ANALISIS PERBANDINGAN ANTARA HIBRID RSA DENGAN AMELSBR DAN HIBRID TRANSPOSISI KOLOM DENGAN AMELSBR

(Skripsi)

Oleh:

ARIF AL FURQON

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2018

ABSTRAK

ANALISIS PERBANDINGAN ANTARA HIBRID RSA DENGAN AMELSBR DAN HIBRID TRANSPOSISI KOLOM DENGAN AMELSBR

Oleh

ARIF AL FURQON

Teknologi membuat cara komunikasi menjadi lebih baik, tidak dibatasi oleh tempat dan waktu. Bentuk komunikasi yang sering digunakan adalah mengirim dan menerima pesan. Hal ini menuntut sistem keamanan yang kuat. Metode kriptografi merupakan salah satu cara pengamanan pesan dengan mengubah bentuk pesan sehingga sulit dipahami. Selain itu, metode steganografi merupakan cara untuk menyembunyikan pesan ke dalam media penampung. Kriptografi dan steganografi membuat keamanan suatu pesan lebih baik. Dalam penelitian ini dilakukan perbandingan antara kriptografi RSA *(Rivest Shamir Adleman)* dan kriptografi transposisi kolom yang disisipkan kedalam media penampung menggunakan steganografi AMELSBR (*Adaptive Minimum Error Least Significant Bit Replacement*), dengan media penampung berupa gambar dengan ekstensi .JPG sebgai *input* (*cover image*), dan menghasilkan *output* .JPG (*stegoimage*). Kesimpulan yang didapat dari penelitian ini adalah kedua metode kriptografi RSA dan Transposisi Kolom berhasil menyandikan pesan dan menyembunyikannya kedalam gambar menggunakan steganografi AMELSBR, serta berhasil mengembalikan dan mengubah pesan tidak beraturan kedalam pesan aslinya. *Ciphertext* transposisi kolom memiliki waktu lebih cepat saat proses penyisipan dan menghasilkan *stegoimage* yang lebih kecil dibandingkan *ciphertext* RSA. Tetapi *ciphertext* RSA lebih tahan terhadap perlakuan pemotongan gambar dibandingkan *ciphertext* transposisi kolom. Sebagian media sosial dapat mengirimkan *stegoimage* secara sempurna apabila tidak terdapat proses kompresi yang dilakukan.

Kata kunci : kriptografi, steganografi, RSA, transposisi kolom, AMELSBR, hibrid, JPG, *brightness*, *contrast*, *crop*, media sosial.

ABSTRACT

COMPARATIVE ANALYSIS BETWEEN THE RSA HYBRID WITH AMELSBR AND COLUMNAR TRANSPOSITION HYBRID WITH AMELSBR

By

ARIF AL FURQON

Technology makes communication a better way, not limited by time and place. The most common form of communication is sending and receiving messages. This demands a strong security system. Cryptography method is one way of securing the message by changing the shape of the message so it is difficult to understand. In addition, the steganography method is a way to hide messages into the container media. Cryptography and steganography make the security of a message better. In this study, the comparison between RSA cryptography (Rivest Shamir Adleman) and column transposition cryptography is inserted into the container media using AMELSBR steganography (Adaptive Minimum Error Least Significant Bit Replacement), with the image media extension .JPG as input (cover image) , and produce output. JPG (stegoimage). The conclusion of this research is that both RSA and Transposition cryptography methods have successfully encoded the message and hide it into the image using AMELSBR steganography, and successfully returned and changed the irregular message into the original message. Ciphertext columnar transposition have faster time during insertion process and result in smaller stegoimage than RSA ciphertext. But RSA ciphertext is more resistant to the image cropping treatment than ciphertext transposition column. Some social media can transmit stegoimage perfectly when no compression process is performed.

Kata kunci : cryptography, steganography, RSA, columnar transposition, AMELSBR, hybrid, JPG, brightness, contrast, crop, social media.

ANALISIS PERBANDINGAN ANTARA HIBRID RSA DENGAN AMELSBR DAN HIBRID TRANSPOSISI KOLOM DENGAN AMELSBR

Oleh :

ARIF AL FURQON

Skripsi

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
SARJANA KOMPUTER

pada

Jurusan Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam

JURUSAN ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
2018

Judul Skripsi	: **ANALISIS PERBANDINGAN ANTARA HIBRID RSA DENGAN AMELSBR DAN HIBRID TRANSPOSISI KOLOM DENGAN AMELSBR**
Nama Mahasiswa	: **ARIF AL FURQON**
No. Pokok Mahasiswa	: 1217051010
Jurusan	: Ilmu Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

Prof. Dra. Wamiliana, M.A., Ph.D.
NIP. 19631108 198902 2 001

Ardiansyah, M.Kom.

2. Mengetahui Ketua Jurusan Ilmu Komputer

Dr. Ir. Kurnia Muludi, M.S.Sc
NIP. 19640616 198902 1 001

MENGESAHKAN

1. Tim Penguji

   Ketua : **Prof. Dra. Wamiliana, M.A., Ph.D.** .....

   Sekretaris : **Ardiansyah, M.Kom.** .....

   Penguji
   Bukan Pembimbing : **Febi Eka Febriansyah, M.T.** .....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Prof. Warsito, S.Si., D.E.A., Ph.D.
NIP 19710212 199512 1 001

Tanggal Lulus Ujian Skripsi : 23 Februari 2018

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul "Analisis Perbandingan Antara Hibrid RSA dengan AMELSBR dan Hibrid Transposisi Kolom dengan AMELSBR" merupakan karya saya sendiri dan bukan karya orang lain. Semua tulisan yang tertuang di skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila dikemudian hari terbukti skripsi saya merupakan hasil penjiplakan atau dibuat orang lain, maka saya bersedia menerima sanksi berupa pencabutan gelar yang telah saya terima.

Bandar Lampung, Februari 2018

ARIF AL FURQON
NPM. 1217051010

RIWAYAT HIDUP

Penulis dilahirkan pada tanggal 23 Januari 1994 di Bandar Lampung, sebagai anak pertama dari empat bersaudara dari Ayah yang bernama Sumardi dan Ibu yang bernama Suprihatiningsih.

Pendidikan Taman Kanak-kanak (TK) Handayani diselesaikan tahun 1999, Taman Kanak-kanak (TK) Fitrah Insani diselesaikan tahun 2000, kemudian Sekolah Dasar (SD) Negeri 2 Gedong Air, Bandar Lampung diselesaikan pada tahun 2006, Sekolah Menengah Pertama (SMP) Negeri 1 Bandar lampung diselesaikan pada tahun 2009, Sekolah Menengah Atas (SMA) Negeri 2 Bandar Lampung diselesaikan pada tahun 2012.

Tahun 2012, penulis terdaftar sebagai mahasiswa Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Selama menjadi mahasiswa beberapa kegiatan yang dilakukan penulis antara lain:

1. Pada bulan Januari 2015 penulis melaksanakan Kuliah Kerja Nyata (KKN) di Desa Bumi Jaya, Kecamatan Negara Batin, Kabupaten Waykanan.
2. Pada bulan Juli 2015 penulis melaksanakan kerja praktek di PT. Lambang Jaya.

PERSEMBAHAN

Dengan mengucap puji dan syukur kehadiarat Allah SWT

kupersembahkan karya kecilku ini untuk:

Ayahanda Sumardi dan Ibunda Suprihatiningsih tercinta yang telah memberi dorongan, kasih sayang serta menjadi motivasi terbesarku selama ini

Nurul Alifia Anggun, Nurmanita Arianti dan Yusuf Ar-Rosis Pasha yang selalu menjadi acuanku untuk menjadi kakak yang lebih baik lagi

Dosen Pembimbing dan Penguji yang sangat berjasa

dalam membantu dan menyelesaikan karya kecil ini

Serta seluruh sahabat-sahabatku dan Almamaterku

yang kubanggakan Universitas Lampung

MOTO

“Pendidikan merupakan senjata paling ampuh yang bisa kamu gunakan untuk merubah dunia"

(Nelson Mandela)

“Semua impian kita bisa terwujud jika kita memiliki keberanian untuk mengejarnya”

(Walt Disney)

“Seseorang bisa duduk di tempat teduh sekarang, karena seseorang telah menanam pohon sejak lama”

(Warren Buffett)

SANWACANA

Alhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT atas berkatrahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan skripsi ini. Skripsi ini disusun sebagai syarat untuk memperoleh gelar Sarjana Komputer di Jurusan Ilmu Komputer Universitas Lampung.

Penyelesaian skripsi ini tidak terlepas dari bantuan banyak pihak yang sangat membantu, baik secara materi maupun moril dan juga saran serta bimbingan dari banyak pihak. Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Kedua orang tua tercinta, Ayah Sumardi dan Ibu Suprihatiningsih, serta adik-adikku Nuruf Alifia Anggun, Nurmanita Arianti, dan Yusuf Ar-Rosis Pasha yang selalu memberi dukungan berupa materi, doa, motivasi dan kasih sayang yang tak terhingga.
2. Ibu Prof. Dra. Wamiliana, M.A., Ph.D. sebagai pembimbing utama, yang telah membimbing penulis dan memberikan ide, kritik serta saran sehingga penulisan skripsi ini dapat diselesaikan.
3. Bapak Ardiansyah, M.Kom. sebagai pembimbing kedua, yang telah memberikan saran, bantuan, dan membimbing penulis sehingga penulisan skripsi ini dapat diselesaikan.
4. Bapak Febi Eka Febriansyah, M.T. sebagai pembahas, yang telah memberikan masukan yang bermanfaat dalam perbaikan skripsi ini.

5. Bapak Prof. Warsito, S.Si., D.E.A., Ph.D. selaku Dekan FMIPA Unila.
6. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc. selaku Ketua Jurusan Ilmu Komputer.
7. Bapak Didik Kurniawan, S.Si., M.T. selaku Sekretaris Jurusan Ilmu Komputer FMIPA Unila.
8. Bapak Dr. Eng. Admi Syarif selaku Pembimbing Akademik selama penulis menjadi mahasiswa Jurusan Ilmu Komputer Unila.
9. Ibu Ade Nora Maela dan Ibu Wiwik yang telah membantu segala urusan administrasi penulis di Jurusan Ilmu Komputer.
10. Roni Setiawan, Dwi Yatmoko Siambudi, Nikko Agustino Ito, Alfabet Setiawan, Afrizka Amidya, Anisa Putri, Gilang Persada Sebayang, Fajar Kurnia Pratomo, Randy Raharja Barlian, Nindia Dara Utama yang telah memberi dorongan, bantuan, serta motivasi untuk menyelesaikan skripsi ini.
11. Keluarga besar Ilmu Komputer teman seperjuangan dalam menuntut ilmu selama kuliah yang tidak bisa saya sebutkan satu-persatu.
12. Almamater Tercinta.

Semoga di balik kekurangan dan kelebihan skripsi ini dapat memberikan manfaat bagi semua pihak yang membutuhkan. Akhir kata, Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna. Untuk itu, Penulis mohon maaf atas segala kekurangan dan keterbatasan pada skripsi ini.

Bandar Lampung, Februari 2018

Penulis,

Arif Al Furqon

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR KODE

Halaman

BAB I

PENDAHULUAN

1.1. Latar Belakang

Berkembangnya teknologi membuat cara setiap individu berinteraksi berubah. Perubahan yang jelas terlihat adalah bentuk komunikasi. Mulanya seseorang harus bertatap muka secara langsung untuk melakukan proses komunikasi dengan lawan bicaranya. Tetapi, peran teknologi komunikasi memungkinkan proses komunikasi antara individu tidak harus dengan bertatap muka. Saat ini dengan berkembangnya teknologi, bentuk komunikasi yang sering digunakan adalah mengirim dan menerima pesan. Pada dasarnya bentuk komunikasi ini bertujuan untuk berinteraksi langsung dengan orang yang dituju, tetapi yang terjadi ada kemungkinan pesan yang dikirim tidak hanya diterima oleh orang yang dituju, melainkan orang lain yang tidak berhak. Dengan demikian, pesan yang bersifat rahasia dapat diketahui, dan ini menimbulkan kerugian dalam bentuk informasi. Untuk menghindari kemungkinan pesan dimengerti secara langsung dapat dilakukan dengan memodifikasi pesan, sehingga pihak lain tidak dapat mengerti pesan yang didapatkan secara langsung. Bentuk penanganan masalah keamanan informasi dan data ini adalah dengan menggunakan kriptografi.

Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan menyandikan informasi tersebut dengan suatu kunci khusus. Informasi ini sebelum disandikan dinamakan *plaintext*, dan setelah disandikan dinamakan *ciphertext*. Teknik kriptografi dapat mengubah pesan rahasia menjadi pesan acak (*ciphertext*) tidak bermakna sehingga pesan hanya dapat dibaca oleh pihak yang memiliki hak. Namun, kecurigaan akan timbul saat seseorang mengirimkan pesan secara acak kepada orang lain. Hal ini akan menimbulkan orang yang tidak berhak untuk mencari cara untuk mengartikan pesan acak tersebut.

Terdapat suatu teknik untuk melindungi pesan rahasia dari kecurigaan pelaku kejahatan dengan menggunakan steganografi. Steganografi merupakan teknik penyembunyian pesan rahasia kedalam media digital sehingga keberadaan pesan rahasia sulit untuk diketahui. Teknik ini sering dikenal dengan seni menyembunyikan informasi untuk mencegah pendeteksi pesan yang disembunyikan dengan cara menyisipkan pesan ke dalam media gambar, audio, dan lain sebagainya. Kelebihan yang dimiliki teknik steganografi terletak pada pesan yang tersembunyi di dalam suatu media penampung (*cover object*) dan tidak terlihat secara langsung sehingga mengurangi kecurigaan terhadap pesan. Namun, penggunaan teknik ini secara langsung pada pesan rahasia tidak menjamin pesan terlindungi dari pelaku kejahatan.

Cara yang dapat digunakan untuk permasalahan tersebut adalah dengan menggunakan kombinasi antara kriptografi dan steganografi. Teknik kriptografi

berperan untuk menyandikan pesan menjadi pesan acak (*ciphertext*) dan teknik steganografi berperan untuk menyisipkan pesan kedalam suatu media penampung (*cover object*).

Saat ini banyak berkembang algoritma kriptografi, contohnya adalah algoritma RSA. Algoritma ini merupakan algortima kriptografi asimetris yang memiliki dua kunci, yaitu kunci publik *(public key)* yang digunakan untuk proses enkripsi dan kunci rahasia *(private key)* yang digunakan untuk proses dekripsi. Algoritma RSA terdiri dari algoritma enkripsi dan dekripsi. Algoritma enkripsi RSA untuk menyandikan pesan menjadi bentuk yang tidak dimengerti maknanya, sedangkan algoritma dekripsi RSA untuk mengembalikan hasil penyandian menjadi pesan yang sebenarnya (Arifin dan Oktoviana, 2013).

Selain itu tedapat algoritma kriptografi tranposisi kolom yaitu algoritma yang melakukan perubahan urutan terhadap rangkaian karakter di dalam teks. Metode ini sering dikenal sebagai permutasi karena transpose setiap karakter di dalam teks sama dengan melakukan permutasi terhadap karakter-karakter tersebut. Algoritma transposisi kolom juga terdiri atas algoritma enkripsi dan dekripsi. Algoritma enkripsi transposisi kolom berguna untuk menyandikan pesan menjadi rangkaian yang tidak berurutan, dan sulit untuk mengetahui maknanya, sedangkan algoritma deskripsi transposisi kolom berguna untuk mengembalikan hasil penyandian menjadi pesan sebenarnya.

Proses enkripsi dan dekripsi yang terjadi pada algoritma kriptografi RSA dan algoritma kriptografi tranposisi kolom menjadikan kedua algoritma dapat dilakukan perbandingan. Proses perbandingan dilakukan ketika disisipkan ke dalam teknik steganografi menggunakan metode AMELSBR pada media penampung (*cover object*).

Pada penelitian sebelumnya Setiawan (2016) telah membahas Hibrid Transposisi Kolom dan AMELSBR menghasilkan sistem untuk menyandikan pesan rahasia menggunakan metode transposisi kolom serta menyembunyikan pesan ke dalam media penampung gambar dengan keluaran berupa file gambar dengan ekstensi file PNG (*Portable Network Graphics*). Selain itu, Ahmad (2016) membahas tentang Hibrid RSA dan AMELSBR menghasilkan sistem untuk menyandikan pesan rahasia menggunakan metode RSA serta menyembunyikannya ke dalam media penampung gambar dengan hasil keluaran file berupa gambar ekstensi file PNG (*Portable Network Graphics*). Berdasarkan kedua penelitian tersebut maka dapat dilakukan beberapa analisis untuk mengetahui keunggulan setiap metode pada penyisisipan menggunakan media gambar.

Media gambar (*cover image)* yang digunakan dua penelitian sebelumnya adalah gambar berformat JPG, sedangkan untuk media gambar hasil penyisipan berupa gambar berformat PNG. Dengan adanya perbedaan format gambar antara input dan output akan membuat kecurigaan apabila digunakan dalam berbagi gambar menggunakan media pengiriman gambar atau media *chatting*. Gambar berjenis JPG lebih sering diunggah ke media internet seperti foto-foto yang diambil dari

kamera digital berjenis JPG dan format jenis ini juga dapat mengurangi kecurigaan apabila gambar tersebut telah disisipkan pesan rahasia.

Teknik steganografi yang diimplementasikan adalah metode *AMELSBR (Adaptive Minimun Error Least Significant Bit Replacement)*. Dalam metode ini penyisipan pesan dilakukan dengan beberapa tahap yaitu *Capacity Evaluation, Minimun-Error Replacement* dan *Error Diffusion*. Ketiga tahap tersebut mempunyai fungsi yang berbeda-beda dan saling berhubungan satu dengan yang lainnya. Sifat dari metode *AMELSBR* beradaptasi dengan karakteristik lokal dan media penampung sehingga tidak menimbulkan distorsi yang berlebihan pada citra penampung yang telah disisipkan data digital rahasia (Prayudi dan Kuncoro, 2005).

Berdasarkan gagasan dan hasil penelitian sebelumnya, pada penelitian ini akan dilakukan perbandingan kedua metode kriptografi transposisi kolom dan RSA saat dilakukan penyisipan menggunakan metode steganografi AMELSBR dengan media penampung (*cover image)* berupa gambar sebelum penyisipan berjenis JPG dan setelah penyisipan juga tetap menghasilkan gambar berjenis JPG.

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana perbandingan hasil ekripsi dan dekripsi pada algoritma RSA dan transposisi kolom.
2. Bagaimana perbandingan hasil file penyisipan algoritma RSA dan tranposisi kolom pada penyisipan media menggunakan algoritma AMELSBR.
3. Bagaimana perbandingan kondisi pesan hasil dekripsi algoritma RSA dan tranposisi kolom setelah disisipkan pada media penampung (*cover object*) yang diberikan beberapa perlakuan.
4. Bagaimana kondisi pesan setelah dilakukan pengiriman melalui berbagai media pengiriman data.

1.3. Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Data yang digunakan berupa teks yang sama dengan format (*.txt).
2. Teks yang akan dienkripsi berupa angka, huruf atau simbol yang dikenal pada table ASCII (*American Standard Code for Information Interchange*).
3. Media penampung (*cover object*) yang digunakan adalah gambar yang sama dengan format (*.jpg) sebagai format *input* dan *output*.
4. Implementasi teknis *steganografi* tidak menggunakan *stego key*.
5. Proses enkripsi dan dekripsi menggunakan algoritma kriptografi RSA dan tranposisi kolom.

6. Media penampung pada hasil penyisipan diberikan perlakuan perubahan *brightness*, *contrast* dan pemotongan (*cropping*).

1.4. Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah untuk membandingkan teknik *kriptografi* dari algoritma RSA dan algoritma tranposisi kolom setelah dilakukan penyisipan pada media gambar menggunakan teknik *steganografi* AMELSBR.

1.5. Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Memberikan informasi tentang perbandingan algoritma kriptografi transposisi kolom dan kriptografi RSA saat penyisipan kedalam *cover image* menggunakan *plaintext* yang sama.
2. Memberikan informasi hasil proses saat menggunakan berkas berekstensi JPG sebagai *input* dan *output* steganografi.

BAB II

TINJAUAN PUSTAKA

2.1. Kriptografi

Kriptografi dalam bahasa Inggris *cryptography* tercatat pertama kali digunakan pada buku berjudul "*The Garden of Cyrus*" oleh seorang dokter sekaligus penulis berkebangsaan Inggris tahun 1658 bernama Thomas Browne. Jika dilihat dari arti kata kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptós*" artinya "*hidden*" (tersembunyi), sedangkan "*gráphein*" artinya "*write*" (tulis), jadi kriptografi diartikan sebagai "*hidden write*" (tulisan tersembunyi). Kriptografi juga bermakna sebagai suatu studi tentang metode untuk mengirimkan pesan secara rahasia, sehingga hanya penerima pesan yang dituju dapat memahami dan membaca pesan (Mollin, 2007).

2.1.1. Istilah-istilah Kriptografi

Dalam kriptografi terdapat beberapa istilah-istilah umum yang digunakan antara lain (Mollin, 2007):

1. *Plaintext*

   Plaintext merupakan pesan asli yang belum disembunyikan.

2. *Ciphertext*

Ciphertext merupakan pesan yang telah disembunyikan.

3. *Cryptogram*

   Cryptogram adalah pesan akhir yang telah disembunyikan rinci informasinya atau dienkapsulasi, dan telah dikirim.

4. *Encryption*

   Encryption adalah proses untuk mengubah pesan asli menjadi pesan yang disamarkan.

5. *Decryption*

   Decryption adalah proses untuk mengubah pesan yang disamarkan menjadi pesan asli, hal ini dilakukan oleh penerima yang memiliki pengetahuan untuk menerjemahkan pesan yang tersembunyi.

6. *Cryptographer*

   Cryptographer adalah siapapun yang terlibat di dalam kriptografi.

7. *Cryptanalysis*

   Cryptanalysis adalah studi atau kajian mengenai teknik matematika yang digunakan untuk memecahkan suatu metode kriptografi.

8. *Cryptanalysts*

   Cryptanalysts adalah siapapun yang berupaya untuk memecahkan suatu metode kriptografi.

9. *Cryptology*

   Cryptology adalah studi atau kajian yang membahas antara keduanya, baik kriptografi maupun kriptanalisis.

10. *Cryptologists*

    Cryptologists adalah siapapun yang mempelajari kriptologi.

2.1.2. Tujuan Kriptografi

Tujuan kriptografi secara umum adalah mewujudkan keempat aspek keamanan dalam teori dan praktek yaitu (Ariyus, 2008):

1. ***Confidentiality*** **(kerahasiaan)**

   Layanan yang ditujukan untuk menjaga pesan tidak dapat dibaca oleh pihak pihak yang tidak berhak.

2. ***Authentication*** **(otentikasi)**

   Penerima pesan dapat memastikan keaslian pengirimnya. Penyerang tidak dapat berpura-pura sebagai penerima ataupun pengirim pesan.

3. ***Integrity*** **(integritas)**

   Penerima harus dapat memeriksa apakah pesan telah dimodifikasi ditengah jalan atau tidak. Seorang penyusup seharusnya tidak dapat memasukkan tambahan kedalam pesan, mengurangi atau mengubah pesan selama data berada diperjalanan.

4. ***Nonrepudiation***

   Pengirim tidak dapat mengelak bahwa dia telah mengirim pesan, penerima juga tidak dapat mengelak bahwa dia telah menerima pesan tersebut.

2.1.3. Jenis Algoritma Kriptografi

Algoritma kriptografi terbagi menjadi dua jenis jika dilihat berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi.

1. Algoritma Simetris
2. Algoritma Asimetris

2.2. Metode Tranposisi Kolom

Pada metode transposisi kolom, huruf-huruf di dalam *plaintext* tetap, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karkater tersebut (Munir, 2006).

Pada metode transposisi kolom, *plaintext* tetap sama, tetapi urutannya diubah. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut. Dalam transposisi kolom, pesan ditulis dalam deretan panjang tetap, dan kemudian membaca lagi kolom dengan kolom, dan kolom yang dipilih disesuaikan dengan rangka yang sudah ditetapkan. Kedua lebar baris dan permutasi dari kolom biasanya ditentukan oleh kata kunci.

Metode transposisi kolom cukup sederhana, yaitu dengan membagi *plaintext* menjadi blok-blok dengan panjang kunci (k) tertentu yang kemudian blok-blok tersebut disusun dalam bentuk baris dan kolom. Terdapat dua metode yang digunakan apabila panjang *plaintext* (n) tidak habis dibagi oleh kunci (k). Pertama adalah *irregular case*, yaitu melakukan enkripsi tanpa merubah *plaintext* dan yang kedua adalah *regular case* yaitu melakukan enkripsi setelah menambahkan karakter-karakter *dummy (pad)* sebanyak d dengan 0<d<n sehingga panjang plainteks habis dibagi kunci. Hasil enkripsi adalah dengan membaca secara vertikal (tiap kolom) sesuai urutan kolom.

Sebagai contoh, kata “zebras” adalah panjang 6 (sehingga baris yang panjang 6), dan permutasi ditentukan oleh urutan abjad dari huruf-huruf dalam kata kunci. Dalam hal ini, order akan “6 3 2 4 1 5”. Dalam transposisi kolom biasa, spasi kadang dipenuhi dengan nulls; ruang yang dibiarkan kosong. Akhirnya, pesan tersebut dibacakan dalam kolom, dalam urutan yang ditentukan oleh kata kunci.

2.3. Metode RSA

Algoritma RSA dibuat oleh 3 orang peneliti dari MIT *(Massachussets Institute of Technology)* pada tahun 1976, yaitu: Ron Rivest, Adi Shamir, dan Leonard Adleman. Menurut Munir (2004) keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci *private.*

Dalam hal ini masalah pemfaktoran terletak pada sulitnya memfaktorkan bilangan *n* menjadi dua faktor primanya, yaitu *p* dan *q*, sedemikian sehingga $n = p \cdot q$. Namun jika *n* berhasil difaktorkan menjadi *p* dan *q*, maka $\phi(n) = (p-1)(q-1)$ dapat dihitung dan selanjutnya, karena kunci enkrispi *e* diumumkan (tidak rahasia), maka kunci dekripsi *d* dapat dihitung dari persamaan $e.d=1 \pmod{\phi(n)}$.

Penemu algoritma RSA menyarankan nilai *p* dan *q* panjangnya lebih dari 100 digit. Dengan demikian hasil kali $n = p \cdot q$ akan berukuran lebih dari 200 digit, dengan begitu usaha untuk mencari faktor prima dari bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun, sedangkan untuk bilangan 500 digit membutuhkan waktu 10^{25} tahun dengan asumsi bahwa algoritma

pemfaktoran yang digunakan adalah algoritma yang tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik (Munir, 2004).

2.3.1. Properti Algoritma RSA

Algoritma RSA memiliki besaran-besaran sebagai berikut (Stinson, 2006).

1. *p* dan *q* bilangan prima (rahasia)
2. $n=p.q$ (tidak rahasia)
3. $\phi(n) = (p - 1)(q - 1)$ (rahasia)
4. *e* (kunci enkripsi) (tidak rahasia)
5. *d* (kunci dekripsi) (rahasia)
6. *m (plaintext)* (rahasia)
7. *c (ciphertext)* (tidak rahasia)

Algoritma pembangkitan pasangan kunci.

1. Pilih dua buah bilangan prima sembarang, p dan q.
2. Hitung $n = p.q$ (sebaiknya $p \neq q$, sebab jika p = q maka n= p2 sehingga p dapat diperoleh dengan numerik akar pangkat dua dari n).
3. Hitung $\phi(n) = (p - 1)(q - 1)$.
4. Pilih kunci publik, *e*, yang relative prima terhadap $\phi(n)$.
5. Hitung kunci dekripsi, *d*, dengan kekongruenan $ed=1 \pmod{\phi(n)}$.

2.3.2. Modulo

Algoritma kriptografi RSA menggunakan aritmatika modulo dalam proses enkripsi maupun dekripsi. Misalkan *a* adalah bilangan bulat dan *m* adalah bilangan bulat > *0*. Operasi *a mod m* (dibaca *"a* modulo *m"*) memberikan sisa

jika *a* dibagi dengan *m*. Bilangan *m* disebut modulus atau modulo, dan hasil aritmetika modulo *m* terletak di dalam himpunan *{0, 1, 2, ..., m – 1}* (Munir, 2006).

2.4. Steganografi

Steganografi *(steganography)* merupakan teknik menyembunyikan pesan rahasia pada suatu media sehingga keberadaan pesan rahasia tidak disadari oleh orang lain. Kata *Steganography* berasal daribahasa Yunani, yaitu gabungan dari kata *steganos* (tersembunyi) dan *graphein* (tulisan), dari pengertian setiap kata dapat disimpulkan bahwa steganografi merupakan tulisan tersembunyi (Nosrati, 2011).

2.4.1. Kriteria Steganografi

Kriteria steganografi yang harus diperhatikan dalam penyembunyian data menurut Munir (2006), yaitu:

1. *Imperceptibility*. Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio, maka indera telinga tidak dapat mendeteksi perubahan pada audio *stegotext*-nya.
2. *Fidelity*. Mutu *stegomedium* tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra stegotext sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext*

berupa audio, maka audio *stegotext* tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.

3. *Recovery*. Pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan lebih lanjut.

2.4.2. Proses Steganografi

Ada dua proses utama dalam steganografi yaitu penyisipan (*embedding*) dan penguraian (*extraction*) pesan atau informasi dalam media cover. *Embedding* merupakan proses menyisipkan pesan atau informasi ke dalam media cover, sedangkan *extraction* adalah proses menguraikan pesan yang tersembunyi dalam gambar stego. Pesan yang akan disembunyikan dalam suatu gambar membutuhkan dua file. Pertama adalah gambar asli yang belum dimodifikasi yang akan menangani pesan tersembunyi, yang disebut gambar penampung (*cover image*). File kedua adalah informasi pesan yang disembunyikan. Suatu pesan dapat berupa *plaintext*, *ciphertext*, gambar lain, atau apapun yang dapat ditempelkan ke dalam *bit stream*. Ketika dikombinasikan, *cover image* dan pesan yang ditempelkan membuat gambar stego (stego *image*) (Mahmudy, 2006).

2.5. Metode AMELSBR

Metode ini pertama kali diperkenalkan oleh Yeuan-Kuen Lee dan Ling-Hwei Chen pada tahun 1999 dalam makalahnya "*An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement*" dan *"High Capacity Image*

Steganographic Model". Di dalam makalahnya, Lee dan Chen (1999) menerapkan citra hitam-putih *(grayscale image)*sebagai media penampung *(cover image)* dan kemudian pada tahun 2003, Mark David Gan mengimplementasikan metode ini dengan citra berwarna *24 bit (true colors image)* sebagai media penampungnya (Gan, 2003).

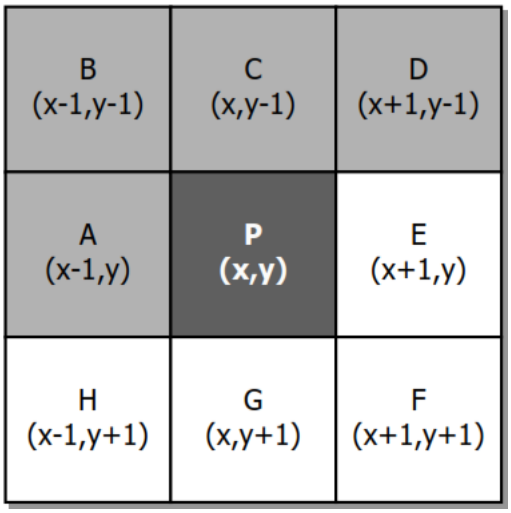
Dari hasil penelitian tersebut ternyata metode ini menawarkan beberapa kelebihan dibandingkan dengan metode LSB, yaitu *bit* data rahasia yang akan disisipkan lebih banyak (pada metode LSB umumnya hanya 1 *bit*) tanpa menimbulkan banyak perubahan pada media penampung (dalam hal ini adalah data citra). Dengan metode ini, setiap *pixel* memiliki kapasitas penyembunyian yang berbeda-beda tergantung dari nilai toleransi *pixel* tersebut terhadap proses modifikasi atau penyisipan. Suatu *pixel* pada data citra bisa dikatakan dapat ditoleransi apabila dilakukan proses modifikasi (penyisipan) dengan skala yang tinggi terhadap nilainya adalah memungkinkan tanpa merubah tampak asli data citra tersebut, atau dengan kata lain area yang halus dan solid pada suatu data citra memiliki kadar toleransi yang rendah *(less tolerant)* terhadap proses modifikasi dibandingkan dengan area yang memiliki tekstur yang kompleks (Gan, 2003).

Metode *AMELSBR* yang diterapkan pada citra berwarna (*jpg/jpeg 24-bit*) memiliki beberapa langkah atau tahapan utama untuk melakukan proses penyisipan, antara lain *Capacity Evaluation, Minimum Error Replacement* dan *Error Diffusion* (Gan, 2003).

Sebelum dilakukan proses penyisipan, maka langkah pertama yang harus dilakukan adalah mengevaluasi kapasitas penyisipan *(capacity evaluation)* dan mencari nilai *color variation*. Kemudian setelah mendapatkan nilai *color*

variation, nilai tersebut diproses kembali untuk mendapatkan kapasitas penyisipan sejumlah *K-bit*. Setelah itu, untuk beradaptasi dengan karakteristik lokal *pixel*, maka sejumlah *K-bit* tersebut ditangani dengan proses evaluasi kapasitas (*capacity evaluation*). Proses selanjutnya adalah mencari *MER*, dimana proses ini akan menentukan apakah *bit* ke *K+1* akan dilakukan perubahan atau tidak, dan yang akan menentukan itu adalah berdasarkan pada nilai *embedding error (Er)* (Gan, 2003).

Ketiga tahapan utama akan diterapkan per bloknya atau per operasi penyisipannya, dimana *bit-bit* data rahasia hanya akan disisipkan pada salah satu komponen warna di *pixel P*.



Gambar 2.1. Menentukan *grayscale pixel* (Gan, 2003).

Capacity evaluation, merupakan tahap pertama dan yang paling krusial dari metode penyisipan AMELSBR. Tahap ini mengacu pada karakterisitik *human visual system* (HVS) yang tidak sensitif terhadap *noise* dan perubahan warna yang terdapat di dalam citra (Lee dan Chen, 1999). Langkah pertama yang akan dilakukan pada evaluasi kapasitas adalah mencari nilai *color variation (V)* atau

variasi warna yang melibatkan *pixel A, B, C* dan *D*. Adapun rumus dari *V* adalah sebagai berikut (Gan, 2003).

$$V = round\ \{(|C-A|+|A-B|+|B-C|+|C-D|)/4\}$$

dengan :

V = variasi warna *(color variation)*

Round = fungsi matematika untuk pembulatan

Rumus di atas akan menghasilkan ketentuan toleransi modifikasi yang akurat di setiap *pixel P*. Langkah ke-dua adalah mencari kapasitas penyisipan *(K)* pada *pixel P* dan dapat diterapkan rumus sebagai berikut (Gan, 2003).

$$K = round\ (|log2\ V|)$$

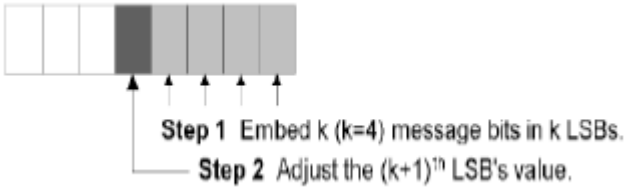
dengan :

K = kapasitas penyisipan pada *pixel P* dalam *bit*.

V = variasi warna

Round = fungsi matematika untuk pembulatan.

Tahap selanjutnya adalah mencari *Minimum-Error Replacement* (MER). Tahap ini berfungsi untuk meminimalkan terjadinya perubahan *pixel* pada citra penampung akibat dari proses penyisipan. Proses MER dilakukan dengan mengubah nilai *bit* ke *K+1* pada *pixel P*. Perubahan ini akan terjadi pada salah satu dari ke-tiga komponen warna (R, G atau B) yang terpilih (Lee dan Chen, 1999).



Gambar 2.2. Proses MER (Lee dan Chen, 1999)

Bila pada langkah sebelumnya (evaluasi kapasitas) didapat $K = 4$, maka *bit* yang ke-lima akan diubah nilainya, misal nilai awal adalah 1, maka akan diubah menjadi 0, begitu juga sebaliknya. Namun demikian pengubahan *bit* ke *K+1* belum tentu dilakukan, karena pada tahap MER juga dilakukan proses pengecekan nilai *embedding error*. *Embedding error (Er)* adalah selisih nilai (dalam desimal) pada komponen warna yang terpilih di *pixel P*, sebelum (original) dan sesudah dilakukan proses penyisipan, atau dengan rumus seperti di bawah ini

$Er = Abs\ [P(x,y) - P'(x,y)]$

dengan :

Abs = Nilai absolut

Er = Nilai *embedding error*

P(x,y) = *Pixel P* asli

P'(x,y) = *Pixel P* yang telah dimodifikasi

Pengubahan pada *bit* ke *K+1* akan dilakukan apabila nilai *embedding error* memenuhi syarat pada saat pengecekan, uraiannya bisa dijelaskan sebagai berikut. Asumsi *P(x,y)* adalah *pixel P* original, *P'(x,y)* adalah *pixel P* yang telah disisipkan sejumlah *K-bit* tanpa mengubah *bit* ke *K+1* dan *P''(x,y)* adalah *pixel P* yang telah disisipkan sejumlah *K-bit* sekaligus mengubah *bit* ke *K+1*. *Minimum error* yang dapat terjadi di *pixelP*haruslah *P'(x,y)* atau *P''(x,y)* (Lee dan Chen, 1999).

Kemudian proses pengecekan nilai *embedding error* dilakukan melalui rumus sebagai berikut

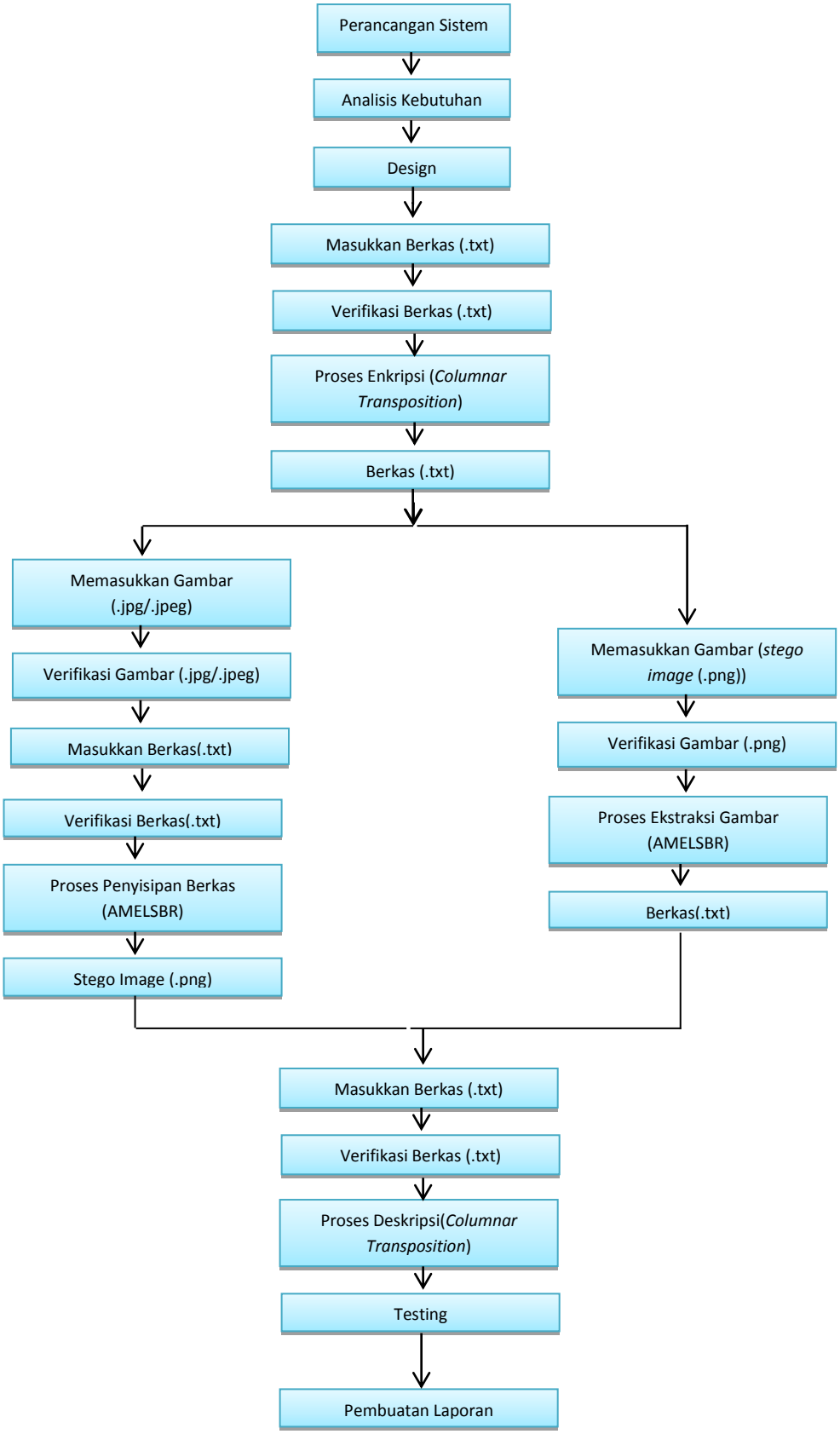
$Er1 = Abs\ [P(x,y) - P'(x,y)]$

$Er2 = Abs\ [P(x,y) - P''(x,y)]$

Apabila $Er1 < Er2$, maka $P'(x,y)$ yang akan menggantikan $P(x,y)$. Jika sebaliknya maka $P''(x,y)$yang akan menggantikan $P(x,y)$ (Lee dan Chen, 1999).

2.6. Hibrid Tranposisi Kolom dengan AMELSBR

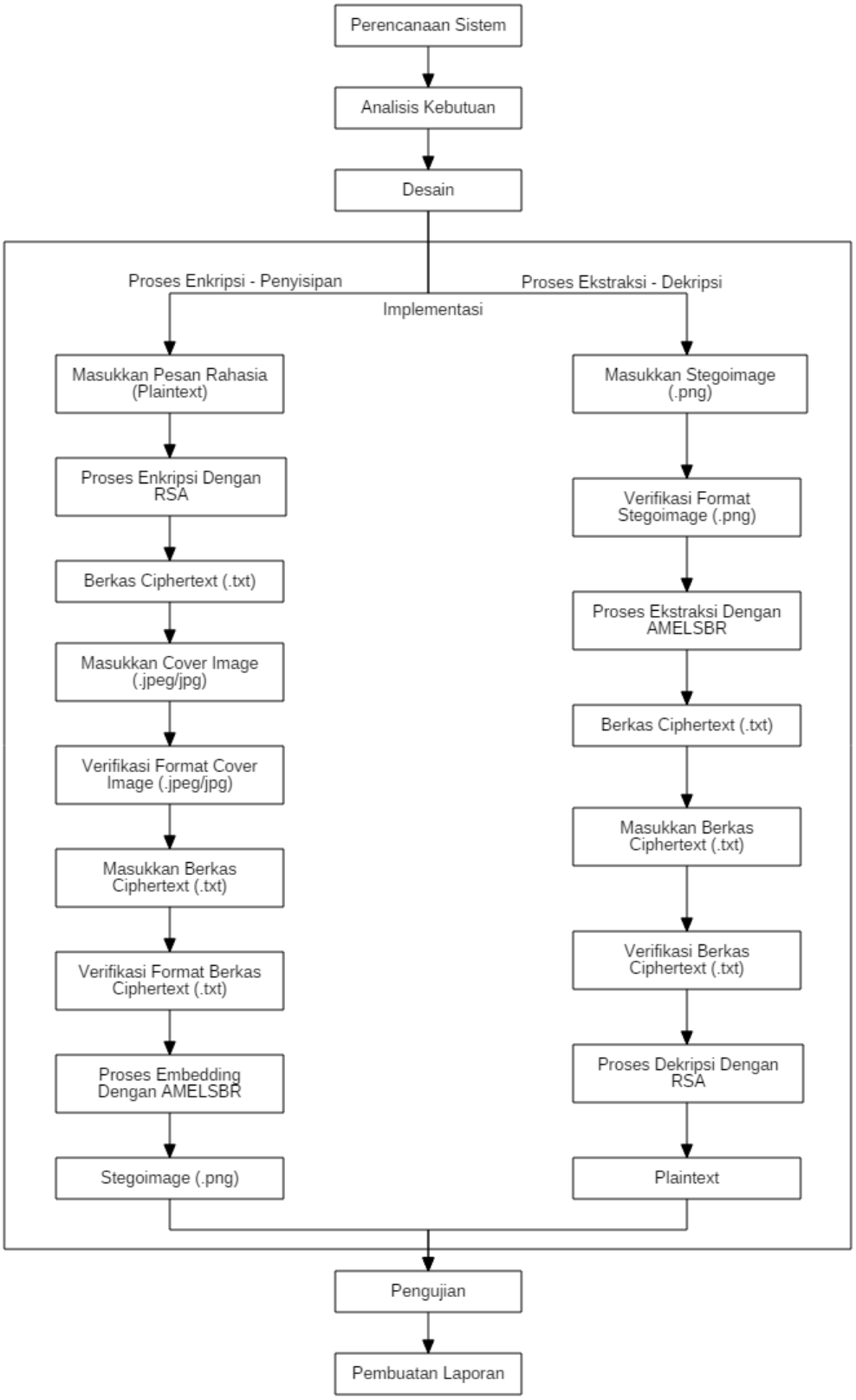
Setiawan (2016) melakukan penelitian untuk mengenkripsi pesan menggunakan metode hibrid transposisi kolom dan *Adaptive Minimum Error Least Significant Bit Repleacement (AMELSBR).* Penelitian tersebut membangun sistem kriptografi tranposisi kolom menggunakan bahasa pemrograman C++ untuk proses deksipsi dan enkripsi. Setelah proses enkripsi dilakukan, berkas hasil enkripsi kemudian disisipkan ke dalam media gambar sebagai cover menggunakan metode AMELSBR dengan bahasa permrograman PHP. Dalam penelitian tersebut tahapan untuk melakukan proses enkripsi dan penyisipan, selanjutnya proses ekstraksi dan dekripsi akan ditunjukkan pada Gambar 2.3.



Gambar 2.3. Tahapan hibrid transposisi kolom dengan AMELSBR

2.7. Hibrid RSA dengan AMELSBR

Ahmad (2016) melakukan penelitian untuk mengenkripsi pesan menggunakan hibrid kriptografi RSA dan steganografi AMELSBR. Penelitian tersebut membangun sistem kriptografi dengan metode RSA untuk proses enkripsi dan dekripsinya menggunakan bahasa pemrograman PHP. Sedangkan untuk proses penyisipan dan ektraksinya menggunakan metode AMELSBR dengan bahasa pemrograman PHP. Tahapan yang dilakukan pada penelitian tersebut yaitu perencanaan sistem, analisis kebutuhan, desain, implementasi, testing, dan pembuatan laporan. Tahapannya ditunjukkan pada Gambar 2.4.



Gambar 2.4. Tahapan penelitian hibrid RSA dengan AMELSBR

BAB III

METODE PENELITIAN

3. 1. Tempat dan Waktu Penelitian

Penelitian yang dilakukan berada di Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Lampung. Waktu penelitian dilakukan pada semester ganjil tahun ajaran 2017-2018.

3. 2. Perangkat Pendukung

Perangkat pendukung yang digunakan dalam melakukan perbandingan antara hybrid tranposisi kolom dengan AMELSBR dan hybrid RSA dengan AMELSBR adalah sebagai berikut:

3.2.1. Perangkat Keras

Perangkat keras yang digunakan adalah satu unit laptop dengan spesifikasi sebagai berikut:

- Prosessor : Pentium® Dual-Core CPU T4500 @2.30GHz
- Memory : 3072MB RAM DDR3
- DirectX Version : DirectX 11
- Harddrive : ATA disk, Hitachi HTS54502, 232GB
- Graphic : Mobile Intel® 4 Series Express Chipset Family

3.2.2. Perangkat Lunak

Perangkat lunak yang digunakan pada penelitian ini adalah sebagai berikut:

1. Sistem Operasi Linux Ubuntu 14.04 LTS

   Ubuntu adalah distribusi Linux berbasis Debian yang dipublikasikan dengan sumber terbuka. Linux Ubuntu versi 14.04 memiliki kode nama *Trusty Tahr* dan didukung oleh LTS (*Long Term Support*) merupakan edisi dengan dukungan jangka panjang, berupa dukungan keamanan dan kestabilan.

2. *Browser* Mozila Firefox 42.0 (32-bit)

   Mozila Firefox adalah aplikasi peramban web yang sudah menerapkan beberapa standar web termasuk HTML5, XML, XHTML, CSS, JavaScript.

3. Apache-2.4

   Apache merupakan suatu *web server* yang dapat dijalankan di berbagai *platform* seperti Linux dan Windows. Apache mampu melayani koneksi *transfer data* dalam protokol HTTP (*Hyper Text Transfer Protocol*).

4. MySQL-5.5

   MySQL merupakan implementasi dari sistem manajemen basisdata yang didistribusikan secara gratis. Setiap pengguna dapat secara bebas menggunakan MySQL dengan batasan tidak dijadikan produk turunan yang bersifat komersial.

5. PHP-5.5

   PHP awalanya adalah singkatan dari *Personal Home Page*, namun sekarang lebih dikenal sebagai *PHP: Hypertext Preprocessor*. PHP disebut bahasa pemrograman *server-side* karena PHP diproses pada komputer server. Hal ini berbeda dibandingkan dengan bahasa pemrograman *client-side* seperti JavaScript yang diproses pada *web browser* (*client*).

6. Text Editor (gedit)

   Gedit merupakan aplikasi pengolah teks yang secara *default* sudah ada pada sistem operasi ubuntu, khususnya gnome.

7. GIMP 2.8.18

   GIMP adalah perangkat lunak pengolah gambar yang dapat digunakan untuk memanipulasi gambar dengan format jpg, png, bmp, gif, svg untuk diberikan perlakuan seperti *cropping* , perubahan *brightness* dan perubahan *contrast* .

8. *Source Code* steganografi AMELSBR yang dikembangkan oleh Panditatwa (2015).

9. *Source Code* kriptografi tranposisi kolom yang dikembangkan oleh Setiawan (2016).

10. *Source Code* kriptografi RSA yang dikembangkan oleh Ahmad (2016).

3. 3. Metode Penelitian

Metode penelitian yang digunakan adalah studi literatur, yaitu dengan memperoleh informasi dari buku, jurnal, skripsi, dan internet. Tujuannya adalah memperoleh referensi teori serta penelitian yang telah dilakukan sebelumnya. Informasi yang diperoleh berkaitan dengan metode kriptografi tranposisi kolom dan RSA serta metode steganografi AMELSBR.

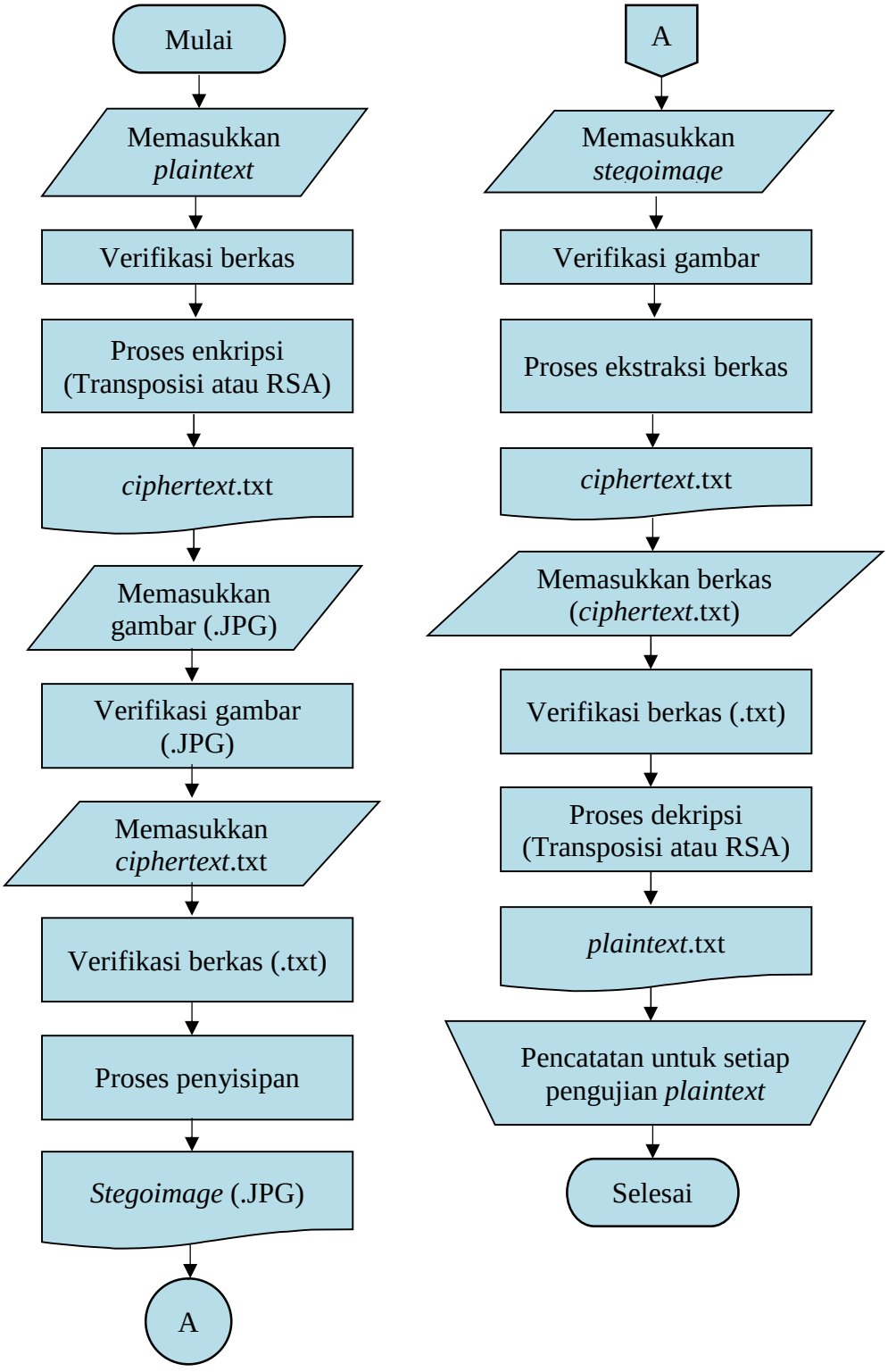
Selain studi literatur, metode yang digunakan adalah analisis, yaitu, mengidentifikasi algoritma kriptografi yang akan diuraikan serta dibandingkan pada hasil dan pembahasan. Metode kriptografi yang dibahas adalah metode kriptografi tranposisi kolom dan metode kriptografi RSA. Algoritma steganografi yang digunakan adalah AMELSBR.

3. 4. Skenario Pengujian

Tahapan pengujian yang akan dilakukan yaitu:

1. Pengujian Enkripsi dan Dekripsi

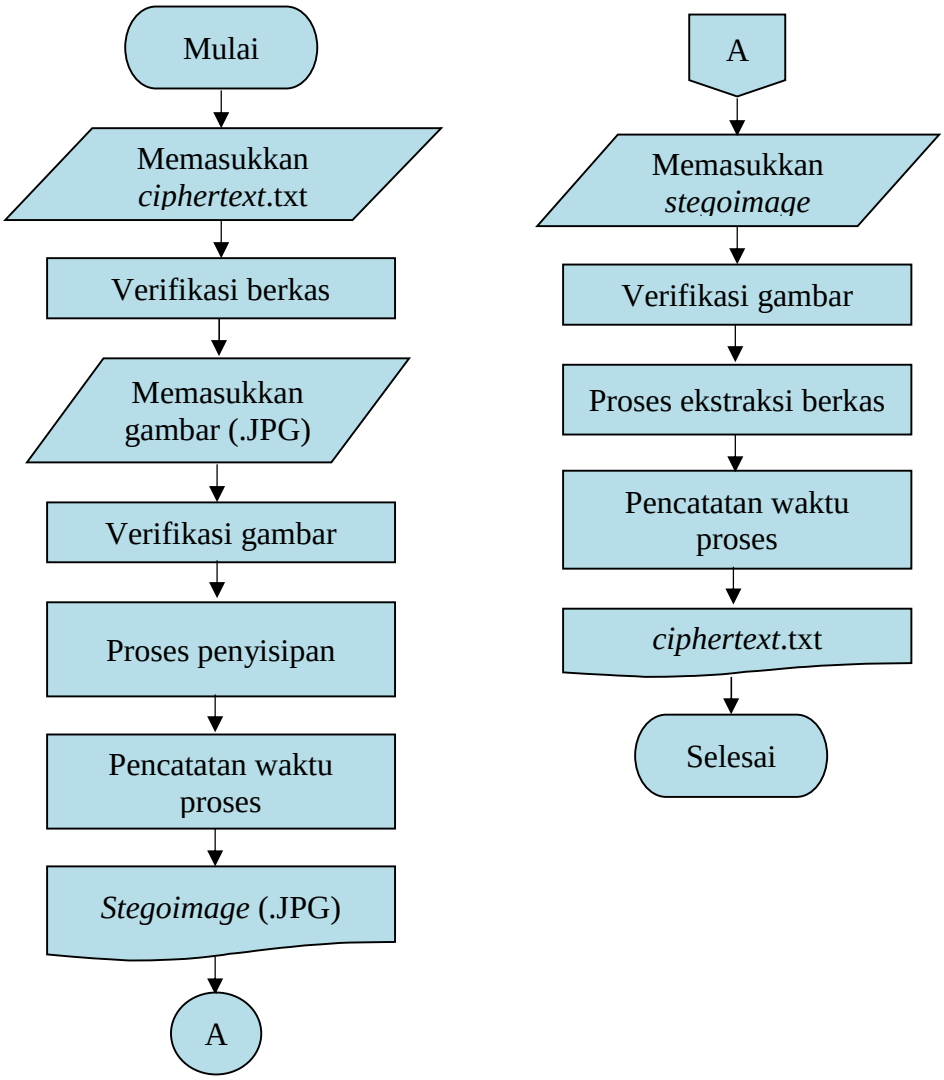
Pengujian ini dilakukan untuk membuktikan apakah proses enkripsi pesan rahasia dapat diubah kedalam bentuk yang tidak dimengerti maknanya dan sebaliknya pada saat dekripsi, apakah pesan yang tidak bermakna tersebut berhasil dikembalikan kedalam bentuk yang memiliki makna sesuai dengan aslinya tanpa mengurangi, menambah, dan memodifikasi isinya antara kriptografi tranposisi kolom dan RSA.



Gambar 3.1. Alur pengujian enkripsi dan dekripsi.

2. Pengujian Waktu Proses Penyisipan dan Ekstraksi

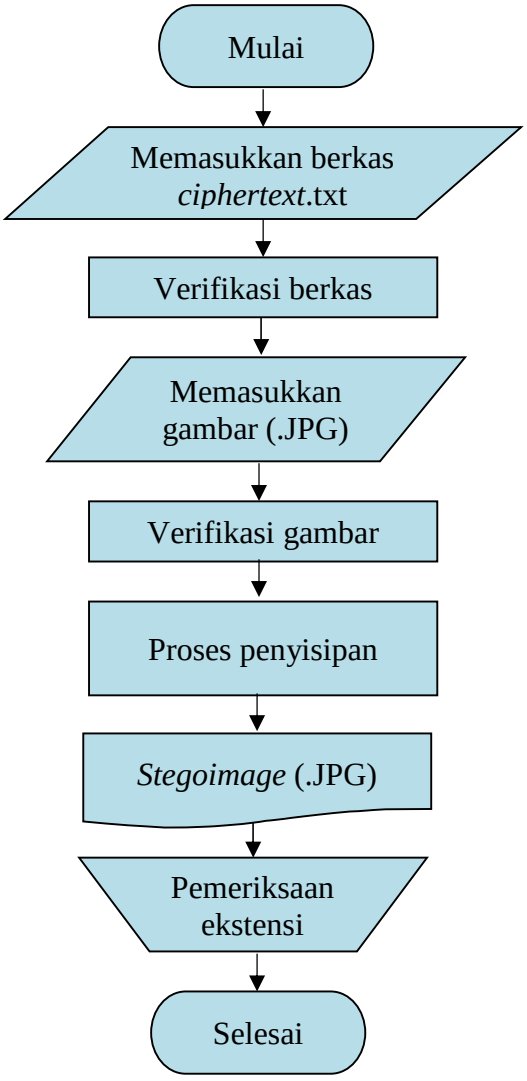
Pengujian ini dilakukan untuk membuktikan lama proses penyisipan dan ekstraksi untuk setiap metode kriptografi, baik metode kriptografi tranposisi kolom maupun kriptografi RSA pada steganografi AMELSBR.



Gambar 3.2. Alur pengujian waktu penyisipan dan ekstraksi.

3. Pengujian Terhadap Format *File*

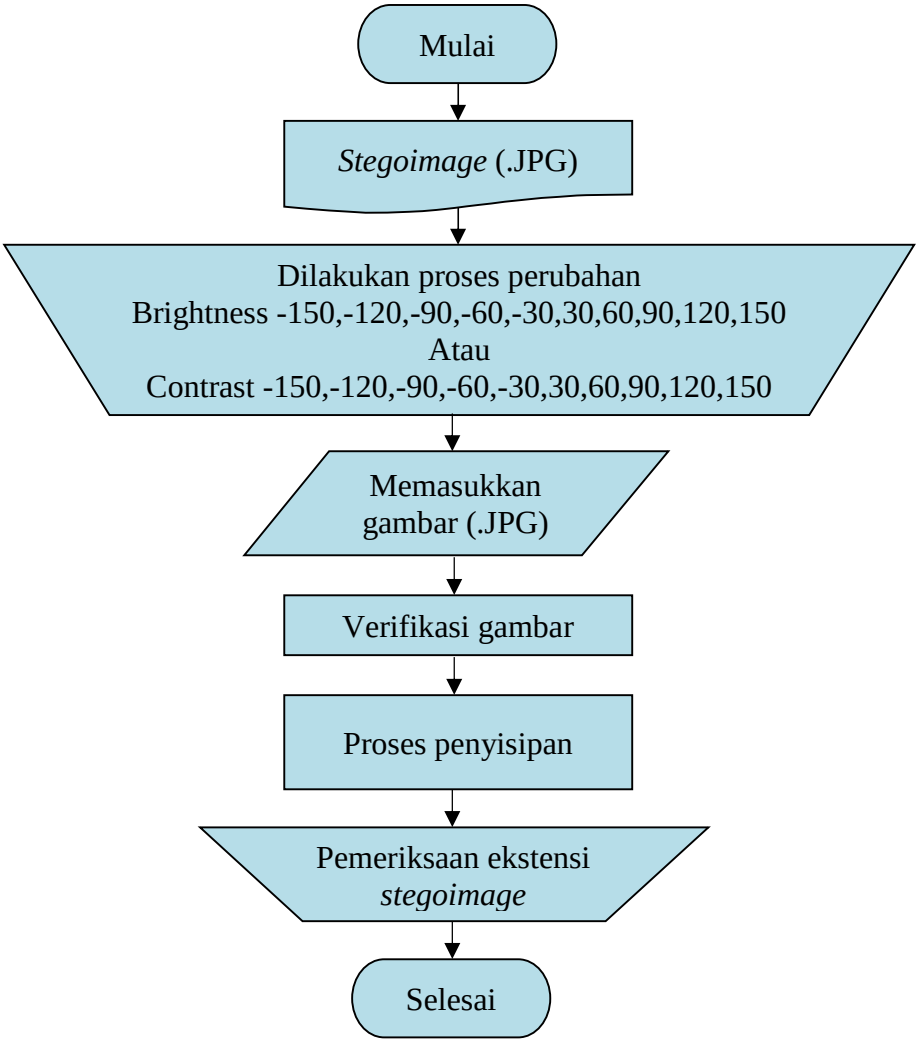
Pengujian ini dilakukan untuk membuktikan bahwa gambar dengan format (.jpeg/jpg) sebagai input, sedangkan sebagai output juga adalah gambar dengan format (.jpeg/jpg), yang mana format jenis ini merupakan format *file* yang baik digunakan untuk tahap proses steganografi.



Gambar 3.3. Alur pengujian terhadap format file.

4. Pengujian Terhadap Perubahan *Brightness* dan *Contrast*

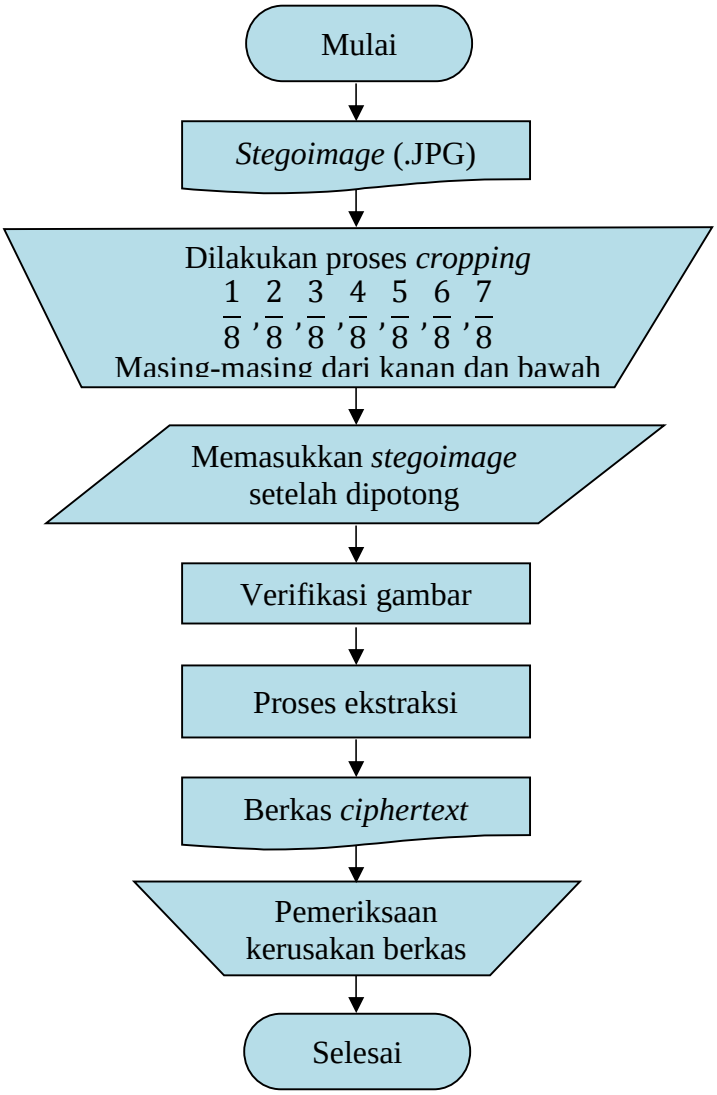
Pengujian ini dilakukan untuk membuktikan apakah perubahan pada *brightness* dan *contrast* mempengaruhi isi pesan yang terkandung di dalam *stegoimage*. Pengujian ini bertujuan mengetahui tingkat kerusakan pesan yang terkandung pada *stegoimage*.



Gambar 3.4. Alur pengujian terhadap perubahan *brightness* dan *contrast*.

5. Pengujian Terhadap Pemotongan Gambar *(Cropping)*

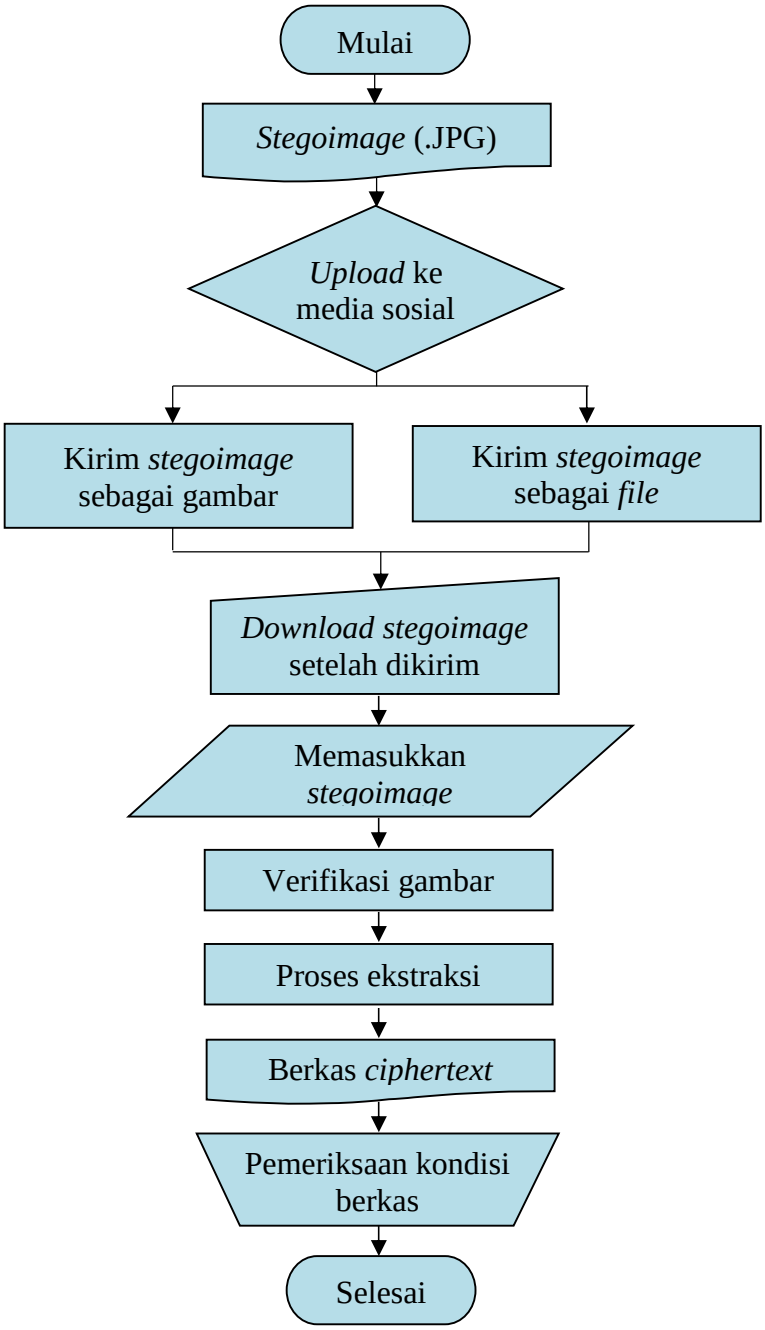
Pengujian ini dilakukan untuk membuktikan apakah dengan melakukan pemotongan gambar *(cropping)* dapat mempengaruhi isi pesan yang terkandung di dalam *stegoimage*. Pengujian ini dilakukan dengan memotong *stegoimage* pada bagian-bagian tertentu. Pengujian ini bertujuan mengetahui tingkat kerusakan pesan yang terkandung pada *stegoimage*.



Gambar 3.5. Alur pengujian terhadap pemotongan gambar.

6. Pengujian Pengiriman *Stegoimage* Melalui Media Sosial

Pengujian dilakukan untuk membuktikan apakah pengiriman *stegoimage* melalui jalur komunikasi pada beberapa aplikasi media sosial dapat sampai dengan utuh tanpa mengalami kerusakan berkas. Pengujian ini akan dilakukan dengan cara mengirimkan *stegoimage* ke beberapa aplikasi media sosial, seperti *Line*, BBM *(Blackberry Messenger)*, *Whatsapp*, *Telegram* dan *Facebook Messenger*.



Gambar 3.6. Pengujian pengiriman melalui media sosial.

4. *Stegoimage* yang berisi *ciphertext* RSA dan *ciphertext* transposisi kolom tidak dapat mengembalikan pesan setelah dilakukan perubahan *brightness* dan *contrast*, hal ini juga dipengaruhi oleh tipe *file stegoimage* adalah .JPG mengakibatkan penurunan ukuran *stegoimage* pada proses manipulasi.
5. Pemotongan bagian *stegoimage* tidak berpengaruh pada berkas yang tersimpan apabila dilakukan pada bagian bawah hingga 7/8 bagian. Pesan dengan 85 karakter dapat utuh setelah pemotongan *stegoimage* hingga 5/8 bagian dari kanan.
6. Pengiriman melalui media sosial dapat dilakukan dengan catatan saat pengiriman file *stegoimage* tidak mendapatkan kompresi.

5.2. Saran

Setelah melakukan pengujian antara kriptografi RSA dan kriptografi transposisi kolom yang disisipkan kedalam media gambar, maka saran yang diberikan adalah sebagai berikut.

1. Implementasi *output stegoimage* sebaiknya menggukan tipe *file* yang memiliki tingkat kompresi yang rendah (*lossless compression*).
2. Penggabungan metode steganografi dengan metode kriptografi sebaiknya tidak menggunakan metode kriptografi dengan algoritma yang mengubah urutan dari *plaintext*, walaupun ukuran dan waktu relatif lebih sedikit, tetapi sangat rentan apabila berkas tidak kembali utuh, hal tersebut membuat *ciphertext* tidak bisa didekripsi.

DAFTAR PUSTAKA

Ariyus, Doni. 2008. *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi*. ANDI: Yogyakarta.

Ahmad, E. I. 2016. Hibrid kriptografi dan steganografi menggunakan RSA dan AMELSBR.(Skripsi).Universitas Lampung. Bandar Lampung.

Arifin, R dan Oktoviana, L. T. 2013. Implementasi Kriptografi dan Steganografi Menggunakan Algoritma RSA dan Metode LSB. Program Studi Matematika. Universitas Negeri Malang.

Gan, M. D. 2003. *Chameleon Image Steganography*. STI Network, STI College Bacoor. Philippines.

Lee, Y. K., dan Chen, L. H. 1999. *An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement*. National Science Council, ROC. NSC87-2213-E-009-006.

Mahmudy,Wayan Firdaus. 2006. *Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion*. Kursor, vol. 2, no. 2, pp. 38-44.

Mollin, Richard A. 2007. *An Introduction to Cryptography Second Edition Discrete Mathematics and Its Applications*. Chapman & Hall/CRC.

Munir, Rinaldi. 2004. *Kriptografi: Algoritma RSA dan ElGamal*. Teknik Informatika. Institut Teknologi Bandung. Bandung.

Munir, Rinaldi. 2006. *Kriptografi. Teknik Informatika*. Institut Teknologi Bandung. Bandung.

Nosrati, Masoud. 2011. An introduction to steganography methods. *World Applied Programming*, Vol (1), No (3). ISSN: 2222-2510.

Panditatwa, Pandya. 2015. Implementasi Teknik Steganografi Menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR).(Skripsi). Universitas Lampung. Bandar Lampung.

Prayudi, Y dan Kuncoro, P. S. 2005. *Implementasi Steganografi Menggunakan Teknik Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)*. Seminar Nasional Aplikasi Teknologi Informasi (SNATI). ISBN: 979-756-061-6.

Setiawan, Roni. 2016. Enkripsi Pesan dalam Media Gambar menggunakan Metode Hibrid Transposisi Kolom dan Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR).(Skripsi). Universitas Lampung. Bandar Lampung.

Stinson, Douglas R. 2006. *Chryptography Theory and Practice 3rd Edition*. Canada: Chapman & Hall/CRC.