hakim A, M. (2008). *Studi dan Implementasi Steganografi Metode LSB dengan Preprocessing Kompresi data dan Ekspansi Wadah*, http://www.informatika.org/~rinaldi/Kriptografi/2007-2008/Makalah1/MakalahIF5054-2007-A-077.pdf, diakses terakhir tanggal 05 Juni 2009
[7] Munir, R. (2008). *Steganografi dan Watermarking*, http://www.informatika.org/~rinaldi/Kriptografi/Steganografi%20dan%20Watermarking.pdf, diakses terakhir tanggal
[8] Soehono, S. (2006). *Audio Steganografi*, Bandung: Informatika Bandung.