TELEMATIKA, Vol. 17, No. 1, APRIL, 2020, Pp. 18 – 25
ISSN 1829-667X

STEGANOGRAFI DENGAN AES PADA MEDIA SUARA BERBASIS INTERNET

Rifki Indra Perwira [(1)], Dessyanto Boedi Prasetyo [(2)] , Fandi Ahmad Juni Haryanto [(3)]
[123]Teknik Informatika, UPN "Veteran" Yogyakarta, Jalan Babarsari 2 Tambakbayan Yogyakarta
e-mail : rifki@upnyk.ac.id[(1)], dess95@gmail.com[(2)], fandiahmadjh@gmail.com[(3)]

Abstract

Information is an important part of the current era. Information has become a necessity so as not to be left behind by the times. By utilizing information, ideas and innovations will emerge. This information can be used for the benefit of many people. The more developed means of communication, the more the use of information is also developing. With the increasing number of ways to access this information, we need an application that can be used to secure information by storing information in containers such as sound, so that information can not be known by others. Steganography is a file hiding technique that becomes confidential so that other people do not understand the secret message that is in it. Cryptography is the science and art of secure messages. Utilizing sound as a media to insert secret messages, as well as adding cryptography as a security message secret before being inserted, so that the process of transferring information can be done safely. The results of this study steganography techniques can be used in sound. By inserting a text message that is first encrypted and then entered into sound by the Least Significant Bit method.

Keywords : Steganography, Cryptography, Least Significant Bit

Informasi merupakan bagian penting di era saat ini. Informasi sudah menjadi kebutuhan agar tidak tertinggal oleh zaman. Dengan memanfaatkan informasi, akan muncul ide dan inovasi. Informasi tersebut bisa digunakan untuk kepentingan banyak orang. Semakin berkembangnya sarana komunikasi, semakin berkembang pula penyelahgunaan informasi. Dengan semakin banyaknya cara mengakses informasi tersebut, maka dibutuhkan sebuah aplikasi yang dapat digunakan untuk mengamankan informasi dengan cara menyimpan informasi didalam wadah seperti suara, sehingga informasi tersebut tidak dapat diketahui oleh orang lain. Steganografi merupakan suatu teknik penyembunyikan file yang menjadi rahasia agar orang lain tidak mengerti pesan rahasia yang ada di dalamnya. Kriptografi adalah ilmu dan seni untuk pesan aman. Memanfaatkan suara sebagai media menyisipkan pesan rahasia, serta menambahkan kriptografi sebagai pengamanan pesan rahasia sebelum disisipkan, sehingga proses pengalihan informasi dapat dilakukan secara aman. Hasil penelitian ini teknik steganografi dapat digunakan pada suara. Dengan menyisipkan pesan teks yang pertama kali dienkripsi dan kemudian dimasukkan ke suara dengan metode *Least Significant Bit*.

Kata Kunci : Steganografi, Kriptografi, *Least Significant Bit*

1. PENDAHULUAN

Perkembangan sarana komunikasi terus mengalami kemajuan. Infrastruktur teknologi terus di tingkatkan sebagai fasilitas kebutuhan masyarakat agar dapat menyesuaikan dengan kemajuan zaman. Jenis komunikasi pun semakin beragam. Dari telepon, pesan singkat, kirim paket suara, bertungkar gambar, *video call* hingga komunikasi secara online. Media internet memberikan informasi yang tak hanya berdampak positif saja, tetapi juga berdapak negatif. Disitus berbagi video terdapat langkah-langkah untuk melakukan penyadapan. Penyadapan tersebut terhubung dengan jaringan internet. Ketika orang tersebut melakukan panggilan, pelaku langsung merekam panggilan tersebut, sehingga informasi yang memiliki aspek kerahasiaan yang sangat penting, dan tidak semua orang mengetahui informasi tersebut bisa saja disalahgunakan dengan tujuan yang tidak baik dan merugikan banyak orang. Dengan semakin banyaknya cara pencurian informasi tersebut, maka diperlukan sebuah aplikasi yang dapat digunakan untuk bertukar informasi dengan cara menyembunyikan informasi yang bersifat rahasia kedalam sebuah media atau wadah seperti suara, gambar hingga video, sehingga informasi tersebut tidak dapat disalahgunakan.

Maka muncul berbagai macam teknik dan metode untuk memberikan rasa aman kepada pengguna ketika berkomunikasi. Steganografi merupakan suatu teknik menyembunyikan data yang bersifat rahasia sehingga orang lain tidak mengetahui pesan rahasia didalamnya. Steganografi adalah ilmu menyembunyikan pesan rahasia sehingga pesan tersebut tidak terdeteksi oleh indera manusia (Munir, 2004).

Kriptografi adalah ilmu dan seni untuk menjaga pesan supaya aman. Pada prinsifnya, kriptografi memiliki empat komponen utama, yaitu *Plaintext* atau pesan yang dibaca, *Chipertext* adalah pesan yang telah diacak, kemudian *Key* atau kunci untuk melakukan kriptografi, dan yang terakhir *Algorithm* atau metode untuk melakukan proses enkripsi dan deskripsi. Perbedaan teknik steganografi dan kriptografi adalah, jika teknik steganografi lebih mementingkan merubahan wadah ketika telah disisipkan pesan didalam. File yang menjadi wadah tidak boleh mengalami perubahan yang dapat dilihat indera. Sementara kriptografi lebih mementingkan keamanan data ketimbang berubahan pada file. Perubahan pada kriptografi sangat terlihat oleh indera.

Teknik steganografi dan kriptografi dapat dikombinasikan dalam satu wadah untuk memperkuat keamanan untuk melindungi pesan rahasia. Kombinasi steganografi dan kriptografi dapat digunakan, deangan memanfaatkan suara sebagai media menyisipkan pesan rahasia, serta ditambahkan kriptografi sebagai pengaman pesan rahasia sebelum disisipkan, sehingga proses pertukaran informasi dapat langsung dilakukan dengan aman, tanpa khawatir pesan rahasia diketahui oleh pihak lain

2. METODE PENELITIAN

2.1 Steganografi

Steganografi adalah teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya tampak seperti informasi normal lainnya. Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu media citra digital, *audio*, atau video. Tujuan utama dari steganografi adalah untuk menyembunyikan informasi ke dalam media lainnya sehingga tidak memungkinkan pihak ketiga untuk mendeteksi keberadaan pesan yang dimaksud, semakin pentingnya nilai dari sebuah informasi, maka semakin diperlukan keamanan untuk menjaga pesan tersebut, maka semakin berkembang pula metode-metode yang dapat digunakan untuk melakukan penyisipan informasi yang didukung pula dengan semakin berkembangnya media elektronik. Steganografi yang baik harus memiliki beberapa syarat yang wajib dipenuhi, yaitu wadah penampungan tidak mengalami banyak perubahan setelah penambahan data rahasia ke dalamnya dan keberadaan data tersebut tetap tersamarkan, kemudian wadah penampungan tidak akan mempengaruhi keberadaan dan kualitas data, selanjutnya data harus bisa dikembalikan ke pada keadaan semula. Dibawah ini merupakan skema proses steganografi yang disisipkan ke dalam media penutup.

2.2 Stukrut Wave

Jenis format Wave merupakan jenis File wave yang paling umum dan hampur dikenal oleh setiap program. Format Wave PCM adalah file wave yang tidak terkompresi, akibatnya ukuran file sangat besar jika file memiliki durasi yang panjang. Format Wave terdiri atas 2 buah SubChunk2: “fmt” dan “data”. SubChunk “fmt“ menggambarkan format *data sound*. SubChunk “data” terdiri atas ukuran besar data dan *data sound* sebenarnya**.**

Wave Audio Format Structure

File Offsite (Bytes)	Field Name	Field Size (Bytes)	Details
0	ChunkID	4	**The "RIFF" chunk descriptor** The format of concern here is WAVE, which requires two sub-chunks: "fmt" and "data".
4	ChunkSize	4	
8	Format	4	
12	Subchunk1ID	4	**The "fmt" sub-chunk** Describes the format of the sound information in the data sub-chunk.
16	Subchunk1Size	4	
20	AudioFormat	2	
22	NumChannels	2	
24	SampleRate	4	
28	ByteRate	4	
32	BlockAlign	2	
34	BitsPerSample	2	
36	Subchunk2ID	4	**The "data" sub-chunk.** Indicates the size of the sound information and contains the raw sound data.
40	Subchunk2Size	4	
44	Data	Subchunk2Size	

Gambar 1. Format Wave Audio

2.3 Pulse Code Modulation

Pulse Code Modulation (PCM) merupakan salah satu teknik untuk proses perubahan dari sinyal analog menjadi sinyal digital yang ekuivalen melalui kode-kode pulsa. PCM merupakan perluasan dari PAM (*Pulse Amplitude Modulation*) yang mana nilai analog akan dibagi menjadi nilai diskrit untuk representasi dari kode diskrit digital. PAM dapat diubah menjadi nilai sistem PCM dengan menambahkan A/D (Analog to Digital) konverter yang sesuai dengan sumber sinyalnya dan D/A (Digital to Analog) konverter pada tempat tujuan. Proses-proses utama pada PCM, diantaranya proses *Sampling* (Pencuplikan), *Quantizing* (Kuantisasi), *Coder* (Pengkodean), *Decoder* (Pengkodean Kembali).

Proses *Sampling* adalah proses mengubah sinyal akustik yang didapat dari perekaman suara menjadi sinyal analog yang sesuai dan kemudian di konversikan dari sinyal analog ke sinyal digital. Perubahan dari sinyal analog menjadi sinyal digital bergantung pada pengambilan *sample* atau contoh. Proses pengambilan contoh harus disesuaikan dengan besaran sinyal analog pada titik tertentu secara teratur dan berurutan untuk mewakili setiap *sample*. Frekuensi *sampling* harus lebih besar dari 2 x frekuensi yang di *sampling*, sekurang-kurangnya memperoleh puncak dan lembah. Hasil penyamplingan berupa PAM. *Quantizing* merupakan proses menentukan segmen-segmen dari amplitudo sampling dalam suara. Pada penerima, sinyal yang masuk telah bercampur dengan berbagai sinyal lain yang tidak diinginkan selama proses pengiriman, hal ini dapat merusak informasi dan akan lebih sulit untuk diproses. Oleh sebab itu sinyal tersebut harus diperbaiki dengan mengunakan blok *Regenerative Repeater*. Didalam *Regenerative Repeater* sinyal tersebut dibersihkan dari sinyal-sinyal yang bercampur selama pengiriman. Selanjutnya dengan prinsip yang sama ketika pengiriman, deretan sinyal biner yang telah diperbaiki dirubah kembali menjadi bentuk analog melalui proses *Decoder*. Sinyal yang telah diubah menjadi seri, dikembalikan menjadi parallel dan dikonversikan ke analog, sehingga keluaran dari *Decoder* berupa sinyal PAM dan kemudian di filter dengan LPF untuk dikembalikan menjadi sinyal informasi.

2.4 Kriptografi

Ada beberapa tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi, yang pertama faktor kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi. Berikutnya yaitu Integritas data yang merupakan berhubungan dengan penjagaan dari perubahan data secara tidak sah. 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. Lalu faktor Autentikasi, adalah berhubungan dengan identifikasi/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. Yang terakhir yaitu Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya

penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

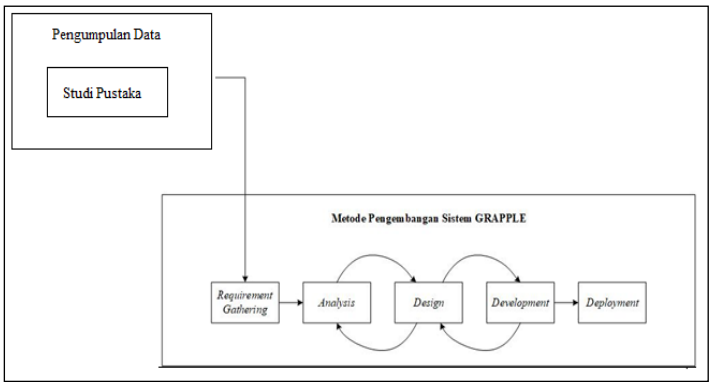
Terdapat beberapa terminologi pada kriptografi yang menjadi dasar dari penggunaan ilmu kriptografi, yang pertama Plainteks dan cipherteks. Pesan adalah suatu informasi atau data yang dapat dibaca dan dimengerti maknanya. Dalam kriptografi, nama lain untuk pesan adalah plainteks. Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan disandikan ke bentuk lain. Bentuk pesan yang tersandi disebut cipherteks. Cipherteks harus dapat ditransformasi kembali menjadi plainteks. Berikutnya pengirim dan penerima dari pesan tersebut. Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas dapat berupa orang, mesin, kartu ATM dan sebagainya. Lalu enkripsi dan deskripsi yang mana Enkripsi (*encryption*) atau *enchipering* adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang dapat dimengerti (plainteks) menjadi sebuah kode yang tidak bisa dimengerti (cipherteks). Sedangkan proses kebalikannya yaitu mengembalikan cipherteks menjadi plainteks disebut dekripsi (*decryption*) atau *deciphering*. Selanjutnya yaitu kunci. Kriptografi modern mengatasi masalah keamanan algoritma kriptografi dengan penggunaan kunci. Kunci (*key*) adalah parameter yang digunakan untuk proses *enchipering* ataupun sebaliknya proses *dechipering*. Kunci biasanya berupa *string* atau deretan bilangan. Dan yang terakhir Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang diberikan. Pelakunya disebut kriptanalis (*cryptanalyst*).

2.5 Studi Literatur

Hasil penelitian maupun gagasan yang tertuang dalam penelitian sebelumnya menjadi landasan teori pada penelitian ini. Adapun penelitian yang terkait dengan penelitian ini, yaitu: Penelitian yang dilakukan oleh (Sudiarta & Sukadarmika, 2009) dengan judul Penerapan Teknologi VoIP Untuk Pengoptimalkan Pengguna Jaringan Internet Kampus Universitas Udayana. Penelitian yang dilakukan oleh (Sitorus, 2015) penelitian tersebut berjudul Teknik *Steganography* Dengan Metode *Least Significan Bit* (LSB). Penelitian yang dilakukan oleh (Purnomo, Priyono, Sari, Ambarwati, & Wulandari, 2012) dengan judul Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi *Voice over Internet Protocol* (VoIP). Penelitian yang dilakukan oleh (Pradipta, A., Nugraha, A. W. W., & Setiawan, I. 2012) yang berjudul Unjuk Kerja Voice over Internet Protocol pada Jaringan Lokal Universitas Jenderal Soedirman. Penelitian yang dilakukan oleh (Setiawan, F. R, & R. R., 2011)dengan judul penelitian Voice over Internet Protocol (VoIP) Menggunakan Asterisk Sebagai Session Initiation Protocol (SIP) Server. Penelitian yang dilakukan oleh (AL-OTHMANI, 2009) dengan judul penelitian Prototype Development of VoIP Steganography.

2.6 Metode Pengembangan Sistem

Pada metodologi pengembangan sistem aplikasi ini menggunakan menggunakan metodologi *Guidelines for Rappid Application Engineering (GRAPPLE).*



Gambar 2. Metodologi *GRAPPLE*

2.2.1 *Requirement Gathering*

Tahapan ini merupakan tahapan untuk menentukan kebutuhan dari sistem berdasarkan berdasarkan informasi yang dikumpulkan pada proses pengumpulan data. Informasi tersebut termasuk perbandingan dengan penelitian sebelumnya

Pengumpulan Informasi

Pengumpulan informasi merupakan proses pencarian informasi-informasi yang berhubungan dengan rumusan masalah penelitian dan perangkat lunak yang akan dikembangkan. Informasi didapatkan berdasarkan analisa data-data yang diperoleh dari tahap sebelumnya. Informasi merupakan hal yang sangat penting, akan tetapi masyarakat masih banyak yang belum sadar akan pentingnya sistem keamanan dalam berkomunikasi. Banyak kasus pencurian informasi yang terjadi disebabkan kurangnya sistem keamanan pada jalur komunikasi. Terdapat berbagai macam cara untuk mengambil suatu informasi. Informasi yang seharusnya bersifat rahasia dan hanya diketahui oleh pihak tertentu bisa disalahgunkan oleh pihak yang tidak bertanggungjawab bahkan dapat merugikan banyak orang. Sehingga dibutuhkan sebuah perangkat lunak yang dapat digunakan sebagai media untuk berkomunikasi yang dapat memberikan keamanan agar informasi tersebut tidak diketahui oleh pihak lain dan kerahasiaan pun tetap terjaga.

Kebutuhan Sistem

Kebutuhan dari sistem yang dikembangkan pada penelitian ini meliputi perangkat keras dan perangkat lunak. Perangkat keras dan perangkat lunak digunakan dalam membuat aplikasi. Penentuan kebutuhan sistem bertujuan agar user memiliki sistem yang sesuai agar dapat menjalankan aplikasi.

2.2.2 *Analysis*

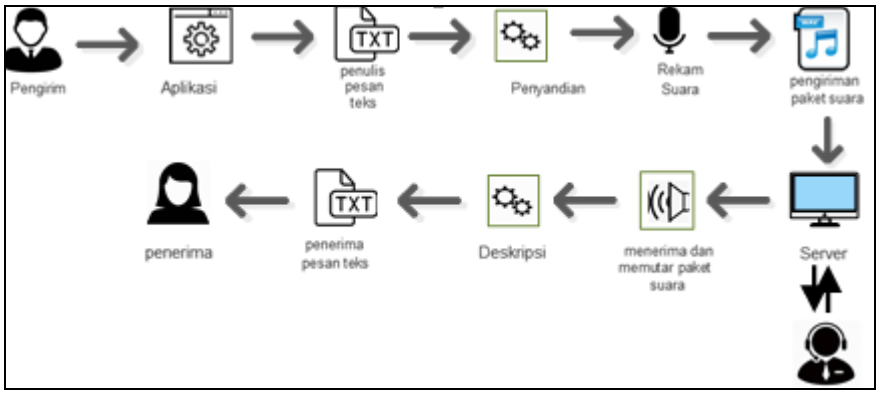
Tahapan selanjutnya yaitu *analysis*. Pada tahapan ini yang dilakukan adalah menggali lebih dalam hasil yang diperoleh dalam tahap sebelumnya. Tahap ini mengkaji permasalahan pengguna dan menganalisis solusinya. Dengan memanfaatkan berbagai macam jenis media, fungsi steganografi dapat digunakan untuk mengamankan informasi dengan cara menyembunyikan pesan rahasia kedalam suatu media tersebut sehingga tidak diketahui orang lain. Steganografi dengan suara sebagai *Cover-media* melalui jaringan IP (*Internet Protocol*) dan pesan teks sebagai *embedded-media*. Pesan teks tersebut terlebih dahulu di enkripsi dan baru kemudian disisipkan pada suara. Pesan yang diterima dalam bentuk suara yang mana dalam pesan suara tersebut terdapat pesan teks yang telah dienkripsi. Agar bisa ketahui isi pesan tersebut, penerima harus mengetahui kuncinya, agar pesan tersebut dapat di deskripsi dan diperoleh informasi dari pesan tersebut.

2.2.3 *Design*

Pada tahap *design* kebutuhan dari tahapan sebelumnya akan dipelajari dan mulai merancang solusi yang dihasilkan oleh tahap *analysis.* Pada tahapan *design* dapat berjalan dua arah saling menyesuaikan sampai diperoleh rancangan yang tepat.

Arsitektur Sistem

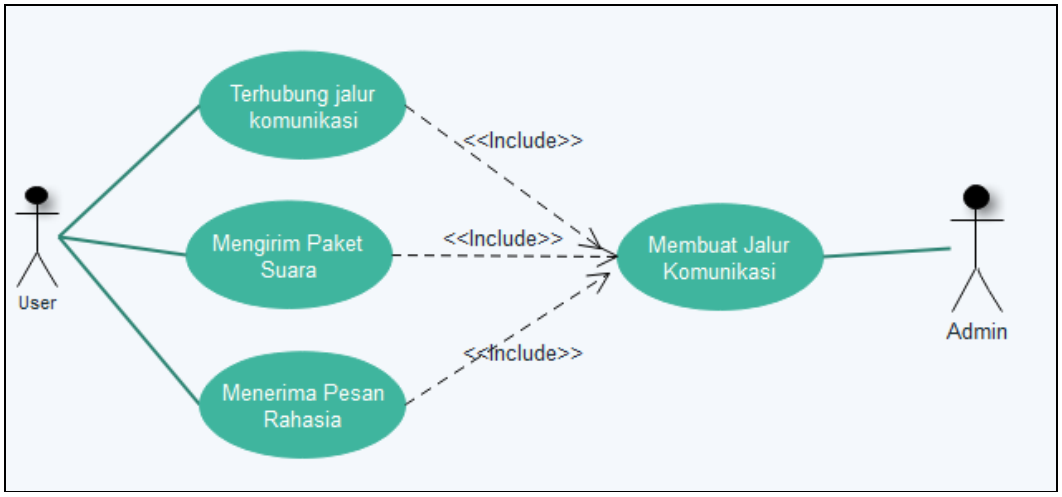
Diagram objek menggambarkan hubungan antar perangkat keras serta perangkat lunak dengan aplikasi penyisipan data pada audio. File teks dapat dibuat ataupun *upload* file teks yang ada oleh *user*.



Gambar 3. Arsitektur Sistem

Use Case Diagram

Use case diagram menggambarkan interaksi antara *user* selaku aktor beserta *use case* dari aplikasi steganografi dengan AES pada media suara berbasis Internet. *Use case* menggambarkan fungsi dari setiap antarmuka pada aplikasi. *Use case* diagram merupakan fungsi dari sistem dimodelkan dengan *use case*.

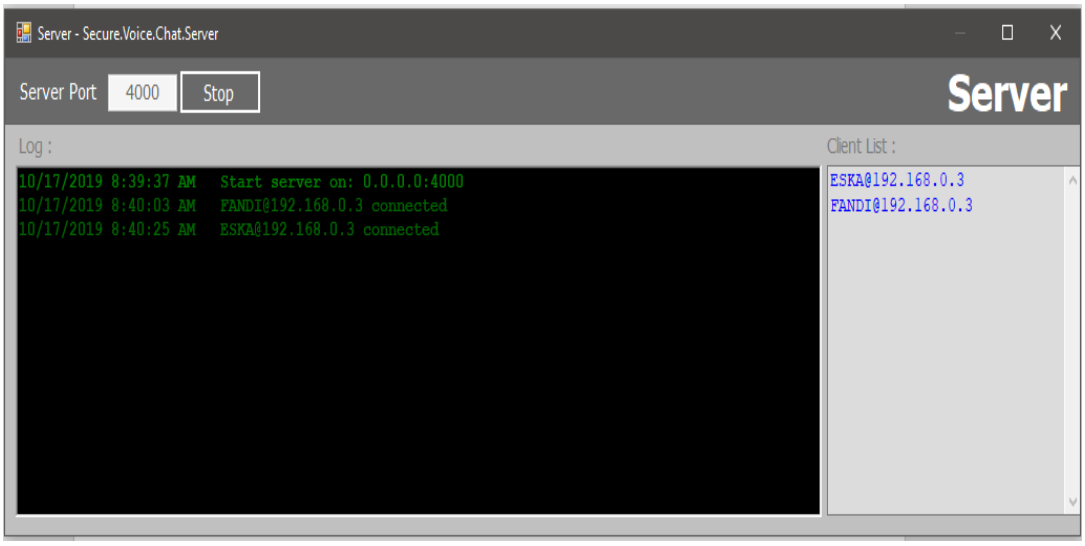


Gambar 4. Use Case Diagram

3. HASIL DAN PEMBAHASAN

3.1 Server

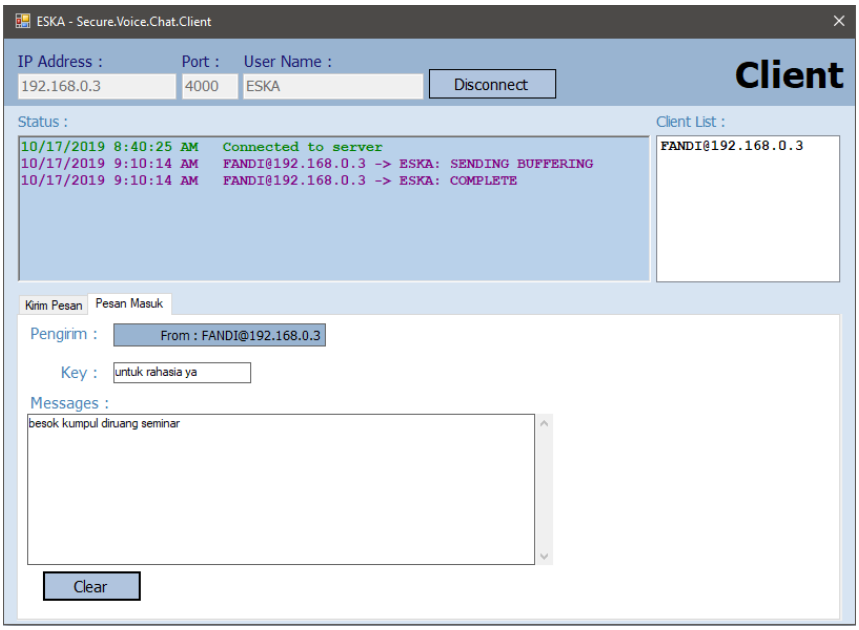
Pada halaman server, admin dapat membuat jalur komunikasi dengan memasukan *port*. Jalur komunikasi dibuat agar *client* dapat terhubung satu dengan yang lainnya. Ketika admin telah memasukan *port*, jika *port* tersedia, maka akan menampilkan status terhubung, dan server bisa digunakan. Jika *port* yang dimasukan admin tidak tersedia, maka akan muncul pemberitahuan bahwa tidak tersedia.



Gambar 5. Halaman Server.

3.2 Client

Jika pengguna ingin melakukan komunikasi dengan pengguna lain, maka masukan IP address dari server, lalu masukan juga port yang ditentukan oleh admin. Jika telah terhubung, paka akan muncul pemberitahuan, kemudian dapat melihat pengguna lain yang telah terhubung dengan server. Jika pengguna ingin mengirim pesan, pilih client tujuan yang tersedia dalam *client list*, kemudian klik, maka secara otomatis akan berada di kolom penerima. Setelah memilih penerima, selanjutnya masukan kunci untuk enkripsi pesan yang akan dirahasiakan, lalu tulis pesan yang akan dikirim kepada penerima. Jika telah selesai, tekan tombol *start talk* untuk merekam suara yang menjadi wadah untuk menyisipkan pesan rahasia tersebut. Durasi rekam suara maksimal 10 detik. Setelah selesai merekam suara, tekan tombol *stop* dan *send*, maka pesan akan dikirim. Dari sisi penerima akan muncul notifikasi, kemudian putar pesan suara, jika telah selesai, tekan tombol *stop*. Untuk membuka pesan, penerima harus memasukan kunci untuk mendeskripsi pesan, jika kunci salah, maka akan muncul umpan balik kunci salah dan pesan tidak terbuka, tetapi jika kunci benar, maka pesan akan ditampilkan



Gambar 6. Halaman Client

3.3 Pembahasan

Aplikasi steganografi ini menggunakan wadah berupa suara. Pesan yang disembunyikan merupakan pesan teks yang sebelum disembunyikan, pesan rahasia di enkripsi menggunakan algoritma AES 128. Algoritma AES 128 merupakan algoritma yang memiliki tingkat keamanan yang kuat dan memiliki waktu proses yang lebih cepat. Pesan disembunyikan didalam suara Selanjutnya penerima bisa mendengarkan suara tersebut yang kemudian suara tersebut di ekstrak hingga didapat pesan yang disembunyikan. Proses penyisipan menggunakan Metode *Least Significant Bit* (LSB). Pada aplikasi ini semua proses berjalan dengan baik. Pesan dapat diterima tanpa merusak suara yang menjadi wadah. Proses keamanan pesan berfungsi dengam baik, sehingga orang yang tidak mengetahi kunci tidak dapat membuka pesan.

KESIMPULAN

Berdasarkan dari hasil penelitian yang telah dilakukan, maka dapat dihasilkan aplikasi steganografi dengan AES pada media suara berbasis Internet. Hasil penelitian yang didapat dari penelitian ini bahwa Steganografi dapat dilakukan pada media suara. Tahapan penyisipan menggunakan metode *Least Significant Bit* yang merupakan menyisipkan pesan di bit terakhir dari wadah. Fungsi kriptografi yang digunakan yaitu AES 128, demikian aplikasi dapat digunakan oleh pengguna yang sesungguhnya.

DAFTAR PUSTAKA

AL-OTHMANI, A. 2009. “Prototype Development of VOIP Steganography.” PhD Thesis. Universiti Teknologi Malaysia.

Munir, 2004, Pengolahan Citra Digital Dengan Pendekatan Algoritmik, Bandung: Informatika.

Purnomo, M, F, E et al. 2012. “Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi Voice over Internet Protocol (VoIP).” *Jurnal EECCIS* 6(2): 183–188.

Setiawan, D. B, Adian F. R, and Isnanto R. R. 2011. “Voice over Internet Protocol (VoIP) Menggunakan Asterisk Sebagai Session Initiation Protocol (SIP) Server.” PhD Thesis. Jurusan Teknik Elektro Fakultas Teknik Undip.

Sitorus, Michael. 2015. “Teknik Steganography Dengan Metode Least Significan Bit (LSB).” *Faklutas Teknik. Universitas Satya Negara Indonesia*.

Sudiarta, and Sukadarmika. 2009. “Penerapan Teknologi Voip Untuk Mengoptimalkan Penggunaan Jaringan Intranet Kampus Universitas Udayana.” *Majalah Ilmiah Teknologi Elektro* 8(2)

Setiawan, D. B, Adian F. R, and Isnanto R. R. 2011. “Voice over Internet Protocol (VoIP) Menggunakan Asterisk Sebagai Session Initiation Protocol (SIP) Server.” PhD Thesis. Jurusan Teknik Elektro Fakultas Teknik Undip.