Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)
Edisi. .. Volume. ... Bulan 20.. ISSN : 2089-9033

PEMBANGUNAN APLIKASI STEGANOGRAFI PADA VIDEO MENGGUNAKAN METODE *SPREAD SPECTRUM* DAN ALGORITMA LOKI97 UNTUK KEAMANAN DATA

Steven A. Barande[1]

[1]Teknik Informatika – Universitas Komputer Indonesia
Jalan Dipatiukur 112-114 Bandung
E-mail : wildpb_13@yahoo.co.id

ABSTRAK

Kriptografi merupakan teknik untuk menyandikan pesan, yaitu merubah pesan asli menjadi bentuk yang tidak beraturan. Sedangkan Steganografi merupakan teknik penyembunyian pesan. Steganografi memerlukan dua properti, yaitu pesan yang akan disisipkan dan media sebagai penampung pesan. Kriptografi dan steganografi sama-sama memiliki kekurangan, pada teknik kriptografi pesan asli dirubah kebentuk yang tidak beraturan, sehingga masih menimbulkan kecurigaan bagi yang melihatnya. Sedangkan pada teknik steganografi jika letak pesan pada media penampung dapat diungkap keberadaannya, maka informasi tersebut akan dapat diketahui.

Berdasarkan permasalahan yang telah diteliti, maksud dari penulisan tugas akhir ini adalah untuk membangun aplikasi steganografi pada video menggunakan metode *spread spectrum* dan algoritma loki97 untuk keamanan data. Metode *Spread Spectrum* ini memanfaatkan domain frekuensi dari suatu gambar. Langkah yang pertama kali dilakukan dalam steganografi dengan metode *Spread Spectrum* ini adalah mentransformasikan gambar ke domain frekuensi. Namun adapula yang tidak menggunakan transformasi koefisien pada media dan hanya menggunakan *Pseudo Random Number Generator* sebagai bibit pembangkit pengacakan pesan dalam menyembunyikan informasi. *Algoritma LOKI97* termasuk dalam jenis algoritma simetris dan *cipher block*. Dengan demikian algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.

Berdasarkan Implementasi dan hasil pengujian maka dapat ditarik kesimpulan sebagai berikut. Penggabungan kriptografi dan steganografi pada penelitian ini menghasilkan aplikasi yang membantu *user* untuk meningkatkan keamanan data agar kerahasiaan data atau informasi tetap terjaga.

Kata kunci : Steganografi, kriptografi, LOKI97

1. PENDAHULUAN

Pesan atau informasi telah menjadi sesuatu yang sangat penting sejak ribuan tahun yang lalu. Untuk melindungi pesan dari pihak yang tidak berkepentingan digunakan beberapa teknik atau metode untuk melindungi kerahasiaan pesan, diantaranya adalah teknik kriptografi dan teknik steganografi.

Kriptografi merupakan teknik untuk menyandikan pesan, yaitu merubah pesan asli (*plaintext*) menjadi bentuk yang tidak beraturan (*chipertext*). Sedangkan Steganografi merupakan teknik penyembunyian pesan. Steganografi memerlukan dua properti, yaitu pesan yang akan disisipkan dan media sebagai penampung pesan. Kriptografi dan steganografi sama-sama memiliki kekurangan, pada teknik kriptografi pesan asli dirubah kebentuk yang tidak beraturan, sehingga masih menimbulkan kecurigaan bagi yang melihatnya. Sedangkan pada teknik steganografi jika letak pesan pada media penampung dapat diungkap keberadaannya, maka informasi atau pesan tersebut akan langsung diketahui. Dengan menggabungkan kedua teknik tersebut dimaksudkan untuk menambah tingkat keamanan pada pesan atau informasi.

2. LANDASAN TEORI

2.1. Keamanan Sistem Informasi

Sistem keamanan informasi (information security) memiliki empat tujuan yang sangat mendasar adalah :

1. *Confidentiality* (Kerahasiaan)

Informasi pada sistem komputer terjamin kerahasiaannya, hanya dapat diakses oleh pihak-pihak yang diotorisasi, keutuhan serta konsistensi data pada sistem tersebut tetap terjaga. Sehingga upaya orang-orang yang ingin mencuri informasi tersebut akan sia-sia.

2. *Availability* (Ketersediaan)

Menjamin pengguna yang sah untuk selalu dapat mengakses informasi dan sumberdaya yang diotorisasi. Untuk memastikan bahwa orang-orang yang memang berhak untuk mengakses informasi yang memang menjadi haknya.

3. *Integrity* (Integritas)

Menjamin konsistensi dan menjamin data tersebut sesuai dengan aslinya, sehingga upaya orang lain yang berusaha merubah data akan segera dapat diketahui.

4. *Legitimate Use* (Penggunaan yang sah)

Menjamin kepastian bahwa sumberdaya tidak dapat digunakan oleh orang yang tidak berhak.

2.2 Video Digital

Video adalah teknologi pengiriman sinyal elektronik dari suatu gambar bergerak. Video Digital pada dasarnya tersusun atas serangkaian frame. Rangkaian frame tersebut ditampilkan pada layar dengan kecepatan tertentu, bergantung pada laju frame yang diberikan (dalam frame/detik) jika laju frame cukup tinggi, mata manusia tidak dapat menangkap gambar per frame, melainkan menangkapnya sebagai rangkaian yang saling bersambung. Masing-masing frame merupakan gambar/citra (image) digital.

Suatu image digital dipresentasikan dengan sebuah matriks yang masing-masing elemennya mempresentasikan nilai intensitas. Jika I adalah matriks 2 dimensi, I (x,y) adalah nilai intensitas yang sesuai pada posisi baris x dan kolom y pada matriks tersebut. Titik-titik dimana image disampling disebut sebagai picture elements atau sering dikenal sebagai piksel. Karakteristik Video Digital ditentukan oleh resolusi (resolution) atau dimensi frame (frame dimension), kedalaman piksel (pixel depth), dan laju frame (frame rate). Karakteristik-karakteristik ini yang akan menentukan kualitas video dan jumlah bit yang dibutuhkan untuk menyimpan atau mentransmisikannya [2].

2.3 Steganografi

2.3.1 Sejarah Steganografi

Steganografi berasal dari bahasa yunani, yaitu *"steganos"* yang artinya "tulisan tersembunyi". Steganografi sudah dikenal oleh bangsa yunani sejak lama. Herodatus, seorang penguasa yunani, mengirimkan oesan rahasia menggunakan kepala budak atau prajurit sebagai media. Caranya, rambut dibotaki, lalu pesan rahasia ditulis pada kulit kepala budak. Setelah rambut budak tumbuh cukup banyak (yang berarti menutupi pesan rahasia), budak tersebut dikirim ketempat tujuan pesan untuk membawa oesan rahasia dikepalanya. Ditempat penerima kepala budak dibotaki kembali untuk membaca pesan yang tersembunyi dibalik rambutnya [1].

2.3.2 Metode Spread Spectrum

Metode *Spread Spectrum* pertama kali dikenalkan pada sekitar pertengahan tahun 1950. *Spread Spectrum* adalah sebuah teknik pentransmisian dengan menggunakan *pseudo-noise code*, sebaga modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar dari pada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replica *pseudo-noise code* tersinkronisasi. *Spread Spectrum* menggunakan pita lebar, *noise-like* sinyal. Karena sifatnya yang *noise-like*, *spread spectrum* sulit untuk terdeteksi, dipotong, atau ter-modulasi. Hal hal inilah yang menyebabkan *spread spectrum* digunakan untuk komunikasi militer selama bertahun-tahun.

Cara atau langkah menyisipkan pesan rahasia kedalam cover-object pun berbeda-beda, seperti penelitian yang dilakukan pada tahun 2006 yang menggunakan transformasi pada media menggunakan perhitungan *FFT (Fast Fourier Transform)* [12]. Namun adapula yang tidak menggunakan transformasi koefisien pada media dan hanya menggunakan *Pseudo Random Number Generator* sebagai bibit pembangkit pengacakan pesan dalam menyembunyikan informasi, Metode *Spread Spectrum* yang digunakan pada penelitan tersebut mengalikan bit-bit pesan dengan *pseudorandom generator* yang sebelumnya telah di sebar dengan *scalar* pengali.

2.4 Algoritma LOKI97

Algoritma LOKI97 termasuk dalam jenis algoritma simetris dan *cipher block*. Dengan demikian algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.

LOKI97 LOKI97 adalah algoritma yang menggunakan ukuran blok data sebesar 128 bit dan menggunakan kunci yang dapat bervariasi yaitu 128,192 dan 256 bit. Algoritma LOKI97 dalam implementasinya menggunakan elemen-elemen sebagai berikut :

2.4.1 Feistel Network

Feistel Network adalah metode yang umum digunakan pada algoritma kriptografi block cipher. Bagian utama dari feistel network adalah fungsi f, yaitu fungsi pemetaan string input menjadi string output. Pada tiap iterasi, blok sumber merupakan input bagi fungsi f dan kemudian, keluaran dari fungsi f tersebut di XOR dengan blok tujuan, setelah itu kedua blok tersebut dipertukarkan. Algoritma LOKI97 menggunakan 16 iterasi

2.4.2 Data Computation

LOKI97 melakukan enkripsi data plaintext dengan ukuran blok 128 bit untuk menghasilkan ciphertext dengan ukuran 128 bit. Data computation adan membagi 128 bit plaintext menjadi dua-64 yaitu L dan R.

2.4.3 Penjadwalan Kunci

LOKI97 menggunakkan penjadwalan kunci berdasarkan pada feistel network, pengoperasiannya pada empat buah 64 bit data. Dengan menggunakan fungsi f yaitu f (A,B) sebagai penghitungan data untuk memberikan non-linear yang cukup dan memastikan bahwa penghitungan dengan kunci

dapat dilakukan. Penjadwalan kunci dapat diinisialisasi dengan ukuran yang bervariasi yaitu 128 bit, 192 bit dan 256 bit, berdasarkan ukuran dari kunci yang dapat dipakai yaitu pada 4 buah 64 bit data [K4|K3|K2|K1].

2.4.4 Fungsi f (A,B)

Fungsi f(A,B) non linear akan menerima dua buah 64 bit masukan nilai A dan B, memprosesnya dengan menggunakan dua buah S box, untuk menghasilkan keluaran 64 bit. Tiga buah permutasi digunakan untuk memastikan avalanche yang maximal pada fungsi tersebut untuk semua bit.

2.4.5 S-Box

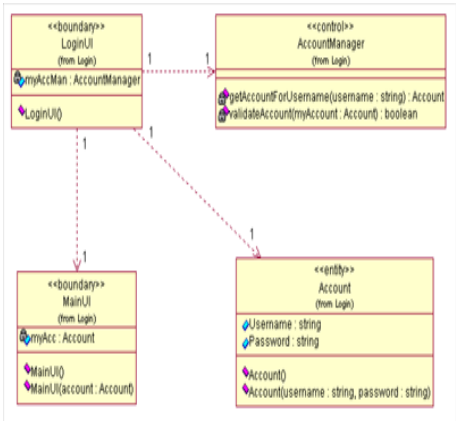
Merupakan suatu table substitusi yang digunakan pada kebanyakan algoritma block cipher. S-box pertama kali digunakan pada Lucifer, kemudian DES dan setelah itu banyak algoritma yang menggunakan LOKI97 menggunakan dua buah S-box yang kesemuanya dibangun dengan menggunkan permutasi bit 8x8 dan kunci.

2.5 *Unified Modelling Language* (UML)

Unified Modelling Language (UML) adalah suatu alat untuk memvisualisasikan dan mendokumentasikan hasil analisa dan desain yang berisi sintaks dalam memodelkan sistem secara visual. UML mempunyai tiga kategori utama yaitu struktur diagram, *behaviour* diagram dan *interaction* diagram. Dimana masing-masing kategori tersebut memiliki diagram yang menjelaskan arsitektur sistem dan saling terintegrasi [9].

***1) Class* diagram**

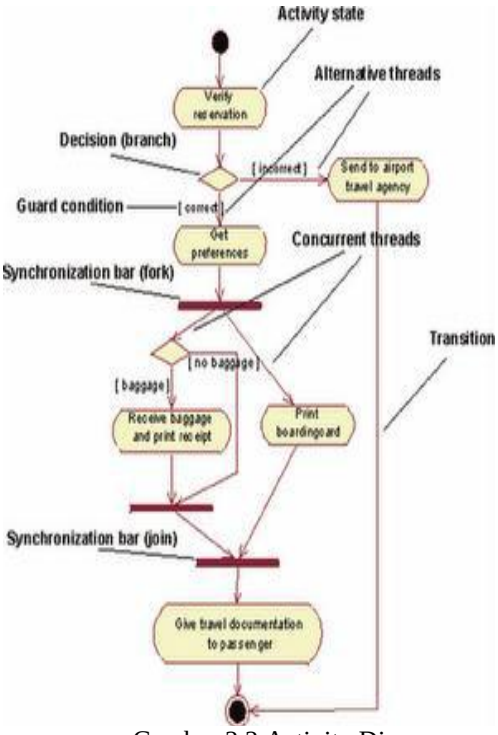
Class diagram menggambarkan struktur statis dari kelas dalam sistem anda dan menggambarkan atribut, operasi dan hubungan antara kelas. *Class diagram* membantu dalam memvisualisasikan struktur kelas-kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak dipakai.



Gambar 2.1 Class Diagram

***2) Activity* diagram**

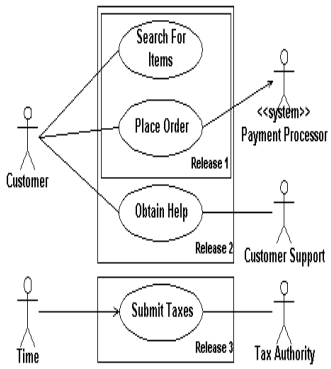
Menggambarkan aktifitas-aktifitas, objek, *state*, transisi *state* dan *event*. Dengan kata lain kegiatan diagram alur kerja menggambarkan perilaku sistem untuk aktivitas



Gambar 2.2 Activity Diagram

***3) Use case* diagram**

Diagram yang menggambarkan *actor*, *use case* dan relasinya sebagai suatu urutan tindakan yang memberikan nilai terukur untuk aktor. Sebuah *use case* digambarkan sebagai elips horizontal dalam suatu diagram UML *use case*. *Use Case* memiliki dua istilah, yaitu *System use case*; interaksi dengan sistem dan *Business use case;* interaksi bisnis dengan konsumen atau kejadian nyata.



Gambar 2.1 *Use Case* Diagram

***4) Sequence* diagram**

Sequence diagram menjelaskan interaksi objek yang disusun berdasarkan urutan waktu. Secara mudahnya *sequence* diagram adalah gambaran tahap demi tahap, termasuk kronologi (urutan) perubahan secara logis yang seharusnya dilakukan untuk menghasilkan sesuatu sesuai dengan *use case* diagram

2.6 Teknologi Java

Java adalah sebuah teknologi yang diperkenalkan oleh Sun Microsystems pada pertengahan tahun 1990. Menurut definisi dari Sun, Java adalah nama untuk sekumpulan teknologi untuk membuat dan menjalankan perangkat lunak pada komputer *stand alone* ataupun pada lingkungan jaringan. Java berdiri di atas sebuah mesin *interpreter* yang diberi nama Java Virtual Machine (JVM). JVM inilah yang akan membaca *bytecode* dalam *file* c*lass* dari suatu program sebagai representasi langsung program yang berisi bahasa mesin.

Oleh karena itu, bahasa *Java* disebut sebagai bahasa pemrograman yang *portable* karena dapat dijalankan pada berbagai sistem operasi, asalkan pada sistem operasi tersebut terdapat JVM. *Platform* Java terdiri dari kumpulan *library*, JVM, kelas-kelas *loader* yang dipaket dalam sebuah lingkungan rutin Java, dan sebuah *compiler*, *debuger*, dan perangkat lain yang dipaket dalam *Java Development Kit* (JDK) [11].

3. ISI PENELITIAN

3.1 Analisis Sistem

Analisis sistem merupakan suatu tahapan yang bertujuan untuk mengetahui dan mengamati apa saja yang terlibat dalam suatu sistem.

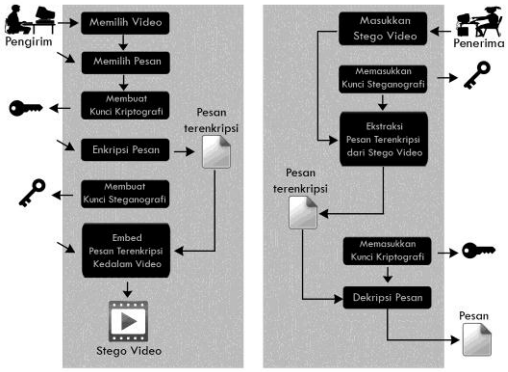
3.1.1. Analisisis Masalah

Dalam mengamankan sebuah informasi atau data rahasia, teknik atau metode yang sering digunakan adalah teknik kriptografi dan teknik steganografi, namun baik kriptografi maupun steganografi masing-masing memiliki suatu kekurangan. Penyandian data dengan teknik kriptografi menghasilkan suatu data yang tidak beraturan sehingga akan menimbulkan kecurigaan bagi pihak yang tidak berkepentingan, sedangkan penyembunyian data dengan teknik steganografi menjadi masalah ketika letak pesan yang ada pada media dapat diketahui, sehingga data atau informasi yang telah disisipkan dapat diungkap oleh pihak yang tidak berkentingan.

3.1.2 Analisis Algoritma

Analisis Algoritma digunakan untuk mengetahui alur proses dari algoritma yang digunakan untuk dapat diterapakan kedalam aplikasi yang akan dibangun. Pembangunan Aplikasi ini menggunakan Algoritma LOKI97 untuk proses enkripsi dan dekripsi sebagai keamanan terhadap informasi yang akan disisipkan. Sedangkan metode steganografi yang digunakan yaitu metode *Spread Spectrum* untuk proses penyisipan dan ekstraksi informasi. Tahapan-tahapan yang dilakukan pada setiap prosesnya yaitu sebagai berikut:

Tahapan-tahapan proses pada aplikasi steganografi yang akan dibangun secara umum dapat dilihat pada gambar 3.1



Gambar 3.1 Gambaran umum aplikasi

3.1.2.1 Analisis Algoritma LOKI97

Algoritma LOKI97 adalah algoritma Kriptografi yang menggunakan ukuran yang simetris dan menggunakan *chiper block*. Sehingga algoritma ini menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Pada algoritma LOKI97 terdapat dua proses yaitu proses penjadwalan kunci dan proses enkripsi.

3.1.2.1.1 Analisis Penjadwalan Kunci

LOKI97 menggunakan penjadwalan kunci berdasarkan pada feistel network, pengoperasiannya pada empat buah 64 bit data. Dengan menggunakan fungsi f yaitu f (A,B) sebagai penghitungan data untuk memberikan non-linear yang cukup dan memastikan bahwa penghitungan dengan kunci dapat dilakukan.

Penjadwalan kunci diinisialisasi dengan ukuran 256 bit, berdasarkan ukuran dari kunci yang dapat dipakai yaitu pada 4 buah 64 bit data $[K4_0|K3_0|K2_0|K1_0]$.

Dengan 256 bit kunci

$[K_a|K_b|K_c|K_d]$, $[K4_0|K3_0|K2_0|K1_0] = [K_a|K_b|K_c|K_d]$

jumlah keseluruhannya 48 iterasi yang dibutuhkan untuk penjadwalan kunci.

3.1.2.1.2 Analisis Enkripsi

Dalam menggunakan enkripsi suatu blok, langkah yang pertama dilakukan adalah penghitungan data dengan membagi dua masukan blok ukuran 128 bit plaintext menjadi dua buah 64 bit data yaitu $[L|R]$ terdiri dari $L_0 = L$; $R_0 = R$.

Proses ini akan mengalami 16 kali iterasi pada feistel network. Setiap iterasi menggunakan operasi XOR dan operasi + untuk nilai 64 bit data dengan keluaran dari fungsi kompleks non linear f (A,B) yang akan menghasilkan nilai avalanche yang maksimal dari semua masukan bit sebagai berikut :

$$R_i = L_{i-1} \text{ xor } f(R_{i-1} + SK_{3i-2}, SK_{3i-1})$$
$$L_i = R_{i-1} + SK_{3i-2} + SK_{3i}$$

Hasil dari proses enkripsi dari masukan 128 bit data plaintext menjadi keluaran 128 bit ciphertext adalah sebagai berikut : $[R_{16}|L_{16}]$.

Proses dekripsi menggunakan algoritma LOKI97 merupakan kebalikan dari proses enkripsi. Untuk proses deskripsi yaitu dengan membagi ciphertext dengan 2 buah 64 bit data yaitu: $[R_{16}|L_{16}]$

Setelah membagi ciphertext menjadi dua maka melakukan proses kebalikan dari proses enkripsi sebanyak 16 kali iterasi. Maka diperoleh hasil deskripsi sebesar 128 bit plaintext, nilainya yaitu :

$$L_i = R_i \text{ xor } f(L_i - SK_{3i-}, SK_{3i-1})$$
$$R_i = L_i - SK_{3i} - SK_{3i-2}$$

Sehingga menghasilkan plainteks awal sebelum proses enkripsi, yaitu :

$[R_0|L_0]$

3.1.2.2 Analisis Metode *Spread Spectrum*

Metode *Spread Spectrum* yang digunakan pada penelitian ini tidak menggunakan fungsi transformasi media. Pesan disisipkan dengan cara disebar dengan *scalar* pengali kemudian di lakukan pengacakan pesan dengan menggunakan bilangan acak *pseudorandom generator* sebagai kunci. Proses dari metode ini adalah mengacak posisi bit pesan dan bit file penampung dengan menggunakan rumus *Linear Congruental Linier* dan fungsi XOR (*Exclusive* OR) kemudian disisipkan pada bit akhir piksel frame.

3.1.2.2.1 Analisis Proses Penyisipan

Sebelum dilakukan proses penyebaran (*spreading*), proses yang dilakukan adalah mengubah pesan kebentuk heksadesimal kemudian ke bentuk biner.

Kemudian biner pesan disebar dengan besaran *scalar* pengalinya empat, akan menghasilkan segmen baru.

Langkah selanjutnya adalah pembangkitan pseudonoise dengan bibit pembangkitan yang ditentukan berdasarkan kunci masukan

Setelah mendapatkan nilai dari kata kunci (101) kemudian nilai tersebut digunakan sebagai bibit awal pembangkitan bilangan acak. Perhitungan pembangkitan bilangan acak sesuai rumus pembangkitan bilangan acak LCG (*Linear Congruential Generator*) .

Sebagai contoh dilakukan lima kali penyebaran, dan hasilnya adalah ”**44 83 74 5 8**” jika diubah dalam bentuk biner menjadi ”**00101100 01010011 01001010 00000101 00001000**”.

Untuk mendapatkan hasil modulasi, segmen pesan akan dimodulasi dengan *pseudonoise signal* menggunakan fungsi XOR (*Exclusive* OR).

Hasil dari proses modulasi inilah yang akan disisipkan ke bit-bit gambar.

3.1.2.2.1 Analisis Proses Ekstraksi

Pada proses ekstraksi prosesnya adalah kebalikan dari proses penyisipan. masukkan kata kunci seperti pada waktu proses penyisipan. selanjutnya pada *body* gambar dilakukan proses penyaringan agar mendapatkan bit-bit hasil modulasi

setelah semua bit-bit hasil modulasi diperoleh, kemudian dilakukan proses demodulasi dengan pseudonoise signal dari kata kunci yang sama pada proses modulasi agar memperoleh bit-bit yang berkorelasi.

Proses berikutnya adalah *de-spreading* yaitu dengan membagi empat hasil *demodulasi*, yang berguna untuk menyusutkan hasil demodulasi menjadi isi pesan yang sebenarnya.

Hasil akhir “**01110100 01100101 01110011 01110100**” merupakan segmen pesan yang sama ketika disembunyikan pada proses embedding. Hasil tersebut kemudian diubah kebentuk karakter akan menjadi menjadi bentuk semula.

3.1.3 Analisis Kebutuhan non-Fungsional

Analisis kebutuhan nonfungsional adalah sebuah langkah dimana seorang pembangun aplikasi menganalisis sumber daya yang dibutuhkan untuk menggunakan aplikasi yang akan dibangun.

3.1.3.1 Analisis Pengguna

Pengguna yang akan menggunakan aplikasi steganografi ini terdiri dari pengirim dan penerima dengan kebutuhan keterampilan seperti pada tabel 3.1.

Tabel 3.1 Kebutuhan Pengguna Aplikasi

Tipe Pengguna	Hak Akses	Tingkat Keterampilan	Jenis pelatihan
Pengirim	Dapat melakukan operasi enkripsi pesan dan penyisipan pesan kedalam video	Dapat mengoperasikan komputer dan memahami konsep steganografi dan kriptografi.	Tidak diperlukan pelatihan khusus.
Penerima	Dapat melakukan operasi dekripsi pesan dan ekstrak pesan video.	Dapat mengoperasikan komputer dan memahami konsep steganografi dan kriptografi.	Tidak diperlukan pelatihan khusus.

4. PENUTUP

4.1 Kesimpulan

Kesimpulan yang didapat berdasarkan hasil analisis, perancangan, implementasi dan pengujian sistem yang dilakukan sebagai berikut :

1. Mayoritas responden menyetujui aplikasi memudahkan user dalam menyandikan dan menyembunyikan data atau informasi rahasia kedalam video.
2. Berdasarkan hasil kuesioner, aplikasi ini memenuhi kriteria-kriteria kriptografi dan steganografi, sehingga tujuan untuk meningkatkan keamanan data agar dapat menjaga kerahasian data telah terpenuhi.

Daftar Pustaka

[1] Munir, Rinaldi. 2006. *Kriptografi.* Informatika, Bandung.

[2] Izza Anshory, Indah Sulistiyowati. Simulasi Penerapan MPEG-4 Untuk Pengiriman Video Melalui Jaringan Wireless. Universitas Muhamadiyah Sidoarjo, Sidoarjo.

[3] A.A. Ngurah Pradnya Adhika. Enkripsi Dan Dekripsi Audio Format AMR Dengan Algoritma Kriptografi LOKI97. Universitas Udayana, Denpasar.

[4] M.A. Ineke Pakereng, Yos Richard Beeh, Sonny Endrawan. 2010. Perbandingan *Steganografi* Metode *Spread Spectrum* Dan *Least Significant Bit* (LSB) Antara Proses Waktu Dan Ukuran *File* Gambar. Universitas Kristen Duta Wacana, Yogyakarta.

[5] Aries Pratiarso, Mike Yuliana, Hadi, M. Zen Samsono Hadi, Fatchul Bahri H., Brahim W. 2012. Analisa PSNR Pada Teknik Steganografi Menggunakan *Spread Spectrum.* Politeknik Elektronika Negeri Surabaya, Surabaya.

[6] Sri Hartati Monalisa. 2014. Steganografi Pada Citra Untuk Pengamanan Data Menggunakan Metode *Spread Spectrum*. STMIK Budidarma, Medan.

[7] Asep Budiman. Aplikasi Steganografi Pada Video Dengan Metode *Least Significant Bit* (LSB). Universitas Komputer Indonesia, Bandung.

[8] Paryati. 2008. Keamanan Sistem Informasi. UPN, Yogyakarta.

[9] Haviluddin. 2011. Memahami Penggunaan UML *(Unified Modelling Language)*. Universitas Mulawarman, Samarinda.

[10] Mahmuddin Yunus, Agus Harjoko. 2014. Penyembunyian Data Pada *File* Video Menggunakan Metode LSB dan DCT. UGM, Yogyakarta.

[11] Farrell, Joyce. 2012. *Java Programming*. Course Technology, United State of America.

[12] Riko Arlando Saragih. 2006. Metode Parity Coding Versus Metode Spread Spectrum Pada Audio Steganography. Universitas Kristen Maranatha, Bandung.

[13] Dinny Devi Triana. Skala Pengukuran sebagai Alat Evaluasi dalam Menilai Tari Karya Mahasiswa. Universitas Negeri Jakarta. Jakarta