Prosiding Seminar Nasional Teknologi Informasi dan Kedirgantaraan : Peran Teknologi untuk Revitalisasi Bandara dan Transportasi Udara, Yogyakarta, 10 Desember 2019
SENATIK 2019, Vol. V, ISBN 978-602-52742-1-3
DOI: 10.28989/senatik.v5i0.334

IMPLEMENTATION OF STEGANOGRAPHY ON VOICE OVER INTERNET PROTOCOL (VOIP)

Budi Santosa[1)], Fandi Ahmad Juni Haryanto[2)], Rifki Indra Perwira[3)], Dessyanto Boedi Prasetyo [4)]
Teknik Informatika, UPN "Veteran" Yogyakarta
Jalan babarsari 2 Tambakbayan Yogyakarta
Email : [1]dissan@gmail.com, [2]fandiahmadjh@gmail.com,
[3]rifki@upnyk.ac.id, [4]dess95@gmail.com

Abstract

Steganography is the science of hiding messages into a container without changes detected by the human senses. Cryptography is the science to keeping the message still safe. Combine between Steganography and cryptography can be used, but if there is exchange information still use separately, worry about there is a change in file size, which can result in damage. VoIP is a technology that allows to communicate with use communication lines on a network. VoIP refers more to voice communication. I am utilizing VoIP as a voice communication channel with voice as a medium for inserting secret messages. The research results that steganography techniques can be used with VoIP. By inserting a text message that is first encrypted and then entered into sound by the Least Significant Bit method. The test results, the Alpha testing, and Beta testing, resulted in a percentage above 90%.
Keywords*: Steganography, voice, LSB, cryptography*

1. Pendahuluan

Pada media internet merupakan media yang sangat tinggi tingkat penyalahgunaan informasi. Disitus berbagi video terdapat cara untuk melakukan penyadapan, kemudian pelaku dapat langsung mempraktikan, contohnya dengan 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, sehingga informasi tersebut tidak dapat disalahgunakan.

Steganografi adalah ilmu menyembunyikan pesan rahasia sehingga pesan tersebut tidak terdeteksi oleh indera manusia [1]. Pada steganografi digital bisa menggunakan media digital sebagai sarana penampungan, misalnya menggunakan media gambar, suara, teks, dan video. Pesan rahasia yang disembunyakan dapat berupa citra, suara, teks, atau video. Saat ini banyak bentuk data, akan tetapi dalam steganografi membutuhkan dua media, yaitu *cover-media* merupakan wadah menyembunyikan sesuatu yang dirahasiakan, dan *embedded-media* adalah data atau sesuatu yang disembunyikan. Dalam hal pengamanan data steganografi perlu di kombinasikan dengan metode yang dapat menjaga keamanan file. Kriptografi adalah ilmu 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.

Teknik steganografi dan kriptografi dapat dikombinasikan dalam satu wadah untuk memperkuat keamanan untuk melindungi pesan rahasia. Kombinasi steganografi dan kriptografi bisa digunakan agar memberikan keamanan lebih pada pesan tersebut [8]. Dalam

oenerapan steganografi, ilmu kriptografi yang digunakan bisa berbagai macam, tergantung kebutuhannya [9]. Dari beberapa referensi yang ditemukan, kombinasi steganografi dan kriptografi dapat berjalan dengan baik, akan tetapi hanya sebagai aplikasi keamanan saja. apabila ingin bertukar informasi masih dilakukan secara terpisah, dikhawatirkan terjadi perubahan ukuran file yang mengakibatkan data yang disisipkan menjadi rusak, sehingga informasi menjadi salah atau tidak dapat terbaca.

VoIP (*Voice Over Internet Protocol*) adalah teknologi yang memungkinkan melakukan komunikasi dengan menggunakan jalur komunikasi data pada suatu jaringan. VoIP lebih mengacu pada komunikasi suara (*voice*), *faksimili*, dan *voice messaging application* [2]. Dari teori tentang VoIP, diperoleh penjelasan bahwa VoIP dapat digunakan untuk media komunikasi, terutama mengacu dalam komunikasi suara.

Memanfaatkan media VoIP sebagai jalur komunikasi suara dengan steganografi menggunakan suara tersebut 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. Penerapan steganografi dengan memaafkan media VoIP merupakan hal yang menarik, karena percakapan dalam VoIP digunakan sebagai kamuflase untuk menyembunyikan pesan rahasia, karena data suara secara alami diasumsikan hanya data yang dilakukan di saluran VoIP, lalu komunikasi dengan VoIP biasanya singkat, sehingga tidak memberikan cukup waktu untuk pelaku mendeteksi kemungkinan adanya pesan rahasia pada jalur percakapan tersebut [7].

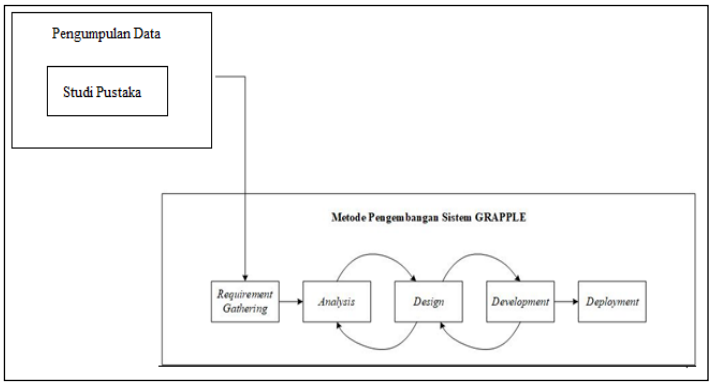
2. Metodologi Penelitian

a. Studi pustaka

Hasil penelitian maupun gagasan yang tertuang dalam penelitian sebelumnya menjadi landasan teori pada penelitian ini. Pada steganografi dengan memanfaatkan media digital seperti teks, suara, gambar, video dan file dan diimplementasikan dengan menfaatkan metode penyisipan. Metode *Least Significant Bit* (LSB) dapat digunakan untuk menyisipkan pesan di bit terakhir dari barisan binner, Karena bit terakhir memiliki nilai yang paling kecil [10]. VoIP adalah teknologi yang memungkinkan percakapan suara dari jarak jauh melalui media internet. Data suara dikonversi menjadi kode digital dan dialirkan melalui jaringan yang mengirimkan paket data. VoIP merupakan salah satu media untuk berkirim pesan berbentuk suara. VoIP mengirimkan data berupa suara menggunakan paket-paket IP. VoIP dilengkapi dengan field untuk steganografi. Field tersebut akan digunakan sebagai covert channel, dimana pesan rahasia dapat dialirkan secara tersembunyi. Selain itu dapat diterapkan juga metode *Least Significant Bits* (LSB) pada data suara yang akan dikirimkan melalui VoIP [11].

b. Metode Pengembangan Sistem

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



Gambar 1. Halaman Server

Langkah-langkah yang dilakukan adalah sebagai berikut:

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

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.

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

4. *Development*

   Tahap ini ditangani oleh pengembang program untuk membangun code program dan *user interface.* Pengujian program dan dokumentasi sistem dilakukan pada tahap ini.

5. *Deployment*

   Tahap *deployment* adalah tahap pendistribusian produk yang dihasilkan kepada pengguna. Tahap ini mencakup instalasi dan perencanaan *backup* data bila diminta oleh pengguna sesuai dengan perjanjian sebelumnya

c. Steganografi

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. Berbagai macam media elektronik kini telah dapat digunakan untuk melakukan berbagai fungsi steganografi dengan berbagai macam tujuan dan fungsi yang diharapkan oleh penggunanya. 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.

Terdapat beberapa jenis teknik steganografi berdasarkan teknik yang digunakan, yaitu sebagai berikut [3]:

1. *Injection*

   Merupakan teknik menanamkan pesan rahasia secara langsung terhadap suatu media, kekurangan dari teknik ini adalah media yang diinjeksi akan menjadi lebih besar dari ukuran normalnya sehingga mudah terdeteksi. Teknik ini juga disebut *embedding*.

2.*Substitution*

   Teknik ini mengubah data normal menjadi data rahasia, hasil dari teknik ini biasanya tidak akan terlalu mengubah ukuran data asli tetapi tergantung pada data yang akan disembunyikan. Teknik ini akan menurunkan kualitas media yang ditumpangi.

3. Transformasi Domain

   Teknik ini sangat efektif, yaitu merubah proses perubahan bentuk citra untuk mendapatkan suatu informasi. Pada dasarnya, transformasi domain menyembunyikan data pada *transform space*.

4. *Spread Spectrum*

   Teknik pentransmisian menggunakan *pseudo-noise code*, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwith*) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.

5. *Statistical Method*

   Teknik ini disebut juga skema steganografi 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.

d. *Voice Over Internet Protocol*

Voice over Internet Protocol (VoIP) merupakan istilah yang masuk pada klasifikasi teknologi transmisi pengiriman komunikasi suara melalui jaringan IP (*Internet Protocol*) seperti internet atau jaringan *packet-switched* lainnya. VoIP adalah metodologi dan kelompok teknologi untuk pengiriman komunikasi suara dan sesi multimedia melalui jaringan Protokol Internet (IP), seperti Internet. Istilah telepon Internet, telepon *broadband*, dan layanan telepon *broadband* secara khusus merujuk pada penyediaan layanan komunikasi (suara, faks, SMS, pesan suara) melalui Internet publik, daripada melalui jaringan telepon sakelar publik (PSTN).

Bentuk paling sederhana dalam sistem VoIP adalah dua komputer terhubung dengan internet. Dengan dukungan software khusus, kedua pemakai komputer bisa saling terhubung dalam koneksi VoIP satu sama lain. Bentuk hubungan tersebut bisa dalam bentuk pertukaran *file*, suara, gambar dan lain sebagainya, akan tetapi penekanan utama dalam VoIP adalah hubungan dalam bentuk suara.

TCP/IP (*Transfer Control Protocol/Internet Protocol*) merupakan sebuah protokol yang digunakan pada jaringan internet. Pada protokol TCP/IP terdapat 2 bagian, yaitu TCP dan UDP serta lapisan yang ada dibawah bagian tersebut terdapat protokol yang disebut IP. TCP (*Transmission Control Protocol*) merupakan protokol yang menjaga reliabilitas hubungan komunikasi antara *end-to-end*. Cara kerja TCP adalah mengirim dan menerima segmen-segmen informasi dengan panjang data yang bervariasi pada suatu datagram Internet. UDP (*User Datagram Protocol*) merupakan salah satu protokol utama di atas IP, yang lebih sederhana dibandingkan dengan TCP.

e. *Least Significant Bit*

Least Significant Bit (LSB) merupakan suatu metode yang mana mengunakan barisan pada data biner dengan nilai yang paling kecil atau paling kanan dari barisan *bit*. *Least Significant Bit* sering kali digunakan untuk kepentingan menyisipkan data kedalam suatu media digital.

Dengan menyisipkan nilai pada bit terakhr dari media yang disediakan, tidak akan berpengaruh besar dari nilai yang semula. Misalkan bit pada gambar dengan ukuran 3 pixel sebagai berikut:

(0011111 11101001 11001000)
(0011111 11001000 11101001)
(1100000 00100111 11101001)

Pesan yang akan disisipkan adalah karakter 'A' yang memiliki biner 10000001, stego audio yang akan dihasilkan adalah :

(0011111 11101000 11001000)
(0011110 11001000 11101000)
(1100000 00100111 11101001)

Dari contoh tersebut dapat disimpulkan bahwa metode LSB hanya mengganti satu nilai dari posisi yang paling kanan dari setiap *bytes* data pada media penampung data. Nilai yang diganti merupakan *bit* dari pesan yang akan disembunyikan. Karena bit yang diganti adalah bit dengan nilai yang paling kecil, maka ukuran dari file pembawa tidak akan berubah sehingga akan sulit untuk terdeteksi [4].

f. Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga keamanan pesan. Selain itu kriptografi juga merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [5].

g. Algoritma *Advanced Encryption Standard* (AES - 128)

Pada sekitar tahun 1990, *National Institute of Standards and Technology* (NIST) menetapkan algoritma *Data Encryption Standard* (DES) sebagai sebagai standar enkripsi data Federal Amerika Serikat. DES termasuk dalam algoritma enkripsi yang sifatnya cipher block, yang berarti DES mengubah data masukan menjadi blok-blok 64-bit dan kemudian menggunakan kunci enkripsi sebesar 56-bit. Setelah mengalami proses enkripsi maka akan menghasilkan output blok 64-bit. Setahun kemudian pada tahun 2000, algoritma Rijndael terpilih sebagai algoritma kriptografi yang selain aman juga efisien dalam implementasinya dan dinobatkan sebagai AES (*Advanced Encryption Standard*). Nama Rijndael sendiri berasal dari gabungan nama penemunya

Algoritma Rijndael atau AES termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. AES mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun AES mempunyai ukuran blok dan kunci yang tetap. Yaitu sebesar AES-128, AES-192, AES-256 bit. Pengelompokkan ini berdasarkan panjang kunci yang digunakan. Angka – angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tiap – tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya round yang dipakai. AES-128 menggunakan 10 round, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 round. AES memiliki ukuran blok yang tetap sepanjang 128 bit dan ukuran kunci

sepanjang 128, 192, atau 256 bit. Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran blok yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap – tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan. Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok – blok tersebut dalam bentuk heksadesimal, kemudian blok itu akan diproses dengan metode berikutnya. Metode yang digunakan dalam algoritma ini yaitu *add round key*, *subbytes*, *shift rows*, *mix columns* [6].

h. Pengujian Alpha testing dan Beta Testing.

1. Alpha Testing

Pengujian pada penelitian ini merupakan pengujian *Alpha* yaitu pengujian yang digunakan dalam pengembangan perangkat lunak. Pengujian *alpha testing* bertujuan melihat penilaian dari sisi pengembang (*developer*) bagaimana pengguna (*user*) menggunakan aplikasi sehingga dapat merekam seluruh permasalahan yang terdapat pada aplikasi. Para penguji merupakan mahasiswa dan alumni Teknik Informatika UPN "Veteran" Yogyakarta.

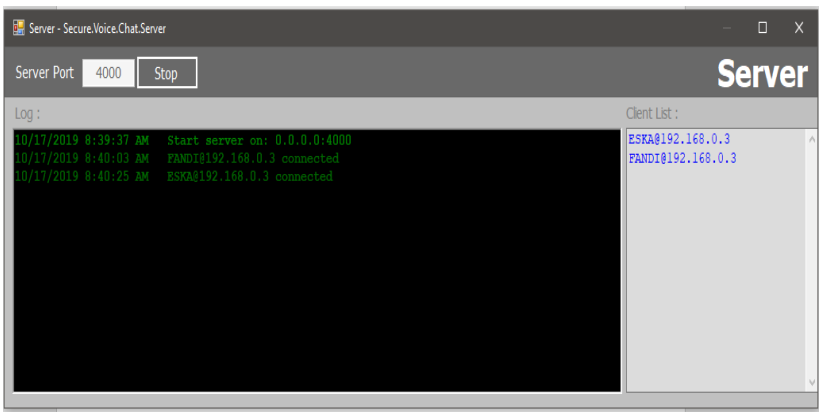
2. Beta Testing

Pengujian *Beta* merupakan pengujian yang dilakukan pada akhir untuk memastikan kegunaan dan fungsi dari perangkat lunak yang dibuat. Pada pengujian perangkat lunak pihak pengembang dapat masukan langsung dari pengguna sebenarnya tentang desain, fungsi, dan kegunaan dari perangkat lunak yang dibuat. Pengujian *Beta Testing* bertujuan melihat penilaian dari sisi pengguna (*user*) menggunakan aplikasi sehingga dapat merekam seluruh permasalahan yang terdapat pada aplikasi. Para penguji merupakan mahasiswa dari beberapa Universitas di D.I Yogyakarta.

3. Hasil dan Pembahasan

a. Halaman Server

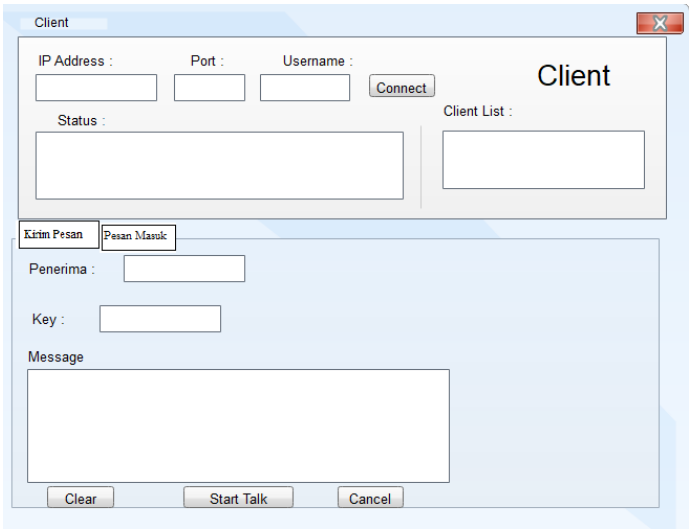
Pada halaman server, admin dapat membuat jalur komunikasi dengan memasukan port. Jalur komunikasi dibuat agar client dapat terhubung satu dengan yang lainnya. Ketika admin telah memasukan port, jika port tersedia, maka akan menampilkan status terhubung, dan server bisa digunakan. Jika port yang dimasukan admin tidak tersedia, maka akan muncul pemberitahuan bahwa tidak tersedia. Tampilan halaman server tersaji pada Gambar 1.



Gambar 2. Halaman Server.

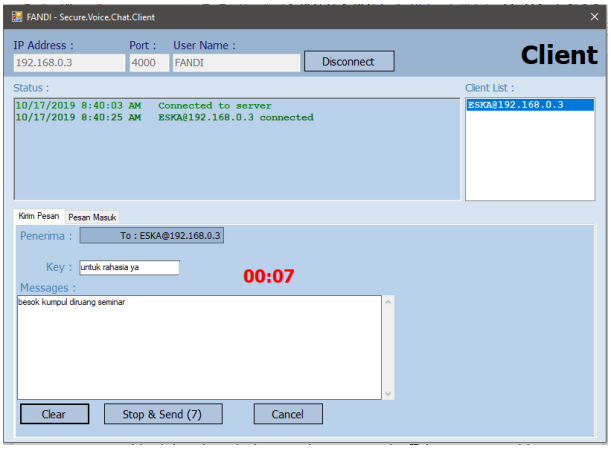
b. Halaman Client

Halam client pada Gambar 2 merupakan halaman yang diberikan kepada pengguna untuk melakukan komunikasi dengan pengguna lain yang telah terhubung dengan server. 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.



Gambar 2. Halaman Client

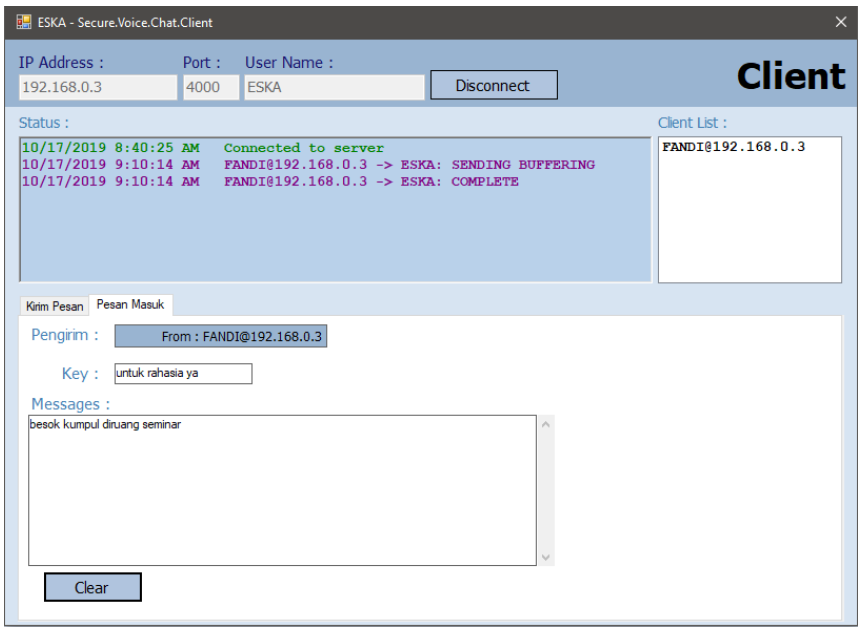
. Jika pengguna ingin mengirim pesan, pilih client tujuan yang tersedia dalam *client list*, kemudian klik, maka secara otomatis akan berada di kolom penerima. Setelah memilih penerima, selanjutnya masukan kunci untuk enkripsi pesan yang akan dirahasiakan, lalu tulis pesan yang akan dikirim kepada penerima. 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. Halaman proses kirim dapat dilihat pada Gambar 3.



Gambar 3. Halaman Client Proses Kirim Pesan

. Dari sisi penerima (Gambar 4), 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 4. Halaman Client Menerima Pesan

c. Pembahasan

Aplikasi steganografi pada ini menggunakan IP sebagai menghubung dengan client lain. Setiap pengguna bisa melakukan komunikasi jika terlebih dahulu tersambung dengan server. Jika dibandingkan dengan penelitaan sebelumnya[10], Pada aplikasi ini dapat bertukar informasi secara langsung dengan penerima pesan tanpa harus melakukan peertukaran secara manual. 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, jika dibandingkan dengan algoritma yang lain[8]. Pesan disembunyikan didalam suara tersebut merupakan suara hasil rekaman pihak pengirim. 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. Pihak pengirim dapat melakukan rekaman suara, dan pihak penerima dapat menerima dan memutar suara. Proses keamanan pesan berfungsi dengam baik, sehingga orang yang tidak mengetahi kunci tidak dapat membuka pesan.

4. Kesimpulan

Berdasarkan dari hasil penelitian yang telah dilakukan, maka dapat dihasilkan aplikasi steganografi dengan media *voice over internet protocol* (VoIP). Hasil penelitian yang didapat dari penelitian ini bahwa Steganografi dapat dikombinasikan dengan media VoIP yang dapat langsung diterima oleh penerima tanpa harus bertukar secara manual. Pada VoIP wadah yang digunakan berupa suara/audio. Tahapan penyisipan menggunakan metode *Least Significant Bit* yang merupakan menyisipkan pesan di bit terakhir dari wadah. Fungsi kriptografi yang digunakan yaitu AES 128. Pengujian menggunakan *Alpha testing* dan *Beta testing*. Dari hasil pengujian tersebut, pada *Alpha testing* dan *Beta testing* dihasilkan prosentase diatas 90%, demikian aplikasi dapat digunakan oleh pengguna yang sesungguhnya.

.

Daftar Pustaka

[1] Munir, R. (2004). Pengolahan citra digital dengan pendekatan algoritmik. *Informatika, Bandung*.

[2] Setiawan, D. B., Fatchur Rochim, A., & Isnanto, R. R. (2011). *Voice over Internet Protocol (VoIP) Menggunakan Asterisk Sebagai Session Initiation Protocol (SIP) Server* (Doctoral dissertation, Jurusan Teknik Elektro Fakultas Teknik Undip).

[3] Ariyus, D. (2009). Keamanan Multimedia, Penerapan Steganografi dalam Berbagai Bidang Multimedia. *Penerbit Andi Offset, Skripsi Amikom Yogyakarta*.

[4] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM systems journal*, *35*(3.4), 313-336.

[5] Sadikin, R. (2012). Kriptografi untuk keamanan jaringan. *Penerbit Andi, Yogyakarta*.

[6] Arifin, R., & Oktoviana, L. T. (2013). Implementasi Kriptografi dan Steganografi menggunakan Algoritma RSA dan metode LSB. *Universitas Malang*.

[7] Prasetiyo, B., Gernowo, R., & Noranita, B. (2014). Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data. *Scientific Journal of Informatics*, *1*(1), 79-93.

[8] Sitorus, M. (2015). Teknik Steganography Dengan Metode Least Significan Bit (LSB). *Faklutas Teknik. Universitas Satya Negara Indonesia*.

[9] Rosida, D. (2008). Studi Mengenai Penerapan Steganografi Pada VoIP Dengan LSB dan *Covert Channel*. *Program Studi Teknik Informatika, Institut Teknologi Bandung*