PENGEMBANGAN TEKNIK MENYEMBUNYIKAN PESAN RAHASIA DENGAN KEAMANAN BERLAPIS MENGGUNAKAN PENGGABUNGAN METODE STEGANOGRAFI DAN KRIPTOGRAFI CAESAR CIPHER YANG TELAH DIMODIFIKASI

Nazori Agani[1], Angga Kusuma Nugraha[2]

Program Studi Magister Komputer Program Pasca Sarjana Universitas Budi Luhur Jakarta
Jln. Ciledug Raya Petukangan Utara, Jakarta Selatan 12260
[1]nazori.agani@gmail.com,[2]me@incredibleangga.net

ABSTRAK

*Komunikasi dunia maya praktis, cepat dan terkadang rahasia, sehingga kemanan menjadi faktor penting. Steganografi bisa menyembunyikan pesan rahasia dengan disisipkan pada media, salah satunya citra digital. Sayangnya faktor keamanan steganografi belum maksimal. Teknik steganografi semakin populer sehingga banyak yang membuat aplikasi untuk mengekstrak pesan rahasia dari stego image. Pesan rahasia menjadi mudah diungkap oleh pihak yang tidak dikehendaki. Penelitian ini menambahkan keamanan pada steganografi dengan kriptografi Caesar Cipher yang telah dimodifikasi dengan membalik urutan pesan rahasia kemudian digeser 5 karakter, pesan rahasia lalu disisipkan kedalam gambar digital dengan metode Least Significant Bit (LSB). Pengujian dilakukan dengan metode kualitatif dengan Power Signal Noise Ratio (PSNR) serta perubahan ukuran file dan metode kuantitatif. Dari evaluasi diketahui aplikasi penguji dapat menyembunyikan pesan rahasia pada gambar digital dengan ekstensi populer. Selain itu diketahui file dengan ekstensi *.PNG memiliki sifat paling baik untuk digunakan sebagai cover image.*

Kata kunci **:** Steganografi, Kriptografi, Caesar Cipher, *Least Significant Bit (LSB)*, *Power Signal Noise Ratio* (PSNR)

1. PENDAHULUAN

Komunikasi melalui jaringan internet menjadi 6mplici karena dapat dilakukan dengan mudah dan melalui banyak media. Faktor keamanan adalah hal yang penting saat berkomunikasi pada jaringan internet. Banyak kasus kebocoran informasi yang terjadi saat berkomunikasi lewat jaringan internet. Salah satu metode untuk mengamankan pesan rahasia adalah Steganografi. Steganografi mengamankan pesan rahasia dengan menyisipkannya melalui media digital seperti citra, video, maupun suara.

Seiring berkembangnya penelitian mengenai teknik Steganografi, berbagai metode digunakan untuk menyisipkan pesan rahasia kedalam gambar menggunakan Steganografi. Salah satu metode yang 6mplici adalah *Least Significant Bit* (LSB) karena metodenya yang cukup sederhana yaitu menyembunyikan pesan rahasia yang telah diubah kedalam bentuk biner dengan cara menyisipkannya pada piksel terakhir yang menyusun file tersebut. Beberapa aplikasi menggunakan teknik ini dan dapat digunakan secara bebas dengan mengunduhnya dari internet adalah OpenStego dan Silent Eyes. Dengan semakin populernya dan banyak digunakan, perlu kemanan tambahan pada Steganografi sehingga apabila pesan rahasia tersebut berhasil diekstrak oleh pihak yang tidak diinginkan, pesan tersebut tetap belum dapat terungkap.

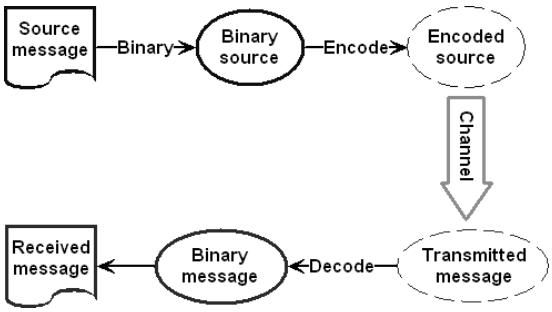
Pada penelitian ini, penulis mengajukan teknik pengamanan pesan rahasia Steganografi dengan keamanan berlapis, dengan menambahkan Kriptografi terhadap pesan rahasia yang akan disisipkan kedalam citra digital kemudian pesan disisipkan kedalam citra digital melalui Steganografi menggunakan metode LSB. Berbagai teknik Kriptografi 6mplici yang telah banyak digunakan sehingga source code untuk memecahkannya banyak tersebar dibeberapa situs internet. Oleh karena itu diperlukan Kriptografi berlapis dan unique agar pesan rahasia menjadi acak. Dengan cara tersebut diharapkan pesan yang akan disampaikan keamanannya lebih terjaga dan tidak mudah terungkap oleh pengguna yang berusaha mencuri informasi.

2. LANDASAN TEORI DAN KERANGKA KONSEP

A. Steganografi

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain pengirim dan penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia [1]. Dengan Steganografi maka pemilik data dapat menyembunyikan informasi hak ciptanya seperti identitas pembuat, tanggal dibuat, hingga pesan kepada seseorang yang dikehendaki. Steganografi menyembunyikan informasi kedalam berbagai jenis data seperti: gambar, audio, video, teks atau file biner.

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain pengirim dan penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia [1]. Dengan Steganografi maka pemilik data dapat menyembunyikan informasi hak ciptanya seperti identitas pembuat, tanggal dibuat, hingga pesan kepada seseorang yang dikehendaki. Steganografi menyembunyikan informasi kedalam berbagai jenis data seperti: gambar, audio, video, teks atau file biner Metode Steganografi sedemikian rupa dalam menyembunyikan isi suatu data didalam suatu sampul media atau data digital lain yang tidak diduga oleh orang biasa sehingga tidak menimbulkan kecurigaan kepada orang yang melihatnya.



Gambar 1. Ilustrasi Dasar Konsep Steganografi

Sebuah pesan yang akan dikirimkan diubah terlebih dahulu menjadi kode biner dan dimasukkan kedalam kode biner data lain yang menjadi media atau sampulnya. Lalu kedua kode biner tersebut dikodekan sehingga menjadi satu kesatuan tanpa mengubah integritas media yang ditumpangi. Selanjutnya data tersebut dikirimkan dan diterima oleh penerima pesan. Penerima pesan lalu mengkodekan kembali pesan tersebut sehingga pesan 7mpl dibaca.

Sebagai contoh, pengirim pesan mulai dengan berkas citra biasa, lalu mengatur warna setiap piksel ke-50 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada yang menyadarinya jika tidak memperhatikan dengan seksama).

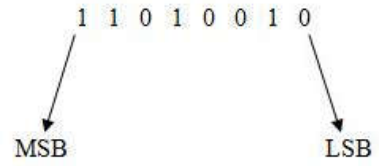
Dalam membuat Steganografi ada dua 7mplicit yang harus diperhatikan [2], yaitu:

1) *Fidelity*. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil Steganografi masih terlihat dengan baik. Pihak ketiga tidak mengetahui kalau didalam citra tersebut terdapat data rahasia.
2) *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan Steganografi adalah penyembunyian pesan, maka sewaktu-waktu pesan rahasia didalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

B. *Least Significant Bit*

Dalam Steganografi pesan rahasia disembunyikan dalam citra digital. Penyembunyian data dilakukan dengan mengganti *bit* data didalam segmen gambar dengan *bit* pesan rahasia.

Metode yang paling sederhana adalah metode modifikasi *Least Significant Bit* (LSB). Pada susunan bit didalam sebuah *byte* (1 *byte* = 8 *bit*), ada *bit* yang paling berarti (*Most Significant Bit* atau MSB) dan bit yang paling kurang berarti (*Least Significant Bit* atau LSB).



Gambar 2. Bit pada MSB dan LSB

Metode LSB adalah metode yang digunakan untuk menyembunyikan pesan dengan cara menyisipkannya pada bit rendah atau bit yang paling kanan pada data piksel yang menyusun file tersebut. Pada citra bitmap 24 bit, setiap piksel (titik) pada citra tersebut terdiri dari tiga susunan warna, yaitu merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap piksel citra bitmap 24 bit kita dapat menyisipkan 3 bit data. Kekurangan dari metode LSB ini adalah dapat secara drastis mengubah unsur pokok warna dari piksel jika tidak tepat dalam mengganti bit atau pesan yang dimasukkan terlalu panjang. Sehingga dapat menunjukkan perbedaan yang nyata dari gambar asli dengan gambar yang telah disisipkan pesan. Sementara kelebihan dari metode LSB adalah algoritma yang dipakai cepat dan mudah.

Karena bit yang diganti adalah bit rendah, maka perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil. Misalkan segmen data citra sebelum perubahan:

0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0

Data yang akan disembunyikan adalah '1 1 1'. Segmen data gambar setelah ‘1 1 1‘ disembunyikan:

0 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 1 1 0 0 0 1 1

Ukuran data yang akan disembunyikan bergantung pada ukuran gambar penampung. Pada citra 24 bit yang berukuran 256x256 piksel terdapat 65536 piksel, setiap piksel berukuran 3 byte (komponen RGB), berarti seluruhnya ada 65536x3=196608 byte. Karena setiap byte hanya bisa menyembunyikan satu bit pada LSB-nya, maka ukuran data yang akan disembunyikan didalam gambar maksimum adalah: 196608/8 = 24576 byte. Semakin besar data disembunyikan didalam gambar, semakin besar pula kemungkinan data tersebut rusak akibat manipulasi pada gambar penampung.

C. Kriptografi

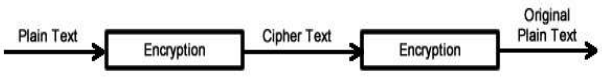
Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim kepada penerima tanpa mengalami gangguan dari pihak ketiga.

Kata Kriptografi berasal dari bahasa Yunani, "*kryptós*" yang berarti tersembunyi dan "*gráphein*" yang berarti tulisan. Sehingga kata Kriptografi dapat diartikan berupa frase "tulisan tersembunyi". Menurut *Request for Comments* (RFC), Kriptografi merupakan ilmu matematika yang berhubungan dengan transformasi data untuk membuat artinya tidak dapat dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, Kriptografi juga bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Artinya, Kriptografi dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas.

Menurut Bruce Scheiner yang ditulis dalam bukunya *Applied Cryptography*, ada empat tujuan mendasar dari ilmu Kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1) Kerahasiaan, yaitu layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka atau mengupas informasi yang telah disandi.
2) Integritas, yaitu faktor penjaga dari perubahan data yang tidak diinginkan. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3) Autentikasi, yaitu identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4) Non repudiasi, yaitu usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat

Dalam Kriptografi dikenal istilah enkripsi dan dekripsi. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Enkripsi mengubah pesan yang akan sampaikan menjadi acak dengan metode atau kuci tertentu. Sedangkan dekripsi adalah mengembalikan pesan yang telah acak melalui tahap enkripsi menjadi seperti semula sehingga dapat dibaca oleh pihak yang diharapkan.



Gambar 3. Enkripsi dan Dekripsi

D. *Caesar Cipher*

Sebuah *cipher* adalah sebuah algoritma untuk menampilkan enkripsi dan kebalikannya dekripsi, serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah *encipherment*. Informasi yang asli disebut sebagai *plaintext*, dan bentuk yang sudah dienkripsi disebut sebagai *chiphertext*. Pesan *chipertext* berisi seluruh informasi dari pesan *plaintext*, tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekasnisme yang tepat untuk melakukan dekripsi.

Caesar *Cipher* dikenal juga dengan Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Misalnya, jika menggunakan geseran 3, W akan menjadi Z, I menjadi L, dan K menjadi N sehingga teks terang "wiki" akan menjadi "ZLNL" pada teks tersandi. Nama Caesar diambil dari Julius Caesar, jenderal, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya.

Cara kerja sandi ini dapat diilustrasikan dengan membariskan dua set alfabet sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci). Misalnya sandi Caesar dengan kunci 3, adalah sebagai berikut:

```
Alfabet Biasa:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabet Sandi:   DEFGHIJKLMNOPQRSTUVWXYZABC
```

E. *Software Prototyping*

Software prototyping dalam *Software Development Life Cycle* (SDLC) adalah suatu metode pembuatan dan pengujian perangkat lunak yang mengacu pada aktivitas menciptakan prototipe aplikasi perangkat lunak, yaitu versi lengkap dari program perangkat lunak yang dikembangkan. *Software prototyping* adalah kegiatan yang dapat terjadi dalam pengembangan perangkat lunak dan sebanding dengan prototyping sebagaimana diketahui dari bidang lain, seperti teknik mesin atau manufaktur[4].

Sebuah prototipe biasanya hanya mensimulasikan beberapa aspek dan berbeda dari produk akhir. *Throwaway* atau *Rapid Prototyping* mengacu pada pembuatan model yang pada akhirnya akan diajukan menjadi bagian dari perangkat lunak yang didiharapkan. Setelah kebutuhan utama terpenuhi, model kerja yang sederhana dari sistem dibangun untuk menunjukkan kepada pengguna persyaratan yang mereka butuhkan.

Keuntungan dari *software prototyping* memiliki keunggulan dibandingkan dengan metode SDLC yang lainnya, salah satunya adalah mengurangi waktu dan biaya. *Prototyping* dapat meningkatkan kualitas persyaratan dan spesifikasi yang diberikan kepada pengembang. Karena perubahan kebutuhan akan mengakibatkan perubahan biaya untuk pembangunan dan implementasi perangkat lunak[5].

Keuntungan lainnya adalah meningkatnya keterlibatan pengguna. *Prototyping* memerlukan keterlibatan pengguna dan memungkinkan mereka untuk melihat dan berinteraksi dengan prototipe yang memungkinkan mereka untuk memberikan umpan balik dan spesifikasi yang lebih baik dan lebih lengkap.

F. *Power Signal Noise Ratio*

Rasio signal-to-noise (sering disingkat SNR atau S / N) adalah ukuran yang digunakan dalam sains dan teknik yang membandingkan tingkat sinyal yang diinginkan dengan tingkat kebisingan latar belakang. Hal ini didefinisikan sebagai rasio dari daya sinyal dengan daya *noise*, sering dinyatakan dalam desibel. Rasio yang lebih tinggi dari 1:1 (lebih besar dari 0 dB) menunjukkan sinyal yang lebih dari kebisingan. Sementara SNR umumnya dikutip untuk sinyal-sinyal listrik, dapat diterapkan untuk setiap bentuk sinyal (seperti tingkat isotop dalam inti es atau biokimia sinyal antara sel-sel). Semakin kecil *noise* atau kebisingan maka kualitas sinyal semakin bagus.

Semua pengukuran nyata terganggu oleh kebisingan atau *noise*. Hal ini termasuk suara elektronik, tetapi juga dapat mencakup peristiwa eksternal yang mempengaruhi fenomena diukur - angin, getaran, gaya tarik gravitasi bulan, variasi suhu, variasi kelembaban, dll, tergantung pada apa yang diukur dan sensitivitas perangkat . Hal ini sering mungkin untuk mengurangi kebisingan dengan mengontrol lingkungan. Jika tidak, ketika karakteristik kebisingan dikenal dan berbeda dari sinyal, adalah mungkin untuk menyaring atau memproses sinyal.

G. Tinjauan Studi

Tinjauan studi yang dijadikan acuan dalam melakukan penelitian ini mengacu pada beberapa penelitian terkait yang telah dilakukan sebelumnya yaitu sebagai berikut.

1) Miftahur Rahim A.A, Achmad Hidayanto & R. Rizal Isnanto [6] membuat penelitian mengenai Teknik Penyembunyian Data Rahasia Dengan Menggunakan Citra Digital Sebagai Berkas Penampung menggunakan metode kualitatif dan algoritma CBC (*cipher block channel*). Data sebelum disisipkan kedalam citra, dibuat dalam blok-blok berukuran 64-bit lalu di-XOR-kan dengan inisialisasi dan kunci 64-bit melalui proses enkripsi CBC, sehingga keamanan data rahasia dapat terjaga.

2) Novi Dian Nathasia dan Anang Eko Wicaksono[7] membuat penelitian mengenai Penerapan Teknik Kriptografi *Stream Cipher* Untuk Pengamanan Basis Data menggunakan algoritma *Caesar Cipher*. Algoritma yang digunakan adalah menggeser ke kanan sebanyak 3 karakter dengan rumus : (P + 3) mod 26 untuk enkripsi dan (P-3)mod 26 untuk dekripsi

3) Khalil Challita dan Hikmat Farhat [8] melakukan penelitian mengenai *Combining Steganography and Cryptography: New Directions* dengan kombinasi algoritma MCO *(multiple cover object*). Membuat kesepakatan antara pengirim dan penerima pesan dalam informasi *password* yang di gunakan sebagai kata kunci.

4) M. Anggrie Andriawan, Solikin & Setia Juli Irzal Ismail [9] melaukan penelitian mengenai Implementasi Steganografi Pada Citra Digital File Gambar Bitmap (Bmp) Menggunakan Java dengan Penyisipan pesan ke dalam bit terendah (LSB) bitmap 24 bit. Menyembunyikan pesan rahasia dengan metode LSB untuk mengeksploitasi keterbatasan sistem penglihatan manusia.

5) David, A. Murtado & Utin Kasma[10] melakukan penelitian mengenai Steganografi Pada Citra Bmp 24-Bit Menggunakan Metode *Least Significant Bit* dengan teknik *pseudo-random number generator* (PRNG). Nilai BPC digunakan sebagai kunci (*key*) untuk mendekripsi pesan rahasia. Kandungan nilai BPC (1 sampai dengan 8).

6) Kavita Kadam, Ashwini Koshti & Priya Dunghav [11] melakukan penelitian mengenai *Steganography Using Least Signicant Bit Algorithm* dengan kombinasi algoritma DCT (*Discrete cosine transformations*). Menyisipkan pesan rahasia kedalam gambar yang dilindungi dengan password pribadi yang terenkripsi

7) Shamim Ahmed Laskar dan Kattamanchi Hemachandran[12] melakukan penelitian mengenai *Secure Data Transmission Using Steganography And Encryption Technique* dengan kombinasi algoritma DCT (*Discrete cosine transformations*). Proses enkripsi dengan cara menggeser ke kanan sebanyak *'n'* dan menggeser ke kiri sebanyak *'n'* karakter sebagai deskripsi.

8) Jamilia Aeni [13] melakukan penelitian mengenai Rancangan Implementasi Protokol S/MIME pada Layanan E-Mail Sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi Secara Online: Studi Kasus PT. XYZ. Penelitian ini menerapkan teknik Kriptografi berupa tanda tangan digital. Memberikan aspek keamanan informasi, dengan mengimplementasikan S/MIME seperti confidentiality, integrity, authentication dan non-repudiation pada tanda tangan digital.

9) Jithesh K and Dr. A V Senthil Kumar [14] melakukan penelitian mengenai *Multi Layer Information Hiding -A Blend Of Steganography And Visual Cryptography*. Penelitian ini melakukan enkripsi gambar rahasia menjadi *n* image sharing. Gambar dipecah menjadi beberapa ('n'), setiap n-1 tidak menunjukkan informasi tentang gambar asli. Setiap gambar dicetak terpisah, dan dekripsi dilakukan dengan menggabungkan file sharing tersebut. Ketika semua *n* yang digabung, gambar asli akan muncul. Satu gambar berisi piksel acak dan gambar lain berisi informasi rahasia.

3. METODOLOGI DAN RANCANGAN PENELITIAN

Dalam penelitian ini metode yang dilakukan sebagai langkah awal dalam observasi terhadap teknik Steganografi dan Kriptografi adalah metode studi pustaka dengan mempelajari landasan teori yang dibutuhkan mengenai Steganografi dan mempelajari Kriptografi pada beberapa literatur dan referensi lainnya. Referensi tersebut berupa data-data dari internet, buku elektronik, publikasi, paper dan dokumen lain yang terkait dalam hal menentukan dan membangun alat penguji penelitian

Tujuan dari penelitian ini yaitu untuk memberikan keamanan berlapis pada Steganografi dengan cara menambahkan Kriptografi pada pesan rahasia yang disisipkan pada *cover image*, dan Kriptografi yang digunakan merupakan modifikasi Kriptografi Caesar Cipher dengan membalikan urutan pesan rahasia kemudian mengesernya 5 karakter. Berdasar kepada tujuan yang disebutkan diatas, penelitian kali ini akan menggunakan metode penelitian eksperimen sebagai metode pengujian. Penelitian eksperimen adalah penelitian dimana peneliti dapat melakukan manipulasi kondisi yang ada sesuai dengan keinginan dan harapan peneliti, berdasar kepada kondisi nyata atau kondisi sebenarnya.

Dalam kondisi yang telah dimanipulasi pada metode eksperimen, biasanya dibuat dua kelompok yaitu kelompok kontrol dan kelompok pembanding. Kelompok kontrol akan diberikan perlakuan tertentu sesuai dengan tujuan penelitian dan kemudian hasil dari perlakuan ini yang akan dijadikan pembanding terhadap kelompok pembanding[15].

A. Teknik Analisis Data

Teknik analisis data dalam penelitian ini menggunakan pendekatan kualitatif dimana data yang telah dikumpulkan sebelumnya dianalisis tidak dengan menggunakan analisis data statistik. Analisis data secara kualitatif dilakukan dengan menganalisis hasil pencatatan teknik Steganografi yang digunakan, penyisipan pesan, keamanan tambahan yang digunakan dan jenis Kriptografi yang digunakan, yaitu dengan membandingkan langkah-langkah dari setiap instrumen yang ada.

B. Rancangan

Salah satu fokus utama penelitian ini adalah keamanan berlapis berupa Kriptografi. Dasar teknik Kriptografi yang digunakan pada penelitian ini adalah Caesar Cipher. Caesar Cipher merupakan teknik Kriptografi dengan menggeser urutan abjad sejumlah n sehingga membentuk kata yang acak. Secara sederhana, Kriptografi Caesar Cipher dengan menggeser 5 karakter dapat dilihat pada simulasi dibawah ini:
Kunci Urutan:

'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z',',','0','1','2','3','4','5','6','7','8','9','!','@','#','$','%','^','&','(',')','A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','+','-','*','/','[',']','{','}','<','>','?','_'

Pesan : ANGGA KUSUMA NUGRAHA

Hasil : FSLLF4PZXZRF4SZLWFMF

Pada penelitian kali ini dilakukan modifikasi terhadap teknik Kriptografi Caesar Cipher menjadi dua tahap. Pada tahap pertama pesan rahasia akan dibalik urutan abjad nya sehingga yang pertama menjadi terakhir sedangkan yang terakhir menjadi yang pertama. Tahap yang kedua pesan rahasia yang telah dibalik urutannya akan di geser sebanyak 5 karakter. Secara sederhana proses Kriptografi pada penelitian dapat disimulasikan sebagai berikut:
Pesan : ANGGA KUSUMA NUGRAHA
Tahap 1 : AHARGUN AMUSUK AGGNA
Tahap 2 : FMFWLZS4FRZXZP4FLLSF

C. Pengujian Prototipe Model

Pada penelitian ini pengujian sistem atau uji coba terhadap alat penguji dilakukan dengan metode kualitatif dan kuantitatif. Metode kualitatif dengan cara melakukan ujicoba terhadap alat penguji dengan berbagai jenis gambar sebagai cover image dan berbagai jenis karakter sebagai pesan rahasia yang akan disisipkan, kemuadian akan diuji tingkat Power Signal Noise Ratio (PSNR) yang terdapat pada antara file gambar yang belum disisipi pesan dengan gambar setelah menjadi stego image. Sedangkan metode kuantitatif dilakukan dengan melakukan ujicoba terhadap alat penguji dengan sejumlah gambar sehingga diketaui tingkat keberhasilan secara statistik. Dengan hal tersebut dapat diketahui tingkat keberhasilan penelitian yang dilakukan.

D. Rencana Strategi

Aspek sistem pada penelitian ini meliputi sistem yang digunakan untuk implementasi alat penguji. Sistem ini digunakan oleh pengirim pensan rahasia maupun penerima pesan rahasia yang memanfaatkan Steganografi. Sistem yang digunakan berupa komputer yang dilengkapi dengan jaringan untuk bertukar pesan rahasia.

Sistem yang dibuat cukup ringan sehingga tidak memerlukan spesifikasi komputer yang terlalu tinggi. Aplikasi telah dicoba pada komputer dengan prosesor Intel Pentuim 4 dan tidak ditemui masalah. Aplikasi penguji dibangun menggunakan bahasa pemrograman Java sehingga bisa berjalan dalam berbagai sistem operasi, aplikasi penguji juga berjalan lancar pada sistem operasi terbaru dari Microsoft yaitu Windows 8.

Setelah melalui tahap pengujian dan evaluasi aplikasi akan diunggah ke public repository yaitu Source Forge (http://sourceforge.net) agar dapat digunakan oleh pengguna interenet secara luas. Tahap ini dilakukan setelah peneliti selesai melakukan perbaikan aplikasi berdasarkan penilaian para reviewer. Proses ini memakan waktu yang cepat, tetpi memerlukan koneksi internet untuk mengunggah aplikasi.

4. IMPLEMENTASI

Setelah peneliti melakukan proses analisis dan perancangan sistem, selanjutnya peneliti akan melakukan implementasi sistem yang telah melalui tahap perancangan tersebut. Pada tahap ini peneliti akan membagi penelitian ini menjadi bagian-

bagian yang menjelaskan kokmponen yang harus diperhatikan dalam implementasi sistem. Tahap ini meliputi spesifikasi perangkat keras, perangkat lunak, dan implementasi program.

A. Spesifikasi Perangkat Keras

Berikut ini adalah spesifikasi dari perangkat keras yang digunakan dalam implementasi sistem dan eksperimen aplikasi Steganografi dengan keamanan berlapis.

Tabel 1. Spesifikasi Perangkat Keras

Perangkat Keras	Spesifikasi
Komputer	▪ Prosesor: Intel Core i5 2,5 Ghz ▪ Memori: 4 GB ▪ *Storage*: 500 GB ▪ Sistem operasi: Microsoft Windows 7 Professional 32 bit

B. Spesifikasi Perangkat Lunak

Sedangkan perangkat lunak yang digunakan dalam implementasi sistem dan eksperimen aplikasi Steganografi dengan teknik "Snap and Share" berbasis Android adalah seperti yang ditunjukkan dalam tabel di bawah ini.

Tabel 2. Spesifikasi Perangkat Lunak

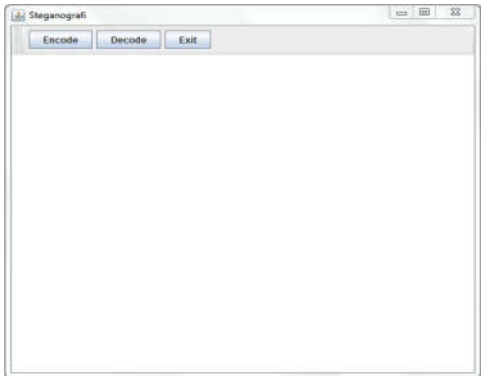
Perangkat Lunak	Spesifikasi
Java Development Kit	JDK 1.7.2.1
JCreator	Pro 3.0.0

C. Implementasi Sistem

Pada tahap implementasi program akan dilakukan penerjemahan rancangan yang dibuat menjadi baris code bahasa pemrograman Java agar dimengerti oleh perangkat komputer untuk mengeksekusi suatu proses. Selain implementasi program untuk mengeksekusi suatu proses akan diimplementasikan pula tampilan GUI dari perancangan layar aplikasi yang dilakukan sebelumnya.

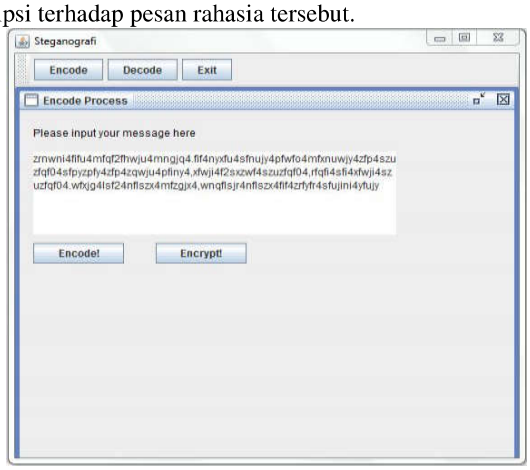
Tahap development dilakuka secara manual menggunakan *software* JCreator Pro 3.0. Pada bagian ini peneliti akan menjelaskan sistem secara urut dan berdasarkan halaman yang ada pada program dan proses yang terjadi.

Pada saat pertama kali aplikasi Steganografi ini dijalankan, yang akan muncul adalah halaman utama dari aplikasi ini. Halaman utama ini memiliki tiga buah tombol, yaitu '*Encode*', '*Decode*' dan '*Exit*'. Tampilan layar halaman utama dapat dilihat pada gambar dibawah ini.



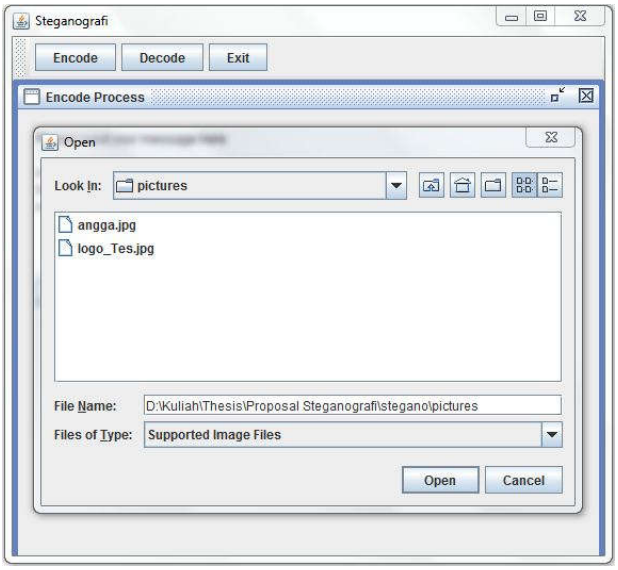
Gambar 4. Halaman Utama

Tahap yang pertama pada mode *encode* adalah proses enkripsi. Dapat dilihat pada gambar 4 terdapat text area pada halaman *encode process* untuk memasukan pesan rahasia yang akan disisipkan. Pengirim dapat mengisi text area tersebut dengan pesan rahasia yang dikehendaki. Setelah itu pengirim perlu menekan tombol '*Encrypt!*' untuk melakukan enkripsi terhadap pesan rahasia tersebut.



Gambar 5. Halaman *Encode Process* Setelah Enkripsi

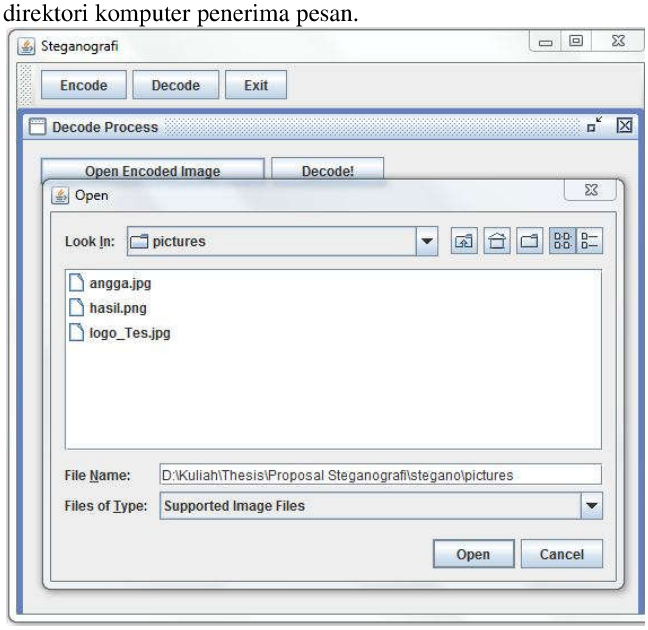
Setelah pesan rahasia dienkripsi, selanjutnya adalah memilih *cover image* dan melakukan encode pesan rahasia kedalam *cover image* yang telah dipilih. Untuk memilih *cover image*, pengirim hendaknya menekan tombol '*Encode!*'. Akan muncul jendela *browse cover image*, pengirim dapat memilih *cover image* dari direktori yang ada pada komputer pengirim. Setelah memilih *cover image* pengirim dapat menekan tombol '*Open*', maka gambar tersebut akan terpilih sebagai *cover image* dan proses encode pesan rahasia kedalam *cover image* tersebut otomatis berjalan



Gambar 6. Tampilan *Browse Cover Image*

Saat memasuki mode *decode*, penerima pesan akan menemukan dua tombol pada halaman *decode process*. Tombol '*Decode!*' berfungsi untuk melakukan *decode* terhadap pesan rahasia yang ada didalam *stego image*, tombol ini akan dijelaskan pada bagian berikutnya.

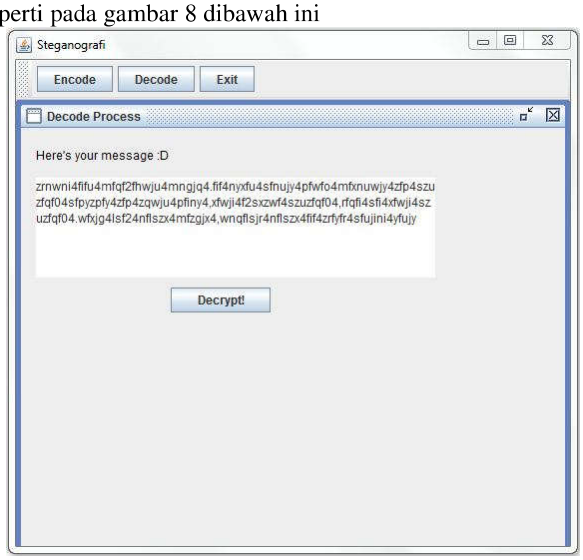
Untuk memilih *stego image* yang akan diekstrak pesan rahasianya, maka penerima pesan harus menekan tombol '*Open encoded image*'. Apabila tombol tersebut ditekan, maka akan tampil jendela *browse stego image*. pada jendela tersebut penerima pesan dapat memilih stego image dari direktori komputer penerima pesan.



Gambar 7. Tampilan *Browse Stego Image*

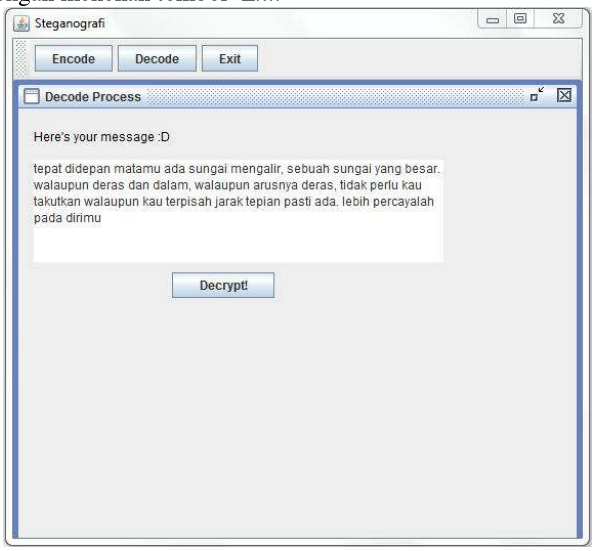
Proses selanjutnya adalah melakukan decode terhadap stego image yang dipilih. Untuk melakukan decode pada stego image yang telah dipilih pada proses sebelumnya, penerima pesan harus menekan tombol '*Decode!*' pada halaman *decode process* yang ditunjukan pada gambar 7.

Apabila penerima menekan tombol '*Decode!*' maka akan tampil halaman *decode process* dengan tombol '*Decrypt!*' seperti pada gambar 8 dibawah ini



Gambar 8. Halaman *Decode Process* Sebelum Dekripsi

Untuk melakukan dekripsi terhadap pesan rahasia yang masih acak tersebut, penerima pesan harus menekan tombol '*Decrypt!*'. Setelah ditekan, maka akan muncul pesan rahasia yang sudah dapat dibaca karena sudah tidak acak. Dengan demikian proses decode sudah selesai, penerima dapat kembali kehalaman utama aplikasi atau keuar dari aplikasi dengan menekan tombol '*Exit*'



Gambar 9. Halaman *Decode Process* Setelah Dekripsi

D. Pengujian Sistem

1) Uji Kualitatif

Pengujian kualitatif dilakukan pada alat penguji dengan sample 2 buah citra digital dengan format ekstensi yang berbeda. Gambar tersebut akan disispi pesan rahasia menggunakan alat penguji, kemudian akan diuji menggunakan *Power Signal Noise Ratio* (PSNR).

Selain *noise* yang menjadi aspek pertimbangan adalah ukuran file, sehingga pada pengujian ini juga akan dibandingkan ukuran file sebelum disisipi pesan dan setelah disisipi pesan dan dicari selisihnya. Dengan demikian bisa didapatkan jenis ekstensi gambar digital yang paling baik untuk digunakan dan yang paling buruk.

Berikut adalah sampel gambar yang ekstensi yang telah disediakan oleh peneliti beserta hasil dari uji kualitatif yang dilakukan.

Tabel 3. Hasil Uji Kualitatif Berdasarkan Noise

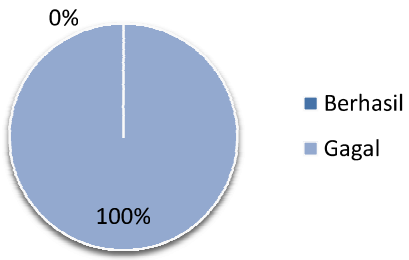
No	File Sebelum	File Sesudah	PSNR
1	jerapah.jpg	jerapah_hasil.png	79.964708586
2	jerapah.png	jerapah_hasil.png	79.955517164
3	jerapah.gif	jerapah_hasil.gif	79.955517165
4	jerapah.bmp	jerapah_hasil.bmp	79.992400145

Tabel 4. Hasil Uji Kualitatif Berdasarkan Ukuran

No	Nama File	Ukuran Sebelum	Ukuran Sesudah	Selisih Ukuran
1	jerapah.jpg	92 KB	611 KB	519 KB
2	jerapah.png	751 KB	677 KB	74 KB
3	jerapah.gif	335 KB	173 KB	166 KB
4	jerapah.bmp	938 KB	199 KB	739 KB

2) Uji Kuantitatif

Pengujian kualitatif dilakukan pada alat penguji dengan melakukan percobaan sebanyak 50 kali pada 50 file citra digital baik proses encode maupun proses decode, sehingga diketahui jumlah keberhasilan dan kegagalan secara statistik.



Gambar 10. Hasil Uji Kualitatif

E. Evaluasi Sistem

Setelah dilakukan pengujian dengan metode kualitatif dan kuantitatif, maka dapat dievaluasi bagaimana kemampuan alat penguji sebagai cerminan dari penelitian ini.

Ujicoba kualitatif dapat diketahui hasilnya dari tabel 3, terbukti aplikasi dapat memproses gambar digital dengan format *.JPG, *.PNG, *.GIF dan *.BMP. Format ekstensi tersebut adalah ekstensi yang populer dan banyak digunakan sebagai gambar digital terutama pada komunikasi dengan jaringan internet, sehingga terbukti aplikasi penguji berhasil menyembunyikan pesan rahasia.

Selain itu pada pengujian ini juga dapat diketahui bahwa gambar digital dengan ekstensi *.PNG setelah melalui proses, adalah gambar dengan tingkat noise paling rendah dan ekstensi *.BMP memiliki tingkat noise yang tinggi.

Apabila dilihat dari perbandingan ukuran file yang ditunjukan pada tabel 4, gambar digital dengan ekstensi *.PNG memiliki selisih paling kecil antara stego image dengan gambar asal. Sedangkan gambar dengan ekstensi *.BMP memiliki selisih ukuran yang besar.

Tingkat noise yang rendah menunjukkan bahwa gambar digital dengan ekstensi tersebut baik digunakan untuk Steganografi dengan keamanan berlapis pada penelitian ini. Hal tersebut karena pada gambar dengan tingkat noise yang rendah, perbedaan antara gambar asal dan stego image rendah sehingga paling mirip sengan aslinya dan paling sulit dibedakan. Oleh karena itu gambar digital dengan ekstensi *.PNG adalah yang terbaik digunakan untuk Steganografi dengan keamanan berlapis dilihat dari faktor banyaknya noise yang dihasilkan.

Selain memiliki tingkat noise yang rendah, gambar digital dengan ekstensi *.PNG juga memiliki selisih ukuran yang paling kecil sehingga gambar digital dengan ekstensi *.PNG juga merupakan terbaik digunakan untuk Steganografi dengan keamanan berlapis dilihat dari faktor selisih ukuran gambar.

Kebalikan dari gambar digital dengan ekstensi *.PNG, gambar digital dengan extensi *.BMP memiliki noise yang tinggi sehingga kurang baik digunakan untuk Steganografi dengan keamanan berlapis pada penenlitian ini dilihat dari faktor tingkat noise. Sedangkan untuk faktor besarnya ukuran file, gambar digital dengan ekstensi *.BMP juga adalah yang paling buruk karena memilik selisih ukuran paling tinggi dengan gambar asal sehingga akan lebih mudah dicurigai oleh pihak ang tidak diinginkan.

Pada ujicoba dengan metode kuantitatif dapat dilihat hasil pada gambar 10 bahwa 50 sampel gambar digital yang diuji semuanya berhasil, maka pada ujicoba kuantitatif ujicoba yang berhasil adalah 100% dan yang gagal adalah 0%.

5. KESIMPULAN

Salah satu solusi keamanan yang dapat ditambahkan adalah kriptografi terhadap pesan rahasia yang akan disampaikan. Pada penelitian ini diterapkan keamanan pada steganografi dengan menambahkan kriptografi Caesar Cipher yang telah dimodifikasi dengan membalik urutan pesan rahasia kemudian digeser 5 karakter. Setelah mengalami enkripsi tersebut pesan rahasia kemudian disisipkan kedalam gambar digital dengan metode *Least Significant Bit* (LSB) yaitu setiap bit pesan rahasia disisipkan pada bit terakhir gambar digital.

Setelah dilakukan pengujian dapat diketahui bahwa aplikasi dapat menyembunyikan pesan rahasia dengan keamanan berlapis dan bekerja pada gambar digital dengan ekstensi populer dan sering digunakan terutama dalam komunikasi pada jaringan internet, yaitu *.JPG, *.PNG, *.GIF dan *.BMP. Dari hasil evaluasi diketahui file dengan ekstensi *.PNG memiliki sifat paling baik untuk digunakan sebagai cover image pada steganografi dengan keamanan berlapis. Dengan demikian steganografi memiliki keamanan berlapis yang memberikan tingkat keamanan lebih baik

Berdasarkan hasil penelitian yang telah dilakukan, maka saran yang dapat diberikan penulis sebagai acuan untuk penelitian lebih lanjut adalah sebagai berikut:

1) Pada penelitian lebih lanjut disarankan bahwa media yang disisipi pesan rahasia bisa berupa file audio atau video.
2) Penelitian juga dapat dilanjutkan dengan membangun aplikasi yang disarankan dilengkapi dengan user login
3) Pada penelitian selanjutnya juga disarankan dapat menerapkan aplikasi ini pada perangkat lainnya seperti smartphone dan smart TV sehingga lebih

DAFTAR PUSTAKA

[1] Namita Tiwari and Dr. Madhu Shandilya, *Evaluation of Various LSB based Methods of Image Steganography on GIF File Format*, International Journal of Computer Applications, vol. 6, September 2010.

[2] Rosziati Ibrahim and Law Chia Kee, *MoBiSiS: An-Android based Application for Sending Stego Image through MMS*, ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology, 2012.

[3] John Crinnion, "*Evolutionary Systems Development, a practical guide to the use of prototyping within a structured systems methodology*" - Page 18. Plenum Press, New York, 1991.

[4] John Crinnion, Evolutionary Systems Development, a practical guide to the use of prototyping within a structured systems methodology - Page 18. Plenum Press, New York, 1991.

[5] Smith MF, *Software Prototyping: Adoption, Practice and Management*. McGraw-Hill, London, 1991.

[6] Miftahur Rahim A.A, Achmad Hidayanto & R. Rizal Isnanto, Teknik Penyembunyian Data Rahasia Dengan Menggunakan Citra Digital Sebagai Berkas Penampung menggunakan metode kualitatif dan algoritma CBC (*cipher block channel*), 2006.

[7] Novi Dian Nathasia dan Anang Eko Wicaksono, Penerapan Teknik Kriptografi *Stream Cipher* Untuk Pengamanan Basis Data menggunakan algoritma *Caesar Cipher,* 2011.

[8] Khalil Challita, Hikmat Farhat, *Combining Steganography and Cryptography: New Directions* dengan kombinasi algoritma MCO *(multiple cover object*), 2011.

[9] M. Anggrie Andriawan, Solikin & Setia Juli Irzal Ismail, Implementasi Steganografi Pada Citra Digital File Gambar Bitmap (Bmp) Menggunakan Java dengan Penyisipan pesan ke dalam bit terendah (LSB) bitmap 24 bit, 2012.

[10] David, A. Murtado & Utin Kasma, Steganografi Pada Citra Bmp 24-Bit Menggunakan Metode *Least Significant Bit* dengan teknik *pseudo-random number generator* (PRNG), 2012.

[11] Kavita Kadam, Ashwini Koshti & Priya Dunghav, *Steganography Using Least Signicant Bit Algorithm* dengan kombinasi algoritma DCT (*Discrete cosine transformations*), 2012.

[12] Shamim Ahmed Laskar dan Kattamanchi Hemachandran, *Secure Data Transmission Using Steganography And Encryption Technique* dengan kombinasi algoritma DCT (*Discrete cosine transformations*), 2012.

[13] Jamilia Aeni, Rancangan Implementasi Protokol S/MIME pada Layanan E-Mail Sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi Secara Online: Studi Kasus PT. XYZ

[14] Jithesh K, A V Senthil Kumar Dr., *Multi Layer Information Hiding -A Blend Of Steganography And Visual Cryptography,* 2012.

[15] Prasetyo, Bambang dan Jannah, L.M., *Metode Penelitian Kuantitatif*, Jakarta: PT. Rajagrafindo Persada, 2005.